Linux
Professional
Institute

Security Essentials

Versión 1.0
Español

020

Table of Contents

Linux Professional Institute

Tema 021: Conceptos de seguridad

 Esta obra está bajo la licencia CC BY-NC-ND 4.0.

021.1 Objetivos, roles y actores

Referencia al objetivo del LPI

Security Essentials version 1.0, Exam 020, Objective 021.1

Peso

1

Áreas de conocimiento clave

- Comprensión de la importancia de la seguridad informática
- Comprensión de los objetivos comunes de seguridad
- Comprensión de los roles comunes en seguridad
- Comprensión de los objetivos comunes de los ataques contra los sistemas y dispositivos de TI
- Comprensión del concepto de atribución y cuestiones relacionadas

Lista parcial de archivos, términos y utilidades

- Confidencialidad, integridad, disponibilidad y no repudio
- Hackers, crackers, script kiddies
- Hackers de sombrero negro y blanco
- Acceder, manipular o eliminar datos
- Interrupción de servicios y extorsionamiento por rescates
- Espionaje industrial

Linux Professional Institute

Lección 1

Certificado:	Fundamentos de seguridad
Versión:	1.0
Tema:	021 Conceptos de seguridad
Objetivo:	021.1 Metas, roles y actores
Lección:	1 de 1

Introducción

En las últimas décadas, las tecnologías de Internet han cambiado significativamente la forma en que la sociedad interactúa y la forma en que se satisfacen las necesidades y los deseos básicos. Si bien las necesidades humanas básicas (ya sean físicas, psicológicas, emocionales o intelectuales) siguen siendo las mismas, el auge de Internet ha cambiado para siempre los métodos mediante los cuales se cubren esas necesidades. Internet simula el mundo físico y crea un espacio virtual en el que pueden realizarse muchas actividades del mundo real a través de medios digitales.

Por ejemplo, las compras que tradicionalmente requerían una visita física a una tienda, ahora se pueden hacer en línea a través de sitios web y aplicaciones que replican la experiencia de compra. Los consumidores pueden buscar artículos, usar cupones digitales y realizar compras, todo desde la comodidad de sus hogares. Si bien este cambio ha traído consigo una comodidad y eficiencia sin precedentes, también ha introducido nuevos riesgos. A diferencia de hace veinte años, cuando las compras se hacían principalmente en persona, los consumidores de hoy deben ser conscientes de los posibles riesgos asociados con las transacciones digitales.

Esta mayor dependencia de las plataformas digitales genera una necesidad crítica de contar con una seguridad digital sólida. A medida que las transacciones en línea y el almacenamiento de

datos se vuelven algo común, proteger la información personal y los datos financieros de las amenazas cibernéticas se vuelve esencial. Garantizar la seguridad de la información es ahora una parte fundamental de la vida moderna, necesaria gracias a las comodidades que brinda la tecnología digital.

La importancia de la seguridad informática

La seguridad de las tecnologías de la información (TI) es esencial para proteger los datos del acceso, uso y distribución no autorizados. Garantiza que la información confidencial (ya sea personal, financiera o de propiedad exclusiva) permanezca confidencial y segura mientras se almacena, utiliza y comparte entre usuarios legítimos. El objetivo principal de la seguridad de TI es proteger a las personas y entidades que representan esta información, evitando daños que podrían resultar de la divulgación o el uso indebido no autorizados.

La seguridad informática protege una amplia gama de datos, desde información pública como mapas y manuales hasta registros altamente sensibles como detalles de salud privados y documentos financieros confidenciales. Si bien el acceso no autorizado a datos públicos puede no representar una amenaza directa, la vulneración de información sensible puede tener consecuencias graves, como robo de identidad, pérdidas financieras y daño a la reputación. Por lo tanto, las medidas de seguridad informática son una prioridad para proteger estos datos críticos.

Además, a medida que las tecnologías de Internet se han expandido, también lo han hecho las oportunidades de ciberataques, lo que hace que la seguridad informática sea cada vez más vital. Internet conecta millones de dispositivos en todo el mundo, lo que aumenta el alcance de los posibles daños derivados de las violaciones de seguridad. Como resultado, se necesitan prácticas de seguridad informática sólidas para protegerse contra estas amenazas, garantizando la seguridad e integridad de los datos a gran escala. De este modo, la seguridad informática protege no solo la tecnología y los sistemas existentes, sino también a las personas y los datos asociados a ellas, de posibles daños y explotación.

Comprender los objetivos comunes de seguridad

La gama de objetivos de seguridad de la información es tan variada y diversa como las personas y entidades responsables de los datos que se protegen. En las secciones siguientes se abordarán en detalle muchos objetivos y metodologías específicas. Para sentar una base sólida, es prudente comenzar con los conceptos básicos aceptados por muchos profesionales de la seguridad de la información. Para lograr esta comprensión, abordaremos tres objetivos fundamentales de la seguridad de la tecnología de la información.

La tríada de la CIA

Los tres objetivos principales de la seguridad de la información son la *confidencialidad*, la *integridad* y la *disponibilidad*, comúnmente denominados por los profesionales de la seguridad de la información como la *tríada CIA*, donde la designación CIA proviene de las primeras tres letras de los objetivos principales (La confidencialidad, la integridad y la disponibilidad constituyen los objetivos fundamentales de la seguridad informática).

Figure 1. La confidencialidad, la integridad y la disponibilidad constituyen los objetivos fundamentales de la seguridad informática

La *confidencialidad* se centra en proteger la información del acceso y la divulgación no autorizada, garantizando que los datos permanezcan privados y sean accesibles solo para quienes estén debidamente permitidos. En las redes tecnológicas, mantener la confidencialidad es esencial porque preserva la confianza entre los usuarios y los sistemas con los que interactúan, evitando que la información confidencial quede expuesta o se utilice de forma indebida.

Este principio se basa en el supuesto de que toda la información que pasa a través de una red o que se almacena en ella está destinada a personas y fines específicos. La divulgación no autorizada de esta información puede provocar daños importantes tanto a las organizaciones como a las personas. Por ejemplo, la divulgación no autorizada de secretos comerciales puede provocar pérdidas financieras y comprometer la ventaja competitiva de una empresa, mientras que la exposición de información personal puede dar lugar a robo de identidad y graves violaciones de la privacidad.

Las organizaciones protegen la confidencialidad utilizando varias estrategias, incluido el cifrado,

el control de acceso y las medidas de seguridad de la red. El concepto de integridad es el segundo objetivo de seguridad fundamental de la tríada de principios de seguridad de la información. La integridad garantiza que toda la información dentro de una red, o que pasa a través de ella, permanezca inalterada a menos que las personas adecuadas autoricen modificaciones. Este principio se basa en el supuesto de que la precisión y la coherencia de los datos se mantienen durante todo su ciclo de vida, lo que permite confiar en la autenticidad de la información. Cuando personas no autorizadas obtienen acceso a los datos y los alteran sin permiso, se compromete la integridad de los mismos y se elimina la confianza en su autenticidad, lo que puede causar un daño importante.

La integridad puede considerarse como “confianza”. En un mundo en el que nada escrito o comunicado pudiera ser confiable o verificable, se produciría el caos y sistemas enteros podrían fallar. El espacio digital emplea herramientas y metodologías de seguridad para verificar la validez de la información y las identidades de quienes participan en los intercambios de datos. Garantizar la integridad de la información crea una base para el *no repudio*, lo que significa que el remitente no puede negar su participación en una transacción. El no repudio es esencial para mantener la verdad y la rendición de cuentas en las redes digitales al confirmar que una vez que se toman acciones, no se pueden negar.

Para lograr el no repudio se utilizan métodos específicos que garantizan la autenticidad e integridad de las acciones. Las firmas digitales son una herramienta común que identifica de forma única al remitente y confirma que el contenido no ha sido alterado, lo que garantiza que el remitente no pueda negar el envío de la información.

El objetivo de la integridad va más allá del simple no repudio; abarca el mantenimiento de la precisión, la coherencia y la fiabilidad de los datos. Esto es fundamental para garantizar que los datos permanezcan inalterados respecto de su estado original, lo que permite tomar decisiones precisas basadas en información fiable.

El concepto de *disponibilidad* es el tercer objetivo de seguridad fundamental de la tríada de principios de seguridad de la información. La disponibilidad garantiza que toda la información dentro de una red o que pasa por ella sea accesible para los usuarios autorizados siempre que sea necesario. Este principio se basa en el supuesto de que los usuarios y los sistemas deben poder recuperar la información de manera oportuna, en particular cuando es crítica o urgente. Si una red se ve comprometida y la información solicitada deja de estar disponible, tanto la entidad como sus usuarios no pueden funcionar de manera eficiente, lo que puede provocar interrupciones operativas y pérdida de productividad.

La disponibilidad garantiza que los usuarios autorizados tengan acceso confiable a la información y los recursos según sea necesario, lo cual es esencial para mantener la continuidad del negocio y garantizar que los servicios y operaciones críticos no se interrumpan. Para lograrlo, se emplean

varias estrategias clave, como mecanismos de redundancia y conmutación por error.

Comprensión de los roles comunes en seguridad

Contrariamente a la creencia popular, no todos los roles y responsabilidades asociados con la seguridad de la información son puramente tecnológicos. En esta sección se examinarán brevemente cuatro de los roles más populares asociados con la seguridad de la información: el *director de información*, el *director de seguridad de la información*, el *arquitecto empresarial* y el *administrador de red* o *de sistema*.

El director de sistemas informáticos (CIO) se encuentra en la "C-Suite" (oficinas ejecutivas) de la organización y es responsable de todos los aspectos tecnológicos de la organización. En empresas más pequeñas, este rol también puede incluir responsabilidades administrativas y de seguridad física. Esta persona es responsable de la elaboración de presupuestos, la solicitud y la implementación de cualquier activo bajo su control que cumpla una función tecnológica.

El director de seguridad de la información (CISO) es un ejecutivo de alto nivel responsable de la estrategia general de seguridad de la información de la organización. Esta función incluye el desarrollo de políticas y procedimientos, la garantía del cumplimiento de las normas y la dirección de los esfuerzos de la organización para protegerse contra las amenazas cibernéticas. El CISO desempeña un papel fundamental en la alineación de las iniciativas de seguridad con los objetivos empresariales y en la comunicación de la importancia de la seguridad a la junta ejecutiva y a las partes interesadas. El puesto de CISO está formado por personas con una sólida base de conocimientos tanto en el negocio de la empresa como en el sector tecnológico. Dominan los lenguajes de los negocios y la tecnología, y se espera que sean un "puente" entre el escalón superior de la dirección corporativa y los líderes de las iniciativas tecnológicas. El puesto es relativamente nuevo y ha tenido un éxito limitado. Solo el tiempo dirá si este puesto se mantiene dentro del organigrama.

El *Arquitecto Empresarial* generalmente responde directamente al CIO y tiene la responsabilidad sobre el sistema de tecnología de la información físico y lógico de la entidad. Esta persona suele tener una gran cantidad de experiencia técnica (especialmente en administración de redes) y diseña la red de la entidad para proporcionar los requisitos de seguridad necesarios.

Los administradores de sistemas de red diseñan, implementan y mantienen los controles de seguridad técnica que protegen la infraestructura de TI de una organización. Son responsables de implementar cortafuegos, sistemas de detección de intrusiones (IDS) y protocolos de cifrado. También desarrollan scripts de automatización para optimizar los procesos de seguridad y garantizar que los sistemas sean resistentes a los ataques.

En paralelo a los muchos roles que existen dentro de las filas legítimas de los profesionales de la

tecnología, hay muchos roles y títulos asumidos por aquellos con intenciones ilegítimas. En conjunto, se los conoce en todo el mundo como hackers. Sin embargo, este término general incluye numerosos subgrupos de hackers que operan con una amplia gama de habilidades e intenciones.

Los hackers son personas con conocimientos avanzados de sistemas y redes informáticas. Si bien la percepción pública de los hackers suele ser negativa, no todos tienen intenciones maliciosas. Existen distintos tipos de hackers, que se dividen principalmente en hackers de sombrero negro y de sombrero blanco.

Los hackers de sombrero negro utilizan sus habilidades técnicas para explotar vulnerabilidades con fines maliciosos, como robar datos, interrumpir servicios o dañar sistemas. Operan fuera de los límites de la ley, motivados por el lucro, objetivos políticos o satisfacción personal. Las técnicas que utilizan los hackers de sombrero negro incluyen la implementación de malware, el phishing y la ingeniería social para manipular a las personas para que revelen información confidencial.

Por el contrario, los hackers de sombrero blanco, también conocidos como hackers éticos, emplean sus habilidades para ayudar a las organizaciones a identificar y solucionar vulnerabilidades de seguridad. Los hackers de sombrero blanco suelen ser empleados por empresas o trabajan como consultores independientes para realizar pruebas de penetración y evaluaciones de vulnerabilidad. A diferencia de los hackers de sombrero negro, los hackers de sombrero blanco se adhieren a un estricto código de ética y trabajan dentro de marcos legales para fortalecer la postura de seguridad de una organización y defenderse contra amenazas potenciales.

Por otro lado, los crackers son individuos que se dedican a actividades ilegales, como entrar en sistemas, eludir contraseñas y licencias de software, con la intención de causar daño, robar información o interrumpir servicios. Se considera que los crackers son más maliciosos que los hackers éticos, ya que sus acciones están motivadas únicamente por la intención de explotar sistemas y causar daños sin tener en cuenta la legalidad ni la ética.

Los script kiddies representan una categoría diferente dentro de la comunidad de hackers, que se caracteriza por su falta de experiencia y su dependencia de scripts y herramientas preescritos para llevar a cabo ataques cibernéticos. A diferencia de los hackers expertos, los script kiddies no comprenden del todo las herramientas que utilizan ni suelen tener la capacidad técnica para desarrollar las suyas propias. En cambio, emplean scripts que se encuentran fácilmente disponibles y a menudo obsoletos en Internet para atacar sistemas menos seguros. Su motivación suele surgir del deseo de causar trastornos o ganar notoriedad en lugar de ganancias económicas u objetivos políticos. A pesar de su falta de habilidad, los script kiddies pueden representar una amenaza importante para la seguridad de la información, ya que el uso de herramientas automatizadas puede provocar daños considerables, especialmente cuando atacan sistemas poco

seguros.

Comprender los objetivos comunes de los ataques contra los sistemas y dispositivos de TI

A medida que los dispositivos informáticos se vuelven parte integral de la sociedad, las tácticas y los motivos de los atacantes cibernéticos evolucionan junto con los avances tecnológicos. Cada nuevo dispositivo o tecnología que se adopta de forma generalizada se convierte en un objetivo potencial de explotación, ya que los actores maliciosos buscan hacer un uso indebido de estas herramientas contra usuarios legítimos. La sofisticación de estos ataques puede variar enormemente, desde operaciones técnicas muy avanzadas que requieren habilidades especializadas hasta esquemas más sencillos que dependen de conocimientos informáticos básicos y la colaboración con otros actores maliciosos.

Un objetivo común de los ciberatacantes es acceder, manipular o eliminar datos. El acceso no autorizado permite a los atacantes robar información confidencial, como propiedad intelectual, registros financieros o datos personales. Estos datos pueden luego usarse para obtener ganancias financieras, chantajear o venderse a la competencia. La manipulación de datos implica alterar la información para interrumpir las operaciones, socavar la confianza o manipular los resultados en sectores críticos como los mercados financieros o las elecciones. Eliminar datos importantes puede perjudicar significativamente las operaciones de una organización, lo que provoca pérdidas financieras y tiempo de inactividad operativa. Un claro ejemplo es el ciberataque de 2014 a Sony Pictures, donde los atacantes accedieron y publicaron datos confidenciales, manipularon registros de empleados y eliminaron información valiosa para crear caos y exigir un rescate.

Otro objetivo principal de los ciberatacantes es interrumpir los servicios y exigir rescates. Esto se puede lograr mediante métodos como los ataques de denegación de servicio distribuido (DDoS), que inundan la red de un objetivo con un tráfico excesivo, lo que hace que los servicios no estén disponibles para los usuarios legítimos. Estos ataques se utilizan a menudo para extorsionar un rescate o causar daños a la reputación de la víctima. Los ataques de ransomware implican el cifrado de datos o sistemas críticos y la exigencia de un pago para restablecer el acceso, extorsionando directamente a las víctimas que no pueden permitirse un tiempo de inactividad prolongado. El ataque de ransomware WannaCry de 2017 es un ejemplo notable, que interrumpió los servicios de numerosas organizaciones en todo el mundo mediante el cifrado de datos y la exigencia de pagos de rescate.

El *espionaje industrial* es otro objetivo importante de los ciberatacantes, en particular de aquellos que buscan robar secretos comerciales valiosos o información confidencial de las empresas. Estos ataques suelen ser perpetrados por competidores o estados-nación que buscan ventajas

económicas. Los objetivos del espionaje industrial incluyen robar secretos comerciales para replicar el éxito de un competidor, socavar la posición de mercado de una empresa mediante el acceso a información confidencial y sabotear operaciones, cadenas de suministro o procesos de fabricación para causar pérdidas financieras y dañar la reputación. Un ejemplo destacado de espionaje industrial es la Operación Aurora de 2010, en la que los atacantes atacaron a grandes empresas como Google y Adobe para robar propiedad intelectual e información confidencial.

Entendiendo el concepto de atribución

El concepto de atribución es esencial en los entornos digitales y es una responsabilidad clave para los profesionales de la seguridad de la información. En términos simples, la atribución implica identificar y asignar responsabilidad a las personas por sus acciones en el espacio virtual. Esta lección presenta el concepto brevemente, porque se explorará en varios contextos a lo largo del curso. La aplicación y la importancia de la atribución pueden diferir según el área específica, como la protección de datos, el cifrado, el hardware de red o la gestión de bases de datos, y estas variaciones se analizarán en detalle más adelante.

Comprender quién es responsable de cualquier acción que se realice dentro de una red (ya sea que implique modificar documentos o eliminar registros almacenados) es fundamental para mantener una postura de seguridad sólida. La atribución no solo fortalece las medidas de seguridad, sino que también hace cumplir la rendición de cuentas. Resulta complicado para un usuario negar sus acciones en un entorno tecnológico cuando existen múltiples sistemas de registro, software especializado y protocolos de Internet que rastrean y registran claramente estas actividades.

La atribución establece un marco de rendición de cuentas, pero no se centra únicamente en identificar conductas indebidas. También se utiliza para reconocer y verificar acciones positivas dentro del espacio digital.

En el mundo físico, el principio de atribución es algo que experimentamos con regularidad, tanto los usuarios técnicos como los no técnicos. Por ejemplo, cuando se reconoce a un autor la redacción de un libro o un artículo, se le reconoce su mérito. De manera similar, cuando se nombra a personas como ganadoras de premios, se les reconoce su mérito por sus logros. Incluso cuando un autor menciona una cita, se aplica la atribución. Piense en la atribución como una “huella de responsabilidad”, un aspecto fundamental de la seguridad de la información que se repetirá a lo largo de su carrera en el ámbito de la seguridad.

Sin embargo, en el ámbito digital, lograr una atribución precisa es una tarea compleja que plantea numerosos desafíos para los profesionales de la seguridad. La tecnología permite a los actores maliciosos disfrazar sus identidades, ocultar sus ubicaciones físicas y ocultar sus verdaderas intenciones. A pesar de estos desafíos, existen soluciones de software y hardware diseñadas para

ayudar a los equipos de seguridad a determinar la atribución en entornos digitales, de manera muy similar a las herramientas que utilizan las fuerzas del orden para identificar e investigar la falsificación de moneda. A pesar del conocimiento, la experiencia y las herramientas disponibles para atribuir delitos a sus perpetradores, los delincuentes hábiles a menudo encuentran formas de tener éxito. Las mismas complejidades y desafíos de la atribución en el mundo físico también se aplican al panorama digital.

Ejercicios guiados

1. ¿Por qué es crucial la seguridad informática en el contexto de las transacciones digitales y el almacenamiento de datos?

2. ¿Cuáles son los tres objetivos principales de la seguridad de la información y por qué son importantes?

3. ¿Cuál es el papel de un director de seguridad de la información (CISO) y por qué es importante en una organización?

 Esta obra está bajo la licencia CC BY-NC-ND 4.0. |

Ejercicios exploratorios

1. ¿Por qué muchos ataques a los recursos de información digital tienen éxito?

2. ¿Existe una razón legítima para publicar en Internet una herramienta de piratería que pueda ser utilizada por los script kiddies para llevar a cabo ataques maliciosos y disruptivos?

Resumen

La tecnología de la información, que ha ampliado el alcance y el poder de tantas personas de manera positiva, también amplía el alcance y el poder de los actores maliciosos. Para proteger la seguridad y los derechos de las personas en la actualidad, todos debemos estar atentos a las actividades maliciosas y tomar medidas para prevenirlas o recuperarnos de ellas.

Los objetivos de la seguridad de la información se enmarcan en las categorías generales de confidencialidad, integridad y disponibilidad. Todos ellos son importantes para el funcionamiento de las organizaciones modernas. Un aspecto clave de la integridad es atribuir las acciones a las personas adecuadas. Los tres objetivos requieren apoyo a nivel administrativo, técnico y físico.

Existen muchos puestos de trabajo relacionados con la seguridad en el mercado laboral, y también muchos tipos de atacantes. La mayoría de los hackers de sombrero negro están motivados por objetivos financieros, pero algunos lo están por iniciativas gubernamentales, posturas ideológicas o simplemente por el placer de crear disrupción.

 Esta obra está bajo la licencia CC BY-NC-ND 4.0. |

Respuestas a los ejercicios guiados

1. ¿Por qué es crucial la seguridad informática en el contexto de las transacciones digitales y el almacenamiento de datos?

   La seguridad informática es crucial en el contexto de las transacciones digitales y el almacenamiento de datos porque protege la información confidencial del acceso no autorizado, el uso indebido y la distribución. Con el auge de las tecnologías de Internet, muchas actividades que tradicionalmente se hacían en persona, como las compras, ahora se realizan en línea. Este cambio ha aumentado la cantidad de datos personales y financieros que se almacenan y transmiten a través de Internet, lo que hace que sea esencial proteger estos datos de las amenazas cibernéticas. Las medidas de seguridad informática eficaces garantizan que los datos permanezcan confidenciales, mantengan su integridad y estén disponibles para los usuarios autorizados, lo que evita el robo de identidad, la pérdida financiera y el daño a la reputación.

2. ¿Cuáles son los tres objetivos principales de la seguridad de la información y por qué son importantes?

   Los tres objetivos principales de la seguridad de la información, conocidos como la tríada CIA, son la confidencialidad, la integridad y la disponibilidad. La confidencialidad garantiza que la información confidencial sea accesible solo para aquellos que están autorizados a verla, lo que la protege del acceso y la divulgación no autorizados. La integridad garantiza que los datos permanezcan precisos e inalterados, excepto por los usuarios autorizados, lo que es esencial para mantener la confianza en la información. La disponibilidad garantiza que los usuarios autorizados tengan acceso oportuno a la información y los recursos cuando sea necesario, lo que es crucial para mantener la continuidad del negocio y la eficiencia operativa. En conjunto, estos objetivos ayudan a proteger los datos de las violaciones, mantener la confianza en las interacciones digitales y garantizar la confiabilidad de los sistemas de TI.

3. ¿Cuál es el rol de un Director de Seguridad de la Información (CISO) y por qué es importante en una organización?

   El rol de un Director de Seguridad de la Información (CISO) es supervisar y gestionar la estrategia general de seguridad de la información de una organización. El CISO es responsable de desarrollar e implementar políticas y procedimientos de seguridad, garantizar el cumplimiento de las regulaciones pertinentes y liderar los esfuerzos para proteger a la organización de las amenazas cibernéticas. Este rol es importante porque alinea las iniciativas de seguridad con los objetivos comerciales, comunica la importancia de la ciberseguridad a las partes interesadas y garantiza que la organización esté preparada para responder y recuperarse de posibles incidentes de seguridad. Al gestionar la postura de seguridad de la organización, el CISO ayuda a proteger sus activos digitales, mantener su reputación y

respaldar su éxito operativo general.

 Esta obra está bajo la licencia CC BY-NC-ND 4.0.

Respuestas a los ejercicios exploratorios

1. ¿Por qué muchos ataques a recursos de información digital tienen éxito?

   Existen muchas razones para el éxito de los ataques. En primer lugar, debido a que los ataques a través de Internet son de bajo costo en relación con los ataques físicos y a menudo muy lucrativos, un número cada vez mayor de actores maliciosos están tomando el campo y siempre están buscando nuevas formas de eludir las defensas.

   Desafortunadamente, el costo y el daño a la reputación causados por un ataque son a menudo menores que el costo de prevenirlo (aunque el ransomware cambia la ecuación al imponer enormes daños y costos). Esta falta de incentivos para proteger los recursos, junto con la escasez de personal de seguridad experto, lleva a muchas organizaciones a invertir poco en protección. + El phishing (mensajes de correo electrónico fraudulentos) permite ingresar a una red a través de un empleado relativamente poco capacitado y desprevenido.

2. ¿Existe una razón legítima para publicar en línea una herramienta de piratería que pueda ser utilizada por script kiddies para llevar a cabo ataques maliciosos y disruptivos?

   Sí. Las herramientas de piratería son muy importantes para investigar y verificar la seguridad de las redes. Los hackers de sombrero blanco utilizan estas herramientas constantemente con el objetivo de proteger los activos. Si no hubiera herramientas de intrusión de alta calidad disponibles para los usuarios legítimos, el campo sería más vulnerable a los ataques de herramientas poderosas creadas por actores maliciosos.

021.2 Evaluación y gestión de riesgos

Referencia al objetivo del LPI

Security Essentials version 1.0, Exam 020, Objective 021.2

Peso

2

Áreas de conocimiento clave

- Conozca las fuentes comunes de información en cuanto a seguridad
- Comprensión del esquema de clasificación de incidentes de seguridad y tipos de vulnerabilidades
- Comprensión de los conceptos de evaluación de seguridad y análisis forense de TI
- Conocimiento de los sistemas de gestión de seguridad de la información (SGSI) y de los planes y equipos de respuesta a incidentes de seguridad

Lista parcial de archivos, términos y utilidades

- Vulnerabilidades y exposiciones comunes (CVE)
- Identificación CVE
- Equipo de respuesta ante emergencias informáticas (CERT)
- Pruebas de penetración
- Ataques no dirigidos y amenazas persistentes avanzadas (APT)
- Vulnerabilidades de seguridad de día cero
- Ejecución remota y explicación de vulnerabilidades de seguridad
- Escala de privilegios debido a vulnerabilidades de segurida

Lección 1

Certificado:	Fundamentos de seguridad
Versión:	1.0
Tema:	021 Conceptos de seguridad
Objetivo:	021.2 Evaluación y gestión de riesgos
Lección:	1 de 1

Introducción

Comprender cómo evaluar el riesgo asociado con una vulnerabilidad de seguridad, y determinar la necesidad y urgencia de una respuesta es fundamental para mantener un entorno seguro y resistente. Esta lección profundiza en las habilidades y los procesos necesarios para navegar de manera eficaz por la amplia gama de datos de seguridad disponibles, destacando la importancia de distinguir las amenazas críticas de los problemas menores y tomar decisiones informadas que protejan los sistemas y los datos de posibles daños.

Fuentes de información de seguridad

En el panorama digital en rápida evolución de hoy, la capacidad de encontrar e interpretar información de seguridad relevante es esencial para cualquier profesional de la ciberseguridad. En esta sección se exploran las fuentes clave de información de seguridad y se explica cómo contribuyen a una postura sólida en materia de ciberseguridad.

En primer lugar, es fundamental conocer las fuentes habituales de información sobre seguridad. Estas fuentes suelen ser lugares u organizaciones de confianza que proporcionan datos actualizados y precisos sobre vulnerabilidades de seguridad, amenazas emergentes y mejores

prácticas. Estar familiarizado con estas fuentes permite a los profesionales de la ciberseguridad anticiparse a las amenazas potenciales, reaccionar con rapidez a los riesgos emergentes y aplicar las medidas de seguridad más recientes para proteger sus sistemas.

Una de las fuentes de información de seguridad más reconocidas es el sistema de vulnerabilidades y exposiciones comunes (Common Vulnerabilities and Exposures, CVE). CVE es una lista estandarizada que identifica y clasifica las vulnerabilidades en los sistemas de software y hardware. Sirve como punto de referencia para los profesionales de la ciberseguridad de todo el mundo, ya que proporciona un lenguaje común para analizar y abordar las vulnerabilidades. Al estandarizar la identificación de vulnerabilidades, CVE facilita el intercambio de información entre diversas plataformas y organizaciones, lo que permite una respuesta coordinada a las amenazas de seguridad.

A cada vulnerabilidad incluida en la base de datos CVE se le asigna un identificador único conocido como *CVE ID*. Estos identificadores son fundamentales para rastrear vulnerabilidades específicas y garantizar que todas las partes interesadas estén debatiendo el mismo problema. Un CVE ID generalmente incluye detalles sobre aspectos de la vulnerabilidad, los sistemas afectados y el impacto potencial.

Una entrada CVE generalmente describe una vulnerabilidad de seguridad específica en software o hardware que se ha identificado, documentado y divulgado públicamente. A continuación, se muestra un ejemplo de una entrada CVE (CVE-2024-29824):

```
Nombre: Vulnerabilidad de inyección SQL en Ivanti Endpoint Manager (EPM)
Descripción: Una vulnerabilidad de inyección SQL no especificada en el servidor principal de
Ivanti EPM 2022 SU5 y versiones anteriores permite que un atacante no autenticado dentro de
la misma red ejecute código arbitrario.
Puntuación: 9,6
Gravedad: Crítica
Versión: 3,0
Proveedor: Ivanti
Producto: EPM
Acción: Aplique mitigaciones según las instrucciones del proveedor o deje de usar el
producto si las mitigaciones no están disponibles.
Fecha de adición: 2024-10-02
Fecha de vencimiento: 2024-10-23
Publicado: 2024-05-31
Actualizado: 2024-05-31
```

Otra fuente vital de información sobre seguridad es el Equipo de Respuesta a Emergencias Informáticas (CERT, por sus siglas en inglés). Los CERT son grupos especializados de expertos en

ciberseguridad dedicados a responder a incidentes de ciberseguridad y difundir información sobre posibles vulnerabilidades y amenazas. Estos equipos suelen estar afiliados a agencias gubernamentales, instituciones educativas o grandes corporaciones, y sirven como primera línea de defensa en la gestión y mitigación de incidentes cibernéticos. Los CERT desempeñan un papel fundamental en la coordinación de respuestas a amenazas cibernéticas generalizadas, proporcionando alertas oportunas y ofreciendo orientación para mitigar riesgos. Los CERT también actúan como valiosos centros de intercambio de información, que pueden proporcionar información sobre patrones de amenazas emergentes y recomendar las mejores prácticas para prevenir futuros ataques.

Comprensión de la clasificación de incidentes de seguridad y tipos de vulnerabilidades

En el campo de la ciberseguridad, comprender cómo se clasifican los incidentes de seguridad y reconocer los diferentes tipos de vulnerabilidades que pueden explotarse es crucial para desarrollar defensas efectivas.

Los esquemas de clasificación de incidentes de seguridad son marcos que categorizan los incidentes de seguridad en función de criterios específicos, como el tipo, la gravedad y el impacto. Estos esquemas ayudan a las organizaciones a evaluar rápidamente la naturaleza y el alcance de un incidente, determinar la respuesta adecuada y comunicar la situación de manera eficaz a todas las partes interesadas relevantes.

Es igualmente importante comprender los tipos de vulnerabilidades que pueden ser explotadas por los atacantes. Las vulnerabilidades son debilidades en un sistema que pueden ser explotadas para obtener acceso no autorizado, causar daños o robar información. Se presentan en diversas formas y pueden surgir de fallas en el software, hardware o incluso errores humanos. Entre los tipos de vulnerabilidades más preocupantes se encuentran las *vulnerabilidades de día cero*. Se trata de fallas previamente desconocidas en el software o hardware que aún no han sido descubiertas por el proveedor o desarrollador, lo que deja a los sistemas desprotegidos y altamente vulnerables a los ataques. Las vulnerabilidades de día cero son particularmente peligrosas porque no existe un parche o solución, lo que permite a los atacantes explotarlas libremente hasta que se detecten y solucionen.

Otro tipo importante de vulnerabilidad está relacionada con la *ejecución remota*. Las vulnerabilidades de ejecución remota permiten a los atacantes ejecutar código arbitrario en un sistema de destino desde una ubicación remota. Esta capacidad puede comprometer la totalidad del sistema, lo que permite a los atacantes instalar malware, robar información confidencial o incluso tomar el control de toda la red. Las vulnerabilidades de ejecución remota suelen explotarse mediante ataques basados en la red, en los que los atacantes utilizan paquetes

diseñados o cargas útiles maliciosas para activar la vulnerabilidad y obtener acceso no autorizado.

Las vulnerabilidades de escala de privilegios representan otra amenaza crítica. Estas vulnerabilidades ocurren cuando un atacante obtiene acceso o permisos superiores a los permitidos normalmente, lo que potencialmente le otorga la capacidad de ejecutar acciones no autorizadas o acceder a datos restringidos. El escalar privilegios puede ser vertical, donde los atacantes obtienen privilegios de nivel superior a su nivel actual, u horizontal, donde los atacantes acceden a privilegios asignados a otros usuarios con niveles de acceso similares. Este tipo de vulnerabilidad es particularmente peligrosa en entornos donde el acceso privilegiado está estrictamente controlado, ya que puede permitir a los atacantes eludir las medidas de seguridad y comprometer sistemas o datos críticos.

Los ataques no dirigidos son intentos amplios y no específicos de explotar vulnerabilidades en cualquier sistema disponible, a menudo ejecutados a través de scripts automatizados o herramientas que buscan debilidades conocidas. Estos ataques son oportunistas y no discriminan entre objetivos, sino que apuntan a causar la mayor cantidad de interrupciones posible o a obtener acceso no autorizado a cualquier sistema vulnerable.

Por el contrario, las *amenazas persistentes avanzadas* (APT, por sus siglas en inglés) son ataques altamente sofisticados y específicos diseñados para infiltrarse en organizaciones o entidades específicas durante un período prolongado. Las APT suelen ser llevadas a cabo por atacantes bien financiados y hábiles, como grupos patrocinados por el estado o cibercriminales organizados que tienen un objetivo claro, y están dispuestos a invertir una cantidad significativa de tiempo y recursos para lograrlo. Las APT se caracterizan por su sigilo y persistencia, y a menudo emplean múltiples vectores de ataque y técnicas avanzadas para evadir la detección y mantener el acceso a la red objetivo durante el mayor tiempo posible.

Comprensión de las evaluaciones de seguridad y la informática forense

En el ámbito de la ciberseguridad, hay dos prácticas cruciales que son esenciales para proteger los sistemas y responder a los incidentes: las *evaluaciones de seguridad* y la *investigación forense de TI*.

Las evaluaciones de seguridad son evaluaciones sistemáticas de los sistemas de información y redes de una organización para identificar vulnerabilidades, evaluar riesgos y determinar la eficacia de las medidas de seguridad existentes. Estas evaluaciones ayudan a las organizaciones a comprender su postura de seguridad e identificar áreas que requieren mejoras. Las evaluaciones de seguridad pueden adoptar diversas formas, incluidas evaluaciones de vulnerabilidad, auditorías de seguridad y pruebas de penetración. Cada tipo de evaluación proporciona diferentes

perspectivas sobre el marco de seguridad de una organización, lo que permite una comprensión integral de los riesgos potenciales.

Las *pruebas de penetración*, a las que a menudo se denomina *ethical hacking*, son una técnica de evaluación de seguridad proactiva que simula ataques a un sistema para identificar vulnerabilidades antes de que los actores maliciosos puedan explotarlas. Durante una prueba de penetración, los evaluadores expertos, a menudo llamados *pentesters*, imitan las tácticas, técnicas y procedimientos de los atacantes del mundo real para descubrir debilidades en las defensas de la organización. El objetivo de las pruebas de penetración es identificar brechas de seguridad que podrían no ser evidentes a través de análisis de vulnerabilidades automatizados u otras formas de prueba. Al identificar estas debilidades, las organizaciones pueden tomar medidas correctivas para fortalecer sus medidas de seguridad y reducir la probabilidad de un ataque exitoso.

Además de las evaluaciones de seguridad, la *ciencia forense informática* o ciencia forense digital se centra en la investigación y el análisis de incidentes cibernéticos para determinar su causa, alcance e impacto. La ciencia forense implica la recopilación, conservación y examen de evidencia digital de sistemas informáticos, redes y otros dispositivos digitales. El objetivo principal de la ciencia forense informática es descubrir los detalles de un incidente de seguridad, incluyendo cómo ocurrió, quién fue responsable y qué datos o sistemas se vieron afectados.

El proceso de análisis forense de TI comienza con la identificación y recopilación de evidencia digital relevante, que debe conservarse cuidadosamente para mantener su integridad y admisibilidad en procedimientos legales. Los analistas forenses utilizan herramientas y técnicas especializadas para analizar la evidencia recopilada, reconstruir eventos e identificar la fuente del incidente. Este análisis a menudo incluye el examen de archivos de registro, tráfico de red y otros artefactos digitales para rastrear las acciones del atacante y determinar cómo obtuvo acceso al sistema.

Uno de los aspectos clave de la investigación forense de TI es su papel en la respuesta a incidentes. Cuando se produce una violación de seguridad, una respuesta rápida y eficaz es crucial para minimizar los daños y evitar más riesgos. La investigación forense de TI proporciona la información necesaria para comprender la naturaleza del ataque y desarrollar un plan de respuesta específico. Al identificar los métodos utilizados por los atacantes y el alcance del daño, las organizaciones pueden tomar las medidas adecuadas para contener el incidente, mitigar su impacto y evitar que vuelva a ocurrir.

Sistema de gestión de seguridad de la información (SGSI) y respuesta a incidentes

En la era digital actual, proteger la información confidencial es una prioridad fundamental para

las organizaciones de todos los tamaños. Para lograrlo, las empresas deben adoptar un enfoque integral de la seguridad de la información que incluya medidas proactivas y reactivas.

Un *Sistema de Gestión de Seguridad de la Información* (SGSI) es un marco sistemático para gestionar los datos confidenciales de una organización y garantizar su seguridad. El objetivo principal de un SGSI es proteger la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de un proceso de gestión de riesgos. Esto implica identificar las amenazas potenciales a los activos de información, evaluar los riesgos asociados a estas amenazas e implementar los controles adecuados para mitigarlos. Un SGSI eficaz no se limita a la tecnología; también abarca a las personas y los procesos, creando un enfoque holístico para gestionar los riesgos de seguridad de la información.

La implementación de un SGSI suele seguir normas internacionales como la ISO/IEC 27001, que proporciona directrices para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información. El cumplimiento de estas normas ayuda a las organizaciones a identificar sistemáticamente los riesgos de seguridad e implementar controles acordes con el nivel de riesgo. El marco del SGSI está diseñado para ser dinámico, lo que permite a las organizaciones adaptarse a las amenazas en evolución y a los entornos empresariales cambiantes. Al revisar y actualizar periódicamente el SGSI, las organizaciones pueden asegurarse de que sus medidas de seguridad sigan siendo eficaces y estén alineadas con sus objetivos empresariales.

Un SGSI asume la máxima responsabilidad por la seguridad de una organización. Se asegura de que los administradores de redes y sistemas conozcan todos los activos. Es sorprendente la frecuencia con la que los ordenadores, los datos o los dispositivos móviles quedan desprotegidos porque los usuarios se han olvidado de informar de su existencia a las personas responsables de la seguridad.

El SGSI determina quién debe tener acceso a cada tipo de datos y asigna personas para asegurarse de que la tecnología refleje estas políticas. Otras políticas pueden orientar los tipos de equipos permitidos en las instalaciones, qué tipos de análisis y pruebas de seguridad se deben realizar y cómo manejar los ataques cuando se descubren.

Además de contar con un SGSI sólido, las organizaciones también deben estar preparadas para responder con rapidez y eficacia a los incidentes de seguridad cuando estos se produzcan. Esto requiere un *Plan de Respuesta a Incidentes* (PRI) bien definido y un *Equipo de Respuesta a Incidentes de Seguridad de la Información* (ISIRT) capacitado. Un PRI describe los procedimientos y las acciones que debe adoptar una organización en caso de una violación de seguridad u otros incidentes. Proporciona una hoja de ruta clara para detectar, analizar, contener, erradicar y recuperarse de los incidentes, garantizando que la organización pueda minimizar los daños y restablecer las operaciones normales lo más rápido posible.

Un componente clave de un IRP eficaz es el establecimiento de un ISIRT. Este equipo está compuesto por personas con funciones y responsabilidades específicas, incluidos expertos técnicos, asesores legales y especialistas en comunicación, quienes trabajan juntos para gestionar y mitigar el impacto de los incidentes de seguridad. El ISIRT es responsable de coordinar el proceso de respuesta a incidentes, garantizar que todos los pasos se ejecuten de acuerdo con el plan y comunicarse con las partes interesadas tanto dentro como fuera de la organización.

El conocimiento del SGSI y la respuesta a incidentes es fundamental para todos los empleados de una organización, no solo para aquellos que desempeñan funciones de TI o seguridad. Todos tienen un papel que desempeñar en la protección de los activos de información, desde seguir las políticas y los procedimientos de seguridad hasta informar sobre actividades sospechosas. Al fomentar una cultura de concienciación sobre la seguridad, las organizaciones pueden capacitar a sus empleados para que actúen como la primera línea de defensa contra amenazas potenciales. Los programas de formación y concienciación periódicos son esenciales para mantener al personal informado sobre las últimas amenazas, la importancia de seguir los protocolos de seguridad y los pasos que deben seguir en caso de incidente.

Además, la integración del SGSI y la respuesta a incidentes es esencial para crear una postura de seguridad resiliente. Si bien un SGSI proporciona la base para gestionar la seguridad de la información de manera proactiva, un plan de respuesta a incidentes garantiza que la organización esté preparada para reaccionar de manera rápida y eficaz ante cualquier infracción. Este enfoque dual permite a las organizaciones minimizar la probabilidad de incidentes de seguridad y mitigar su impacto cuando ocurren, salvaguardando así la reputación, la situación legal y la continuidad operativa de la organización.

Ejercicios guiados

1. ¿Por qué es importante comprobar el número de versión del software para el que se informa de una vulnerabilidad?

2. ¿Cuál es la diferencia entre el análisis de vulnerabilidades y las pruebas de penetración?

3. ¿Por qué se necesitan abogados en un Equipo de Respuesta a Incidentes de Seguridad de la Información (ISIRT)?

Ejercicios exploratorios

1. Enumere los roles organizacionales de las personas que deberían estar en el equipo que diseña un Sistema de Gestión de Seguridad de la Información (SGSI).

2. Imaginemos que un atacante ha tomado el control de una base de datos central. ¿Qué podría hacer un equipo de respuesta a incidentes de seguridad de la información (ISIRT)?

Resumen

La base de datos de vulnerabilidades y exposiciones comunes (CVE) rastrea las fallas de seguridad en software y dispositivos. Muchas herramientas, tanto de código abierto como patentadas, ayudan a los expertos en seguridad a encontrar fallas. Cada organización debe ejecutar análisis de vulnerabilidades y pruebas de penetración con regularidad.

Debido a que el software es complejo y los sistemas informáticos están interconectados, los atacantes pueden aprovechar pequeñas fallas en los sistemas de una organización para crear problemas importantes. Un equipo del Sistema de Gestión de Seguridad de la Información (SGSI) y un Equipo de Respuesta a Incidentes de Seguridad de la Información (ESIRT) deben reunirse periódicamente para evaluar los riesgos y crear un plan que prevenga y responda a los ataques.

Respuestas a los ejercicios guiados

1. ¿Por qué es importante comprobar el número de versión del software para el que se informa de una vulnerabilidad?

   Es posible que esté ejecutando una versión que no esté afectada por la falla, en cuyo caso está a salvo de ella. Por otro lado, desea evitar una “actualización” automática a una versión de software que contiene una vulnerabilidad peligrosa.

2. ¿Cuál es la diferencia entre el análisis de vulnerabilidades y las pruebas de penetración?

   Un análisis de vulnerabilidades solo informa si hay fallas conocidas en un sistema. Las pruebas de penetración son mucho más poderosas, porque intentan activamente entrar en el sistema.

3. ¿Por qué se necesitan abogados en un equipo de respuesta a incidentes de seguridad de la información (ISIRT)?

   Las regulaciones determinan algunos aspectos de su respuesta y, a menudo, exigen que la organización presente documentos legales sobre un ataque.

Respuestas a los ejercicios exploratorios

1. Enumere los roles organizacionales de las personas que deberían estar en el equipo que diseña un Sistema de Gestión de Seguridad de la Información (SGSI).

   Un administrador de sistemas de cada división principal, para comprender los activos de esa división. Un líder empresarial también sería valioso, tanto para identificar los activos como para determinar quién debería tener acceso a ellos.

   Los gerentes de seguridad deberían estar en el equipo por su experiencia.

   Los administradores responsables de probar la seguridad deben estar en el equipo para que estén al tanto de cada sistema que necesita ser revisado y puedan trabajar con el equipo los tipos de pruebas a ejecutar y su frecuencia.

   Se necesitan abogados para garantizar el cumplimiento, y el departamento de recursos humanos para asegurarse de que todos los responsables de la seguridad conozcan su rol y reciban capacitación.

   Un gerente de nivel C debe estar presente para garantizar que la gerencia proporcione los recursos necesarios. La gerencia también puede priorizar qué sistemas vuelven a funcionar después de un ataque y respaldar a los empleados durante las interrupciones necesarias que pueda causar el plan de recuperación.

   Probablemente haya otras personas que valga la pena agregar al equipo, como los responsables de la seguridad física de la instalación.

2. Imagine que un atacante ha tomado el control de una base de datos central. ¿Qué puede hacer un equipo de respuesta a incidentes de seguridad de la información (ISIRT)?

   Los sistemas que ejecutan la base de datos, los sistemas conectados a ellos y los enrutadores que los sirven probablemente deberían eliminarse de la red. El personal de seguridad debería escanear los sistemas con fines forenses.

   Se debe notificar al personal clave que trabaja con la base de datos, junto con la gerencia. Probablemente se debería evitar emitir un anuncio general hasta que se pueda proporcionar un cronograma para la recuperación, a fin de evitar el pánico y mantener la información fuera de las manos de los atacantes.

   Dependiendo de lo que se sepa sobre el alcance del ataque, el ISIRT debería dejar de usar el correo electrónico y los dispositivos corporativos para comunicarse.

Después de identificar cualquier daño a la base de datos, se debe encontrar una copia de seguridad que se sepa que es correcta y libre de malware y se debe iniciar un nuevo sistema para ejecutar esta base de datos para que la organización pueda comenzar a recuperar sus operaciones.

Se deben completar formularios para informar el incidente con fines de cumplimiento y se debe notificar a los contactos de las fuerzas del orden.

Sin duda, hay otras tareas en el camino hacia la recuperación.

021.3 Comportamiento ético

Referencia al objetivo del LPI

Security Essentials version 1.0, Exam 020, Objective 021.3

Peso

2

Áreas de conocimiento clave

- Comprender las implicaciones a los demás de las acciones adoptadas en materia de seguridad
- Manejar responsablemente la información sobre vulnerabilidades de seguridad
- Manejar la información confidencial de manera responsable
- Conocimiento de las implicaciones personales, financieras, ecológicas y sociales de los errores, y las interrupciones en los servicios de tecnología de la información
- Conocimiento de las implicaciones legales de los análisis de seguridad, evaluaciones y ataques

Lista parcial de archivos, términos y utilidades

- Divulgación responsable y completa
- Programas de recompensas por errores
- Derecho público y privado
- Derecho penal, de privacidad y de autor.
- Responsabilidad, reclamaciones de compensación financiera

Lección 1

Certificado:	Fundamentos de seguridad
Versión:	1.0
Tema:	021 Conceptos de seguridad
Objetivo:	021.3 Comportamiento ético
Lección:	1 de 1

Introducción

El trabajo de seguridad a menudo implica el acceso a información personal confidencial, secretos corporativos y otros datos valiosos. Al definir e implementar políticas para proteger a las personas y los datos, los profesionales deben evaluar las consecuencias de su trabajo en cada paso.

Los profesionales de seguridad también utilizan herramientas que podrían utilizarse para causar daño, como software de pruebas de penetración. Por lo tanto, los profesionales operan en una zona gris y deben ser conscientes de todas las implicaciones económicas, éticas y legales de su trabajo.

Implicaciones de las medidas adoptadas en materia de seguridad

Comprender las implicaciones que tienen para los demás las acciones que se toman en materia de seguridad es una habilidad fundamental en el campo de la ciberseguridad. Cuando los profesionales de la seguridad llevan a cabo sus actividades, sus acciones no solo afectan a los sistemas y datos que están directamente bajo su cuidado, sino que también pueden tener

repercusiones legales, éticas y sociales de gran alcance. Por lo tanto, es fundamental que estos profesionales sean conscientes de cómo sus decisiones y acciones pueden afectar a los demás, incluidos los individuos, las organizaciones y la sociedad en su conjunto.

El concepto de *derecho público y privado* es esencial en este contexto. Las acciones que se toman en materia de ciberseguridad pueden tener diversas implicaciones legales según la jurisdicción y la naturaleza de la actividad. El *derecho público*, que rige la relación entre los individuos y el estado, a menudo incluye regulaciones que impactan las prácticas de ciberseguridad. Por ejemplo, las regulaciones gubernamentales sobre protección de datos y privacidad pueden imponer obligaciones sobre cómo se maneja la información personal, lo que afecta la forma en que los profesionales de la ciberseguridad implementan las medidas de seguridad. Por otro lado, el *derecho privado*, que se ocupa de las relaciones entre individuos y organizaciones, puede entrar en juego en situaciones que involucran contratos, responsabilidades y daños relacionados a violaciones de seguridad. Los profesionales de la ciberseguridad deben comprender estos marcos legales para evitar acciones que podrían violar leyes involuntariamente o resultar en disputas legales.

Además del derecho público y privado, son especialmente relevantes áreas específicas como el *derecho penal*, *derecho de la privacidad* y *derecho de autor*. El *derecho penal* se ocupa de los delitos penales y sus sanciones. En materia de ciberseguridad, ciertas acciones, como el acceso no autorizado a los sistemas o las violaciones de datos, pueden ser penalizadas, lo que conlleva graves consecuencias para los implicados. Por ejemplo, piratear un sistema sin permiso o distribuir malware puede dar lugar a cargos penales en virtud del derecho penal. Comprender estos límites legales es vital para evitar infracciones legales involuntarias y garantizar el cumplimiento de las leyes diseñadas para proteger la infraestructura digital y los datos personales.

La ley de privacidad rige cómo se recopila, utiliza y comparte la información personal. En la era digital, donde los datos son un activo valioso, mantener la privacidad es una preocupación importante. Los profesionales de la ciberseguridad deben conocer bien las regulaciones de privacidad, como el *Reglamento General de Protección de Datos _(GDPR) en la _Unión Europea o la Ley de Privacidad del Consumidor de California* (CCPA) en los Estados Unidos. Estas leyes dictan cómo las organizaciones deben manejar los datos personales, y el incumplimiento puede resultar en fuertes multas y daños a la reputación. Comprender la ley de privacidad ayuda a los profesionales de la ciberseguridad a implementar controles de seguridad que protejan la información personal y respeten los derechos de privacidad de las personas.

La ley de *derechos de autor* es otro ámbito en el que las medidas de ciberseguridad pueden tener consecuencias para los demás. La ley de derechos de autor protege las obras originales de los autores, incluidos el software, la documentación y otros contenidos digitales. Los profesionales de la ciberseguridad deben comprender cómo se aplica la ley de derechos de autor a su trabajo,

especialmente cuando implica copiar o modificar software, utilizar herramientas de terceros o compartir información. La infracción de los derechos de autor puede dar lugar a disputas legales y sanciones económicas, por lo que es fundamental conocer estas normas al realizar evaluaciones de seguridad o desarrollar soluciones de seguridad.

Manejo de información sobre vulnerabilidades de seguridad

El manejo responsable de la información sobre vulnerabilidades de seguridad es un aspecto fundamental de las prácticas de ciberseguridad. Cuando se descubren vulnerabilidades de seguridad, representan debilidades potenciales que podrían ser explotadas por actores maliciosos para obtener acceso no autorizado, robar datos o interrumpir servicios. Por lo tanto, la forma en que se gestiona la información sobre estas vulnerabilidades puede tener implicaciones significativas para la seguridad y la estabilidad de los sistemas digitales y el ecosistema de Internet en general. La gestión responsable de la información sobre vulnerabilidades no es solo una necesidad técnica, sino también una obligación ética para proteger a los usuarios y las organizaciones de daños.

La *divulgación responsable* es una práctica que implica informar sobre vulnerabilidades de seguridad de una manera que les dé tiempo a las partes afectadas poder abordar el problema antes de que la información se haga pública. Este proceso generalmente implica comunicarse directamente con el proveedor o desarrollador del software, o sistema donde existe la vulnerabilidad. El objetivo es garantizar que la vulnerabilidad se pueda reparar o mitigar antes de que los detalles se compartan de manera más amplia, lo que minimiza el riesgo de explotación por parte de actores maliciosos. La divulgación responsable se considera una práctica recomendada en la comunidad de ciberseguridad porque equilibra la necesidad de transparencia y concientización con el imperativo de proteger los sistemas y los datos de daños.

Por el contrario, la *divulgación completa* se refiere a la divulgación inmediata de los detalles de la vulnerabilidad al público sin darles primero a las partes afectadas la oportunidad de solucionar el problema. Los defensores de la divulgación completa argumentan que fomenta una reparación más rápida al crear presión sobre los proveedores para que aborden las vulnerabilidades rápidamente. Sin embargo, también puede exponer los sistemas a un mayor riesgo, ya que los actores maliciosos pueden explotar la vulnerabilidad antes de que haya un parche disponible. La decisión entre la divulgación responsable y la divulgación completa a menudo depende de varios factores, incluida la gravedad de la vulnerabilidad, la probabilidad de explotación y la capacidad de respuesta de las partes afectadas.

Los *programas de recompensas* por detección de errores son iniciativas que alientan a las personas a encontrar y denunciar vulnerabilidades a cambio de recompensas monetarias o reconocimiento. Estos programas suelen ser implementados por organizaciones como incentivo para la piratería ética y la divulgación responsable. Al proporcionar pautas claras sobre cómo

denunciar vulnerabilidades y qué constituye un comportamiento aceptable, los programas de recompensas por detección de errores ayudan a garantizar que la información sobre debilidades de seguridad se maneje de manera adecuada. También fomentan la colaboración entre las organizaciones y la comunidad de ciberseguridad en general, creando un enfoque más proactivo y comprometido con la gestión de vulnerabilidades.

El manejo ético de la información sobre vulnerabilidades de seguridad requiere una consideración cuidadosa de los posibles impactos en todas las partes interesadas. Cuando se descubre una vulnerabilidad, los profesionales de la ciberseguridad deben sopesar los riesgos de la divulgación frente a los beneficios. Deben tener en cuenta el daño potencial que podría resultar de la explotación de una vulnerabilidad, la probabilidad de que los actores maliciosos ya estén al tanto de la vulnerabilidad y la capacidad de las partes afectadas para responder de manera eficaz. En muchos casos, trabajar en estrecha colaboración con la organización afectada para proporcionar información detallada y apoyo en el desarrollo de una solución es la línea de acción más responsable.

En última instancia, el objetivo de gestionar las vulnerabilidades de seguridad de forma responsable es proteger a los usuarios y los sistemas de daños, al tiempo que se promueve una cultura de transparencia y responsabilidad. Al adherirse a prácticas establecidas, como la divulgación responsable y la participación en programas de recompensas por errores, los profesionales de la ciberseguridad pueden contribuir a un entorno digital más seguro. La gestión cuidadosa de la información sobre vulnerabilidades no solo ayuda a prevenir la explotación, sino que también genera confianza y cooperación entre investigadores, desarrolladores y usuarios, lo que fomenta tener un Internet más resistente y seguro para todos.

Manejo de información confidencial

El manejo responsable de la información confidencial es una piedra angular de una práctica eficaz de ciberseguridad. La información confidencial, ya sean datos personales, información comercial confidencial o comunicaciones sensibles, debe protegerse para mantener la confianza, cumplir con los requisitos legales y evitar daños. En la era digital, donde las violaciones de datos y el acceso no autorizado pueden tener graves consecuencias, comprender la importancia de salvaguardar la información confidencial es fundamental para cualquier profesional de la ciberseguridad.

El cumplimiento de la legislación sobre privacidad es un aspecto fundamental del manejo de información confidencial. Las leyes de privacidad, como el GDPR y la CCPA, establecen directrices detalladas sobre cómo se deben recopilar, procesar, almacenar y compartir los datos personales. Estas regulaciones están diseñadas para proteger los derechos de las personas a la privacidad y el control sobre su información personal. Los profesionales de la ciberseguridad deben asegurarse de que sus prácticas se ajusten a estos requisitos legales, implementando medidas de seguridad

sólidas, como cifrado, controles de acceso y auditorías periódicas, para evitar el acceso no autorizado y las violaciones de datos. El incumplimiento de las leyes de privacidad puede dar lugar a multas importantes, acciones legales y daños a la reputación de una organización, por lo que es esencial manejar toda la información confidencial con el máximo cuidado.

Más allá de las leyes de privacidad, el derecho penal también desempeña un papel crucial en la forma en que se gestiona la información confidencial. Las leyes penales cubren una amplia gama de actividades delictivas relacionadas con el acceso no autorizado, el uso indebido de datos y otras acciones que podrían comprometer la confidencialidad de la información. Por ejemplo, piratear un sistema para robar secretos comerciales o acceder a las comunicaciones privadas de alguien sin consentimiento puede dar lugar a cargos penales en virtud del derecho penal. Los profesionales de la ciberseguridad deben estar atentos a comprender los límites establecidos por estas leyes para evitar cualquier acción que pueda interpretarse como ilegal. Esto incluye la implementación de métodos de autenticación robustos, sistemas de monitoreo para intentos de acceso no autorizado y garantizar que todas las actividades estén documentadas y justificadas en virtud de un mandato de seguridad legítimo.

La responsabilidad de manejar información confidencial va más allá de simplemente prevenir el acceso no autorizado; también implica fomentar una cultura de concientización y cumplimiento de la seguridad dentro de una organización. Los empleados de todos los niveles deben recibir capacitación sobre la importancia de proteger los datos confidenciales, las políticas y procedimientos específicos establecidos para garantizar su seguridad. Esto incluye comprender los principios del mínimo privilegio, según los cuales el acceso a la información confidencial está restringido a quienes la necesitan para realizar sus funciones laborales, y estar al tanto de posibles ataques de ingeniería social que podrían comprometer la seguridad de los datos.

Además de las medidas de seguridad técnicas y las políticas organizacionales, los profesionales de la ciberseguridad también deben considerar las implicaciones éticas del manejo de información confidencial. No basta con cumplir con los requisitos legales; también existe la obligación moral de respetar la privacidad de las personas y proteger sus datos del uso indebido. Esta perspectiva ética requiere un enfoque proactivo de la seguridad, anticipando las posibles amenazas y vulnerabilidades y tomando medidas para mitigarlas antes de que puedan ser explotadas.

El manejo responsable de la información confidencial implica crear un entorno seguro en el que los datos estén protegidos tanto de amenazas externas como de usos indebidos internos. Al comprender y cumplir las leyes de privacidad y las leyes penales, implementar medidas de seguridad sólidas y fomentar una cultura de concientización y responsabilidad ética, los profesionales de la ciberseguridad pueden ayudar a garantizar que la información confidencial permanezca segura. Esto no solo protege a la organización y a sus partes interesadas, sino que también defiende el derecho fundamental a la privacidad en un mundo cada vez más digital.

Implicaciones de errores e interrupciones en los servicios de TI

La conciencia de las implicaciones personales, financieras, ecológicas y sociales de los errores y las interrupciones en los servicios de tecnología de la información es un elemento crucial de la ciberseguridad. En nuestro mundo cada vez más digital, la dependencia de la tecnología para todo, desde la comunicación personal hasta la infraestructura crítica, significará que cualquier interrupción puede tener consecuencias de gran alcance. Los profesionales de la ciberseguridad deben comprender estas implicaciones para mitigar eficazmente los riesgos y proteger no solo los sistemas y los datos, sino también a las personas y los entornos que dependen de ellos.

Desde una *perspectiva personal*, los errores y las interrupciones pueden afectar significativamente la vida de las personas. Por ejemplo, una filtración de datos que exponga información personal, como números de seguridad social, datos bancarios o registros médicos, puede provocar robo de identidad, pérdidas financieras y una profunda pérdida de privacidad. Los profesionales de la ciberseguridad deben reconocer el potencial de ese daño personal e implementar medidas sólidas para proteger los datos confidenciales. El conocimiento de estas implicaciones personales garantiza que las medidas de seguridad no solo sean sólidas desde el punto de vista técnico, sino que también sean empáticas con los usuarios a los que pretenden proteger.

Las *implicaciones financieras* de los incidentes de ciberseguridad suelen ser las más evidentes de inmediato. Los errores y las interrupciones pueden generar pérdidas financieras directas para las empresas debido al tiempo de inactividad, la pérdida de productividad y el costo de las medidas de reparación. En casos más graves, puede haber problemas de *responsabilidad* importantes en los que las partes afectadas soliciten una compensación económica por los daños sufridos. Por ejemplo, un ciberataque que interrumpa una plataforma de comercio electrónico puede provocar la pérdida de ventas y la confianza de los clientes, mientras que un ataque a una institución financiera puede provocar un fraude financiero a gran escala. Comprender estas implicaciones financieras ayuda a los profesionales de la ciberseguridad a priorizar la protección de los activos y la infraestructura que, si se ven comprometidos, podrían provocar un daño económico significativo.

Además de las consecuencias personales y financieras, los incidentes de ciberseguridad también tienen *implicaciones ecológicas* que hay que tener en cuenta. En sectores como la energía, el agua y la gestión de residuos, los sistemas de tecnología de la información desempeñan un papel crucial en la gestión y el control de las operaciones. Un ciberataque o una interrupción del sistema en estos sectores podría provocar la liberación de materiales peligrosos, la contaminación del agua o incluso daños ambientales generalizados. Por ejemplo, un ciberataque a una planta de tratamiento de aguas residuales podría provocar la liberación de aguas residuales sin tratar en vías fluviales naturales, lo que dañaría los ecosistemas y la salud pública. Los profesionales de la ciberseguridad deben ser conscientes de estos posibles impactos ecológicos y asegurarse de que los sistemas sean seguros tanto contra ataques intencionales como contra errores accidentales

que podrían causar daños ambientales.

Las *implicaciones sociales* de los incidentes de ciberseguridad son igualmente significativas. En el mundo de hoy, la tecnología sustenta muchos aspectos de la infraestructura social, incluidos la atención médica, la educación, el transporte y los servicios gubernamentales. Una interrupción o un error en estos sistemas puede alterar la vida cotidiana, retrasar servicios críticos e incluso amenazar la seguridad pública. Por ejemplo, un ciberataque a los sistemas informáticos de un hospital podría retrasar la atención médica urgente, mientras que un ataque a las redes de transporte público podría causar un caos generalizado y molestias. Los profesionales de la ciberseguridad deben comprender los impactos sociales de su trabajo, asegurándose de priorizar la protección de los servicios que son esenciales para el bienestar y la seguridad públicos.

Para comprender las amplias implicaciones de los errores y las interrupciones en los servicios de tecnología de la información se requiere una perspectiva multidisciplinaria. Los profesionales de la ciberseguridad no deben centrarse únicamente en las soluciones técnicas, sino que también deben tener en cuenta los contextos legales, éticos y sociales en los que operan estas tecnologías. Al reconocer el potencial de demandas por responsabilidad civil y compensación financiera, así como las consecuencias personales, financieras, ecológicas y sociales de los incidentes de ciberseguridad, pueden adoptar un enfoque más integral para proteger la infraestructura digital de la que depende la sociedad moderna. Esta conciencia garantiza que las iniciativas de ciberseguridad no se limiten a prevenir las infracciones, sino también a salvaguardar el tejido fundamental de nuestro mundo interconectado.

Ejercicios guiados

1. ¿Cuáles son las consideraciones clave que deben tener en cuenta los profesionales de la ciberseguridad al manejar información confidencial y realizar actividades de seguridad?

2. ¿Por qué es importante la gestión responsable de las vulnerabilidades de seguridad y qué prácticas la respaldan?

3. ¿Cómo afectan las implicaciones legales a la realización de análisis, evaluaciones y sondeos de seguridad por parte de profesionales de la ciberseguridad?

Ejercicios exploratorios

1. ¿Cómo actuaría una organización ante un agente de seguridad que buscara información en su base de datos sobre la ex novia de su hermano para que este pudiera localizarla?

2. ¿Por qué un investigador podría sospechar que los atacantes conocen una vulnerabilidad de día cero que el investigador descubrió recientemente?

Resumen

La ética, la ley, los requisitos de seguro y otros factores se combinan para definir las reglas que se deben seguir para manejar las infracciones. Todos los profesionales de seguridad tienen responsabilidades con muchas entidades: la organización para la que trabajan, los empleados de la organización, los clientes, los gobiernos y la sociedad en su conjunto.

Los expertos en seguridad tienen acceso a herramientas poderosas que investigan las redes, así como a datos confidenciales. La ética exige que el profesional utilice estas herramientas y datos solo para cumplir con los objetivos de seguridad. La auditoría puede detectar a las personas que abusan del acceso a los datos.

Las infracciones tienen consecuencias legales, financieras y reputacionales. Los profesionales deben conocer las regulaciones públicas y privadas de sus sectores y cumplirlas en la medida de lo posible.

Por último, las personas que informan sobre fallos de seguridad deben hacerlo de forma responsable, y las personas a cargo de los productos afectados deben solucionar los fallos en un plazo de tiempo razonable.

 | Esta obra está bajo la licencia CC BY-NC-ND 4.0. |

Respuestas a los ejercicios guiados

1. ¿Cuáles son las consideraciones clave que deben tener en cuenta los profesionales de la ciberseguridad al manejar información confidencial y realizar actividades de seguridad?

   Los profesionales de la ciberseguridad deben ser muy conscientes de las implicaciones tanto técnicas como éticas de sus acciones. Esto incluye comprender los marcos legales que rigen las actividades de ciberseguridad, como el derecho público y privado, que dictan cómo se deben manejar los datos personales y corporativos, y las circunstancias en las que se permiten determinadas acciones.

2. ¿Por qué es importante la gestión responsable de las vulnerabilidades de seguridad y qué prácticas la respaldan?

   La gestión responsable de las vulnerabilidades de seguridad es vital porque estas vulnerabilidades representan debilidades potenciales que podrían ser explotadas por actores maliciosos. Dos prácticas clave que respaldan la gestión responsable son la divulgación responsable y la divulgación completa.

3. ¿Cómo afectan las implicaciones legales a la realización de análisis, evaluaciones y sondeos de seguridad por parte de los profesionales de la ciberseguridad?

   Las implicaciones legales influyen significativamente en la forma en que los profesionales de la ciberseguridad realizan análisis, evaluaciones y ataques de seguridad. Actividades como las pruebas de penetración o las evaluaciones de vulnerabilidad pueden caer en una zona gris legal, regida por el derecho público y privado, así como por el derecho penal. Sin un permiso explícito, estas actividades podrían considerarse no autorizadas, lo que podría dar lugar a multas, acciones legales o cargos penales. Los profesionales de la ciberseguridad deben obtener el consentimiento explícito para evitar infracciones no deseadas.

Respuestas a los ejercicios exploratorios

1. ¿Cómo actuaría una organización si un agente de seguridad buscara información en su base de datos sobre la ex novia de su hermano para que este pudiera localizarla?

   Se trata de una infracción interna muy grave que podría derivar en violencia. La organización probablemente deba despedir inmediatamente al agente de seguridad y remitir el caso a la policía local. Dado que se han filtrado datos personales sobre la novia, la organización debe notificárselo.

2. ¿Por qué un investigador podría sospechar que los atacantes conocen una vulnerabilidad de día cero que descubrió recientemente?

   El investigador podría enterarse de que las organizaciones fueron atacadas mediante un tipo particular de consulta SQL o llamada API que se puede asociar con la vulnerabilidad. Es valioso para las organizaciones mantenerse en contacto y compartir información sobre las infracciones para descubrir detalles como estos.

Linux Professional Institute

Tema 022: Cifrado

022.1 Criptografía e infraestructura de clave pública

Referencia al objetivo del LPI

Security Essentials version 1.0, Exam 020, Objective 022.1

Peso

3

Áreas de conocimiento clave

- Comprensión de los conceptos de criptografía simétrica, asimétrica e híbrida
- Comprensión del concepto de Perfect Forward Secrecy (PFS)
- Comprensión de las funciones hash, cifrados y algoritmos de intercambio de claves
- Comprensión de las diferencias entre el cifrado de extremo a extremo y el cifrado de transporte
- Comprensión de los conceptos de Infraestructuras de clave pública (PKI), Autoridades de certificación y CA raíz de confianza
- Comprensión de los conceptos de los certificados X.509
- Comprensión de cómo se solicitan y emiten los certificados X.509
- Conocimiento de la revocación de certificados
- Conocimiento sobre Let’s Encrypt
- Conocimiento de algoritmos criptográficos

Lista parcial de archivos, términos y utilidades

- Infraestructuras de clave pública (PKI)
- Autoridades de certificación
- CA raíz de confianza

- Solicitudes de firma de certificados (CSR) y certificados
- Campos del certificado X.509: Sujeto, Emisor, Validez
- RSA, AES, MD5, SHA-256, intercambio de claves Diffie-Hellman, criptografía de curva elíptica

Linux Professional Institute

Lección 1

Certificado:	Fundamentos de seguridad
Versión:	1.0
Tema:	021 Conceptos de seguridad
Objetivo:	022.1 Criptografía e infraestructura de clave pública
Lección:	1 de 2

Introducción

La criptografía es un aspecto fundamental de la ciberseguridad moderna, ya que proporciona los medios para proteger los datos y las comunicaciones confidenciales del acceso no autorizado. En esencia, la criptografía incluye el *cifrado*, que transforma la información legible en un formato ilegible mediante algoritmos específicos. Este proceso garantiza que solo las personas con la *clave* correcta puedan descifrar el texto y devolverlo a su forma original. El cifrado es crucial para salvaguardar los datos durante la transmisión o el almacenamiento, ya sean mensajes personales, información financiera o secretos comerciales.

Además del cifrado, la criptografía también implica el *hashing*, un proceso que genera un resultado único de tamaño fijo, llamado *hash*, a partir de los datos de entrada. El hash se utiliza para verificar la integridad de los datos, lo que garantiza que la información no haya sido alterada.

Comprender estos conceptos básicos de criptografía es esencial para cualquiera que desee comprender los principios que sustentan la protección de la información digital y la integridad de los datos. Estas técnicas criptográficas se utilizan en aplicaciones cotidianas, desde la protección

de sitios web y transacciones en línea hasta la protección de datos personales y comunicaciones digitales.

Funciones hash, cifrados y algoritmos de intercambio de claves

Para obtener una comprensión más profunda de la criptografía, es esencial explorar los conceptos detrás de las funciones hash, los cifrados y los algoritmos de intercambio de claves, que juntos forman los componentes básicos de la comunicación segura y la protección de datos.

Una *función hash* es un algoritmo criptográfico que convierte datos de entrada de cualquier longitud en una cadena de tamaño fijo, conocida como *hash* o *digest*. La propiedad clave de una función hash es que incluso un cambio leve en los datos de entrada da como resultado un hash radicalmente diferente, lo que la hace muy sensible a las alteraciones. Esta característica garantiza la integridad de los datos, ya que cualquier modificación se puede detectar fácilmente. Las funciones hash también están diseñadas para ser unidireccionales, lo que significa que es computacionalmente inviable realizar ingeniería inversa de los datos originales a partir del hash.

Por ejemplo, los encargados del código fuente de Linux y de varias herramientas GNU proporcionan la firma *Secure Hash Algorithm* (SHA-256) de los archivos distribuidos en sus repositorios de software. Esto permite a los usuarios verificar que los archivos descargados no hayan sido alterados durante la transferencia.

En el contexto de las *firmas digitales*, las funciones hash se utilizan para crear una versión condensada de un mensaje o documento, conocida como *message digest*. Este resumen se cifra luego con la *clave privada* del remitente para crear una firma digital. El destinatario puede verificar la firma descifrándola con la *clave pública* del remitente y comparándola con el hash del documento recibido. Si los dos hashes coinciden, se confirma que el documento no ha sido alterado y se autentica la identidad del remitente. Por ejemplo, este método se utiliza ampliamente en comunicaciones seguras por correo electrónico como *Pretty Good Privacy* (PGP) y en la distribución de software para garantizar la autenticidad e integridad de la información transmitida.

Las funciones hash también son fundamentales para almacenar de forma segura las contraseñas. En lugar de almacenar la contraseña real, los sistemas utilizan una función hash para convertir la contraseña en un valor hash único, que luego se almacena en la base de datos. Cuando un usuario intenta iniciar sesión, el sistema realiza un hash de la contraseña ingresada y la compara con el hash almacenado. Si coinciden, se concede el acceso. Este enfoque garantiza que, incluso si un atacante obtiene acceso a la base de datos de contraseñas, no pueda recuperar fácilmente las contraseñas originales. Para mejorar aún más la seguridad, muchos sistemas utilizan una técnica llamada *salting*, en la que se agrega un valor aleatorio (el *salt*) a la contraseña antes de realizar el hash. Esto garantiza que incluso las contraseñas idénticas resulten en diferentes hashes, lo que

hace que sea mucho más difícil para los atacantes utilizar tablas precalculadas (*rainbow tables*) para descifrar los hashes.

Para mostrar el hash en acción, veamos SHA-256 (parte de la familia SHA-2). Este estándar produce un hash de 256 bits, que se usa ampliamente en tecnologías como la cadena de bloques y las comunicaciones seguras. A continuación, se muestra un ejemplo:

Texto orginal

`HelloWorld`

SHA-256 hash

`a591a6d40bf420404a011733cfb7b190d62c65bf0bcda32b53d83a38ac8f0287`

Por el contrario, las funciones hash más antiguas, como *MD5*, se han ido eliminando debido a importantes fallos de seguridad que permiten los *ataques de colisión*. Un ataque de colisión se produce cuando dos entradas distintas generan el mismo valor hash, lo que compromete la unicidad del hash. Esta vulnerabilidad permite a los atacantes sustituir un archivo o mensaje malicioso por uno legítimo sin ser detectados, ya que ambos producirían hashes idénticos. Estas debilidades comprometen la integridad y la seguridad del proceso de hash, lo que hace que MD5 sea inadecuado para las tareas que utilizan hashes, como la verificación de la integridad de los archivos, las firmas digitales o el almacenamiento seguro de contraseñas en las aplicaciones criptográficas modernas.

Cifrado simétrico y asimétrico

Los *cifrados*, otro elemento fundamental de la criptografía, son algoritmos que se utilizan para cifrar y descifrar. Convierten texto simple en texto cifrado mediante una clave de cifrado, y el proceso se puede revertir utilizando una clave de descifrado. Los cifrados se clasifican en dos categorías principales: *simétricos* y *asimétricos*.

Cifrados simétricos

Los *cifrados simétricos*, como el ampliamente utilizado AES (Advanced Encryption Standard), se basan en la misma clave tanto para el cifrado como para el descifrado. Este enfoque es muy eficiente, especialmente para cifrar grandes volúmenes de datos, porque las operaciones de cifrado y descifrado son relativamente rápidas y computacionalmente económicas.

El algoritmo AES es particularmente popular debido a sus sólidas características de seguridad y rápido rendimiento, lo que lo convierte en una opción estándar para proteger información confidencial en una amplia gama de aplicaciones. Se utiliza comúnmente para proteger datos en redes inalámbricas a través de protocolos como WPA2 (*Wi-Fi Protected Access 2*) y también lo

emplean los gobiernos y las organizaciones para salvaguardar información clasificada.

El intercambio de claves simétricas generalmente implica compartir de forma segura una clave secreta entre las partes antes de que puedan comunicarse. Dado que tanto el emisor como el receptor utilizan la misma clave para cifrar y descifrar, esta clave debe transmitirse de manera que impida su interceptación por partes no autorizadas.

Un método común para el intercambio seguro de claves es utilizar un medio físico confiable o una clave precompartida (PSK), donde la clave se intercambia manualmente entre las partes con anticipación. Sin embargo, en las comunicaciones digitales, un método más seguro y eficiente implica el uso de cifrado asimétrico o protocolos de intercambio de claves como Diffie-Hellman para establecer la clave simétrica.

El método Diffie-Hellman permite que dos partes establezcan una clave secreta compartida a través de un canal inseguro, como Internet, sin transmitir directamente la clave. Esto se logra mediante un proceso matemático que implica números primos grandes, lo que hace que sea computacionalmente imposible para un atacante determinar la clave secreta compartida. Una vez que se establece el secreto compartido, se puede utilizar el cifrado simétrico para proteger la comunicación posterior entre las partes. Este método es fundamental para muchos protocolos criptográficos modernos y es crucial para establecer comunicaciones seguras en entornos donde los métodos tradicionales de intercambio de claves no son viables.

He aquí un ejemplo sencillo de cómo funciona el algoritmo simétrico AES en la práctica:

Cifrado

Input (plaintext): `SensitiveData`

Clave simétrica: `mysecretkey12345`

El algoritmo AES cifra el texto simple utilizando la clave, lo que produce la salida(ciphertext): `4f6a79e0f2e041b4c6d61e64a98f0d5a`

Descifrado

Input (ciphertext): `4f6a79e0f2e041b4c6d61e64a98f0d5a`

Clave simétrica: `mysecretkey12345` (a misma clave utilizada para el cifrado)

El algoritmo AES descifra el texto cifrado utilizando la clave, restaurando el mensaje original como salida (plaintext): `SensitiveData` Sin embargo, el cifrado simétrico se enfrenta a un desafío en cuanto a la distribución de claves. Ambas partes deben obtener de forma segura la misma clave. Sin embargo, transmitir esta clave de forma segura, especialmente en redes inseguras, es una tarea compleja. La criptografía asimétrica surgió para resolver este

problema.

Cifrados asimétricos

A diferencia del cifrado simétrico, que requiere que ambas partes tengan la misma clave, el cifrado asimétrico utiliza dos claves diferentes: una para el cifrado (*clave pública*) y otra para el descifrado (*clave privada*).

Este par de claves es crucial para una comunicación segura, ya que permite que cualquiera pueda cifrar un mensaje utilizando la clave pública, pero solo el propietario de la clave privada puede descifrarlo. Este enfoque resuelve eficazmente el desafío de intercambiar claves de forma segura a través de un canal inseguro, lo que lo convierte en una herramienta esencial para el intercambio seguro de claves y las firmas digitales.

RSA (*Rivest-Shamir-Adleman*) es un ejemplo destacado de cifrado asimétrico, a menudo utilizado en certificados digitales y comunicaciones de correo electrónico seguras para garantizar que los datos puedan intercambiarse de forma segura sin compartir previamente una clave.

RSA se basa en la dificultad computacional de factorizar números grandes, lo que lo hace altamente seguro y adecuado para diversas aplicaciones, incluida la comunicación por correo electrónico segura a través de PGP (Pretty Good Privacy) y la autenticación de usuarios en SSH (*Secure Shell*).

Uno de los desafíos de la criptografía asimétrica es verificar que una clave pública pertenece verdaderamente al destinatario previsto. Sin esta verificación, un atacante podría interceptar y reemplazar una clave pública por la suya, lo que daría lugar a un ataque de intermediario (*man-in-the-middle attack*).

Para evitarlo, existe un sistema de infraestructura de clave pública (PKI) que proporciona un marco para autenticar claves públicas mediante certificados digitales emitidos por autoridades de certificación (CA) de confianza. Esto garantiza que las claves públicas sean legítimas y no hayan sido alteradas, lo que permite comunicaciones seguras y confiables a través de redes.

Además de RSA, otros algoritmos asimétricos como *Elliptic Curve Diffie-Hellman* (ECDH) ofrecen una seguridad similar pero con tamaños de clave más pequeños, lo que los hace más eficientes para dispositivos con capacidad de procesamiento limitada, como los teléfonos inteligentes. ECDH utiliza las matemáticas de las curvas elípticas para facilitar los intercambios de claves seguros, lo que proporciona una seguridad sólida con una sobrecarga computacional reducida en comparación con el RSA tradicional.

Criptografía híbrida

La criptografía híbrida combina eficazmente las ventajas del cifrado simétrico y asimétrico para lograr una comunicación segura y eficiente. De este modo, la criptografía híbrida aprovecha las ventajas de cada una de ellas. Una aplicación típica del cifrado híbrido se encuentra en protocolos muy extendidos como *Secure Sockets Layer/Transport Layer Security* (SSL/TLS), que protegen la transmisión de datos a través de Internet.

La criptografía híbrida es una excelente opción porque combina las ventajas de los métodos de cifrado simétrico y asimétrico para crear un sistema robusto y eficiente de protección de datos. El cifrado simétrico, como AES, es muy eficiente y rápido, lo que lo hace ideal para cifrar grandes volúmenes de datos. Requiere menos potencia computacional que el cifrado asimétrico. Esta eficiencia es esencial para aplicaciones que requieren transferencia de datos a alta velocidad, como la transmisión de video o el intercambio de archivos grandes. Por otro lado, el cifrado asimétrico, como RSA, requiere más recursos computacionales, pero ofrece un método seguro para el intercambio de claves en redes no confiables.

En la criptografía híbrida, se utiliza el cifrado asimétrico para transmitir de forma segura la clave simétrica, que luego se utiliza para el cifrado de datos propiamente dicho. Esta estrategia aprovecha los mejores aspectos de ambos métodos: la sólida seguridad del cifrado asimétrico para el intercambio de claves y el alto rendimiento del cifrado simétrico para la transmisión de datos.

Así es como funciona: durante la fase inicial de la comunicación, el remitente genera una *clave simétrica temporal*, conocida como *clave de sesión*, para cifrar los datos reales. Esta clave de sesión se cifra luego utilizando la clave pública del destinatario y se envía junto con los datos cifrados. Al recibir el mensaje, el destinatario utiliza su clave privada para descifrar la clave de sesión y luego utiliza la clave simétrica descifrada para descifrar los datos. Este proceso garantiza que el cifrado y descifrado de los datos sean eficientes mientras que el intercambio de claves sigue siendo seguro.

Por ejemplo, al visitar un sitio web seguro a través de HTTPS, el navegador del usuario y el servidor realizan un intercambio de claves Diffie-Hellman para establecer una clave simétrica compartida, que luego se utiliza para cifrar todos los datos intercambiados durante la sesión. Esto garantiza que, incluso si un atacante intercepta la comunicación, no podrá leer el contenido cifrado sin la clave simétrica, que no puede obtener únicamente de los datos interceptados.

La criptografía híbrida es una piedra angular de la comunicación segura moderna. Permite la transmisión segura de datos en escenarios que abarcan desde la banca en línea y el comercio electrónico hasta el correo electrónico seguro y las conexiones VPN. Al combinar los mejores aspectos de ambos tipos de cifrado, la criptografía híbrida proporciona un marco sólido para proteger los datos en tránsito, lo que garantiza tanto el rendimiento como la seguridad en

diversos entornos digitales.

Perfect Forward Secrecy (PFS)

Los sistemas de cifrado desempeñan un papel fundamental en la protección de las comunicaciones digitales, ya que cifran los datos para evitar el acceso no autorizado. Sin embargo, incluso los sistemas de cifrado más seguros pueden ser vulnerables si un atacante obtiene acceso a las claves a largo plazo que se utilizan para el cifrado. Aquí es donde entra en juego Perfect Forward Secrecy (PFS).

Un principio básico de la criptografía es garantizar que las comunicaciones sigan siendo seguras, incluso si se ve comprometida una clave de cifrado a largo plazo. PFS garantiza que se genere una *clave de cifrado única* para cada sesión de comunicación y se descarte una vez que finalice la sesión.

Esto significa que incluso si un atacante logra obtener la clave privada utilizada para la comunicación, no podrá descifrar sesiones anteriores, ya que las claves específicas de la sesión ya no están disponibles. Este enfoque evita el descifrado retroactivo de los datos y protege la integridad de las comunicaciones anteriores.

El PFS es especialmente crítico en entornos en los que se intercambia información confidencial con frecuencia, como en aplicaciones web, servicios de correo electrónico y VPN. Al implementar PFS, las organizaciones pueden garantizar que incluso en el caso de una futura violación de la seguridad, los datos históricos permanezcan seguros. Esto mejora la seguridad general al proteger no solo las comunicaciones actuales sino también las pasadas, lo que proporciona una defensa sólida contra posibles amenazas.

Los protocolos criptográficos como Diffie-Hellman (DH) y Elliptic Curve Diffie-Hellman (ECDH) son fundamentales para lograr PFS, ya que generan claves de sesión efímeras que se utilizan solo una vez y luego se descartan. Estos algoritmos garantizan que cada sesión de comunicación tenga una clave única, lo que hace imposible descifrar sesiones anteriores incluso si la clave privada de largo plazo se ve comprometida.

Este principio es parte integral de los protocolos de comunicación segura modernos, como TLS, que dependen de PFS para proteger los datos en tránsito y mantener la confidencialidad de las comunicaciones a través de Internet.

Cifrado de extremo a extremo frente a cifrado de transporte

A medida que exploramos más soluciones criptográficas, es importante diferenciar entre dos enfoques ampliamente utilizados para proteger datos que difieren en su alcance e

implementación.

El cifrado de extremo a extremo (E2EE) garantiza que los datos se encripten en su origen y permanezcan encriptados durante todo el trayecto hasta que llegan al destinatario previsto. Solo el remitente y el receptor tienen las claves necesarias para encriptar y desencriptar los datos, lo que hace que el E2EE sea ideal para las comunicaciones privadas. Los intermediarios, como los proveedores de servicios o los servidores, no tienen acceso a los datos no encriptados. Las aplicaciones de mensajería como WhatsApp utilizan el E2EE para proteger la privacidad del usuario.

La principal fortaleza del E2EE es que ofrece total confidencialidad, ya que ningún tercero puede descifrar los datos. Sin embargo, su implementación es más compleja y requiere una gestión cuidadosa de las claves de cifrado para garantizar que solo el destinatario previsto tenga acceso a los datos.

Por otro lado, el *cifrado de transporte* cifra los datos solo mientras se transmiten entre dos puntos, como por ejemplo entre el dispositivo de un usuario y un servidor. Una vez que los datos llegan al servidor, se descifran y pueden almacenarse o procesarse en su forma original. El protocolo TLS, utilizado en HTTPS, es un ejemplo de cifrado de transporte.

El cifrado de transporte es más sencillo de implementar que el de extremo a extremo y ofrece suficiente protección para proteger los datos en tránsito. Sin embargo, una vez que los datos se almacenan o procesan en el servidor, quedan expuestos y son potencialmente vulnerables a ataques internos o amenazas externas.

Ejercicios guiados

1. Explique la diferencia entre criptografía simétrica y asimétrica.

2. Describa cómo Perfect Forward Secrecy (PFS) mejora la seguridad de los protocolos de comunicación como SSL/TLS.

3. ¿Qué papel desempeñan las funciones hash en la verificación de la integridad de los datos? Proporcione un ejemplo de un escenario en el que esto sea crucial.

 | Esta obra está bajo la licencia CC BY-NC-ND 4.0. |

Ejercicios exploratorios

1. Investigar y explicar cómo se implementa la criptografía híbrida en la navegación web segura a través del protocolo HTTPS.

2. Investigar el concepto de computación cuántica y cómo representa una amenaza para los sistemas criptográficos actuales, especialmente el cifrado asimétrico como RSA.

Resumen

La criptografía desempeña un papel crucial en la protección de la información digital mediante el uso de técnicas de cifrado, como los cifrados simétricos y asimétricos, para proteger los datos y las comunicaciones. El cifrado simétrico, como el AES, es muy eficaz para grandes volúmenes de datos, pero requiere un método seguro para la distribución de claves. El cifrado asimétrico, como el RSA, aborda este desafío mediante el uso de un par de claves públicas y privadas para el intercambio seguro de claves, aunque es más exigente desde el punto de vista computacional. Además, las funciones hash mejoran la seguridad al verificar la integridad de los datos mediante la generación de salidas únicas de tamaño fijo, lo que garantiza que cualquier alteración de los datos se pueda detectar fácilmente.

Esta lección también cubre la criptografía híbrida, que combina las ventajas del cifrado simétrico y asimétrico. Los enfoques híbridos, como los que se utilizan en los protocolos SSL/TLS, aprovechan la velocidad del cifrado simétrico para la transferencia de datos y las capacidades de intercambio seguro de claves del cifrado asimétrico. Además, Perfect Forward Secrecy (PFS) agrega una capa adicional de seguridad al generar claves únicas y efímeras para cada sesión de comunicación, lo que garantiza que las comunicaciones anteriores permanezcan protegidas incluso si se comprometen las claves de cifrado a largo plazo. En conjunto, estas técnicas criptográficas brindan una protección sólida para los datos confidenciales y son fundamentales para proteger las comunicaciones digitales en aplicaciones como la banca en línea, las VPN y la navegación web segura.

 | Esta obra está bajo la licencia CC BY-NC-ND 4.0. |

Respuestas a los ejercicios guiados

1. Explique la diferencia entre criptografía simétrica y asimétrica.

   La criptografía simétrica utiliza la misma clave para el cifrado y el descifrado, lo que la hace eficiente pero plantea un desafío para distribuir la clave de forma segura. La criptografía asimétrica utiliza un par de claves (una pública y una privada), donde la clave pública cifra los datos y solo la clave privada correspondiente puede descifrarlos. Esto elimina la necesidad de compartir una clave secreta, pero es computacionalmente más exigente.

2. Describa cómo Perfect Forward Secrecy (PFS) mejora la seguridad de los protocolos de comunicación como SSL/TLS.

   Perfect Forward Secrecy garantiza que cada sesión de comunicación tenga una clave de cifrado única y efímera que se descarta una vez finalizada la sesión. Esto significa que, incluso si se compromete una clave privada de largo plazo, no se pueden descifrar las comunicaciones anteriores. En protocolos como SSL/TLS, PFS utiliza algoritmos como Diffie-Hellman para generar estas claves temporales, lo que protege la confidencialidad de los datos y proporciona una mayor seguridad para las comunicaciones web.

3. ¿Qué papel desempeñan las funciones hash en la verificación de la integridad de los datos? Proporcione un ejemplo de un escenario en el que esto sea crucial.

   Las funciones hash generan un hash único de tamaño fijo a partir de una entrada, que cambia drásticamente incluso con una alteración menor en la entrada. Esta propiedad las hace ideales para verificar la integridad de los datos, ya que cualquier modificación en los datos da como resultado un hash diferente. Un escenario crucial para el uso de hashes es verificar las descargas de software. Por lo tanto, los mantenedores de herramientas Linux y GNU a menudo proporcionan un hash (como SHA-256) para sus archivos, lo que permite a los usuarios verificar que los archivos no se han alterado durante la transferencia. Si el hash del archivo descargado coincide con el hash proporcionado, se confirma que el archivo está intacto y sin modificaciones.

Respuestas a los ejercicios exploratorios

1. Investigue y explique cómo se implementa la criptografía híbrida en la navegación web segura a través del protocolo HTTPS.

   En HTTPS, la criptografía híbrida se implementa mediante el uso de cifrado asimétrico, generalmente RSA, para intercambiar de forma segura una clave de sesión simétrica entre el cliente y el servidor. Esta clave de sesión se utiliza luego para cifrar toda la transmisión de datos posterior mediante cifrado simétrico, como AES. El uso del cifrado asimétrico garantiza que la clave de sesión se intercambie de forma segura incluso en una red no confiable, mientras que el cifrado simétrico proporciona un cifrado de datos rápido y eficiente para la comunicación real. Esta combinación ofrece seguridad y rendimiento, lo que la hace ideal para la navegación web segura.

2. Investigar el concepto de computación cuántica y cómo representa una amenaza para los sistemas criptográficos actuales, especialmente el cifrado asimétrico como RSA.

   La computación cuántica, con su potencial para realizar cálculos complejos exponencialmente más rápido que las computadoras clásicas, plantea una amenaza significativa para los sistemas criptográficos actuales, particularmente los métodos de cifrado asimétrico como RSA y ECC. En particular, RSA se basa en la dificultad de factorizar números primos grandes, un problema que las computadoras cuánticas podrían resolver de manera eficiente utilizando el algoritmo de Shor. Esto haría posible que las computadoras cuánticas rompan el cifrado RSA, volviéndolo inseguro.

   Para abordar estos desafíos, los investigadores están desarrollando algoritmos resistentes a los cuánticos diseñados para soportar ataques de computadoras cuánticas. Los algoritmos resistentes a los cuánticos son cruciales para garantizar que los métodos de cifrado futuros sigan siendo seguros, incluso a medida que avanza la computación cuántica. Estos algoritmos ayudarán a proteger las comunicaciones confidenciales, las transacciones financieras y los datos gubernamentales contra la amenaza potencial de las capacidades de descifrado cuántico.

Linux Professional Institute

Lección 2

Certificado:	Fundamentos de seguridad
Versión:	1.0
Tema:	021 Conceptos de seguridad
Objetivo:	022.1 Criptografía e infraestructura de clave pública
Lección:	2 de 2

Introducción

Basándose en principios criptográficos, una infraestructura de clave pública (PKI) es fundamental para la seguridad de las comunicaciones y la verificación de identidad en el mundo digital. La PKI establece un marco para el uso de claves públicas y privadas en el cifrado, lo que garantiza que las entidades que participan en la comunicación puedan confiar entre sí.

En el núcleo de la PKI se encuentran los *certificados digitales*, que vinculan una clave pública a una entidad, como una persona u organización, y son administrados por las *autoridades de certificación* (CA). Estos certificados desempeñan un papel crucial en el cifrado de datos y la validación de identidades, lo que hace que la PKI sea indispensable para la navegación web segura, la comunicación por correo electrónico y otras actividades en línea. Las autoridades de certificación raíz de confianza (CA raíz) forman el nivel superior de este modelo de confianza y establecen la cadena de confianza que se extiende a los certificados de usuario final.

Esta relación estructurada garantiza que los usuarios y los sistemas puedan confiar en la autenticidad de los certificados digitales que encuentran. Comprender cómo funcionan las PKI y las CA es esencial para comprender el intercambio seguro de información y el papel de los

certificados digitales en el mantenimiento de la integridad y la seguridad de las comunicaciones en línea.

Infraestructura de clave pública (PKI)

La infraestructura de clave pública (PKI) es fundamental para generar confianza y proteger las comunicaciones digitales. En esencia, la PKI proporciona un marco estructurado para gestionar certificados digitales y pares de claves públicas y privadas, que son esenciales para verificar identidades y proteger los intercambios de datos a través de Internet. Cuando dos entidades, como un usuario y un sitio web, necesitan comunicarse de forma segura, la PKI garantiza que cada parte pueda confiar en la identidad de la otra y en la integridad de los datos que se comparten.

La PKI permite una comunicación segura mediante la gestión de claves públicas y privadas. A entidades como sitios web, servidores o personas se les emite un *certificado digital* que vincula su identidad a una clave pública.

Los certificados digitales funcionan como un “pasaporte” electrónico para una entidad, ya sea una persona, un dispositivo o un servicio. Este certificado es emitido por un tercero de confianza conocido como *Autoridad de Certificación* (CA).

Antes de emitir un certificado, el CA realiza un exhaustivo proceso de verificación para confirmar la legitimidad de la identidad de la entidad. Este proceso evita que actores maliciosos se hagan pasar por otra persona. Una vez emitido el certificado, se puede utilizar para cifrar datos con la clave pública de la entidad. Solo la clave privada correspondiente, que la entidad guarda de forma segura, puede descifrar estos datos, lo que garantiza que la información sensible siga siendo confidencial y accesible solo para el destinatario previsto.

CA y CA raíz de confianza

En el corazón de PKI se encuentran las autoridades de certificación y las autoridades de certificación raíz de confianza, que forman la columna vertebral de la cadena de confianza que sustenta la seguridad de los certificados digitales utilizados en la navegación web, el correo electrónico seguro y otras aplicaciones.

Las CA desempeñan un papel fundamental en la PKI al emitir, validar y gestionar certificados digitales. Una vez emitidos, otros usuarios o sistemas que dependen de la autoridad de la CA pueden confiar en el certificado.

Las CA raíz forman la parte superior de la jerarquía de confianza en PKI. Las CA raíz emiten certificados a las CA intermedias, creando una cadena de confianza que se extiende a los certificados del usuario final. Los certificados raíz están preinstalados en los sistemas operativos y

navegadores web, y proporcionan la base para todos los certificados emitidos en la jerarquía.

Esta cadena de confianza es esencial, ya que crea una relación jerárquica entre las CA raíz, las CA intermedias y las entidades a las que emiten certificados. Cada certificado de la cadena es validado por el que está por encima de el, y finalmente conduce a una CA raíz de confianza. Este modelo jerárquico garantiza que los usuarios y los sistemas puedan confiar en los certificados que encuentran en las interacciones digitales.

Ejemplo de la Cadena de Confianza

A continuación se muestra un ejemplo de una cadena de confianza que involucra una CA raíz, una CA intermedia y certificados de entidad final.

Certificado CA raíz

La CA raíz es la máxima autoridad de la cadena y todos los sistemas confían en ella. Está autofirmada, lo que significa que certifica su propia identidad.

```
- Root CA Name: "GlobalTrust Root CA"
  - Subject: "CN=GlobalTrust Root CA, O=GlobalTrust Inc., C=US"
  - Issuer: "CN=GlobalTrust Root CA, O=GlobalTrust Inc., C=US" (Self-signed)
  - Public Key: Contains the public key of GlobalTrust Root CA
  - Validity Period: 20 years (e.g., 2020-2040)
  - Signature: Self-signed using the Root CA's private key
```

El certificado CA raíz está preinstalado en la mayoría de los sistemas operativos y navegadores, lo que lo establece como una autoridad confiable.

Certificado CA intermedio

La CA intermedia recibe un certificado de la CA raíz. Esta CA actúa como puente entre la CA raíz y las entidades finales, lo que permite una mejor gestión de la seguridad y una mejor distribución de la confianza.

```
- Intermediate CA Name: "GlobalTrust Intermediate CA 1"
  - Subject: "CN=GlobalTrust Intermediate CA 1, O=GlobalTrust Inc., C=US"
  - Issuer: "CN=GlobalTrust Root CA, O=GlobalTrust Inc., C=US" (Signed by Root CA)
  - Public Key: Contains the public key of GlobalTrust Intermediate CA 1
  - Validity Period: 10 years (e.g., 2022-2032)
  - Signature: Signed using the Root CA's private key
```

La CA intermedia emite certificados a entidades finales, como sitios web o aplicaciones, después de validar su identidad.

Certificado de entidad final (sitio web o aplicación)

El certificado de entidad final es emitido por la CA intermedia para un sitio web o una aplicación. Es lo que ve el usuario final cuando se conecta a un sitio web seguro.

```
- End-Entity Name: "example.com"
  - Subject: "CN=example.com, O=Example Inc., C=US"
  - Issuer: "CN=GlobalTrust Intermediate CA 1, O=GlobalTrust Inc., C=US" (Signed by
Intermediate CA)
  - Public Key: Contains the public key of example.com
  - Validity Period: 1 year (e.g., 2023-2024)
  - Signature: Signed using the Intermediate CA's private key
```

En este ejemplo, cada certificado de la cadena es verificado por el que está por encima de el, y en última instancia conduce a una CA raíz confiable, que garantiza la integridad y seguridad de la comunicación digital (Representación visual de la cadena de confianza).

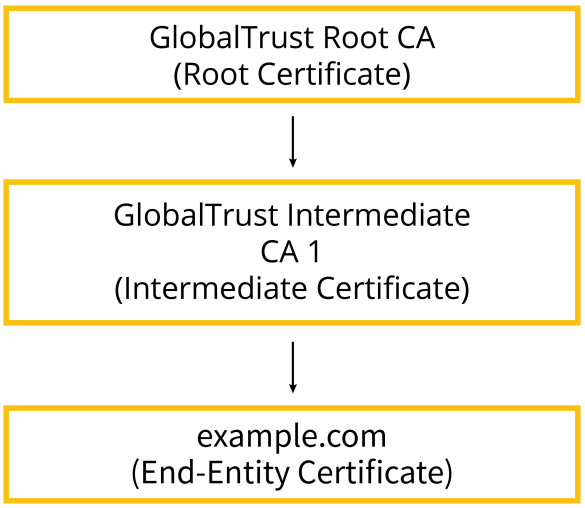

Figure 2. Representación visual de la cadena de confianza

Cuando un usuario visita el sitio web *example.com*, su navegador recibe este certificado. A continuación, el navegador comprueba la validez del certificado siguiendo la cadena de confianza:

1. Comprobación del certificado de entidad final

El navegador verifica que el certificado de *example.com* esté firmado por `GlobalTrust Intermediate CA 1`.

2. Comprobación del certificado de CA intermedia

   El navegador comprueba que el certificado de `GlobalTrust Intermediate CA 1` esté firmado por la `GlobalTrust Root CA`.

3. Comprobación de CA raíz

   El navegador verifica que la CA raíz sea una autoridad confiable preinstalada en su almacén de confianza.

Si todos los certificados de la cadena son válidos y están correctamente firmados, el navegador establece una conexión segura con *example.com* y el usuario puede interactuar de forma segura con el sitio web.

Certificados X.509

Los *certificados X.509* son el formato de certificado digital estándar que se utiliza en la infraestructura de clave pública (PKI) y son esenciales para verificar la identidad de las entidades en comunicaciones seguras. Estos certificados, a los que a menudo se denomina “pasaportes digitales”, establecen una asociación fiable entre la identidad de una entidad y su clave pública mediante la certificación por parte de una autoridad de certificación (CA) de confianza.

Cada certificado X.509 contiene campos que detallan la clave pública de la entidad, el nombre de la CA emisora e información de identidad específica, como el nombre de dominio de la entidad o el nombre de la organización. Este formato estandarizado garantiza que los certificados X.509 proporcionen un método consistente y confiable para autenticar entidades en una amplia gama de aplicaciones digitales.

Comprender la función de los certificados X.509 es esencial porque se utilizan para facilitar conexiones seguras en muchas aplicaciones, incluido HTTPS para la navegación web segura, SSL/TLS para el cifrado de datos y firmas digitales para verificar la autenticidad e integridad de los documentos electrónicos.

El certificado contiene una *firma digital* generada por la CA utilizando su clave privada, que vincula la clave pública a la identidad de la entidad. Esta firma digital puede ser verificada por cualquier persona que utilice la clave pública de la CA, lo que garantiza que el certificado no ha sido alterado y que efectivamente proviene de la CA de confianza.

Estructura de los certificados X.509

Un certificado X.509 contiene varios campos que proporcionan información detallada sobre la entidad y el certificado en sí. Entre ellos se incluyen el *asunto*, que identifica la entidad a la que se emite el certificado, y el *emisor*, que identifica la CA que emitió el certificado. El certificado también contiene la *clave pública* asociada a la entidad, así como la *firma digital* de la CA, que verifica la autenticidad del certificado.

El certificado también incluye un *período de validez*, que indica el período de tiempo durante el cual el certificado se considera válido. Después de este período, el certificado debe renovarse o reemplazarse para mantener la comunicación segura. Además de estos campos, los certificados X.509 pueden incluir *extensiones* que especifican el uso previsto del certificado, como la autenticación del servidor o el cifrado de correo electrónico.

Solicitud y emisión de certificados X.509

El proceso de obtención de un certificado X.509 comienza con la generación de una *Solicitud de Firma de Certificado* (CSR). La CSR es un archivo que contiene la clave pública de la entidad junto con información de identificación, como el nombre de dominio, la organización y la ubicación de la entidad. Esta información ayuda a identificar de forma única a la entidad que solicita el certificado. Luego, la CSR se envía a una CA para su validación.

La CA desempeña un papel fundamental en la verificación de la legitimidad de la información proporcionada en la CSR. Este proceso de validación puede variar en rigor según el tipo de certificado que se solicita. Por ejemplo, un certificado *Domain Validated* (DV) requiere que la CA verifique que la entidad controla el dominio especificado, normalmente a través de un simple proceso de verificación por correo electrónico o DNS. En el caso de certificados más estrictos, como los certificados *Organization Validated* (OV) o *Extended Validation* (EV), la CA realiza comprobaciones adicionales, como la verificación de la existencia legal y la ubicación física de la organización.

Una vez que la CA verifica con éxito los datos de la entidad, emite el certificado X.509 firmándolo digitalmente con la clave privada de la CA. Esta firma digital garantiza la autenticidad e integridad del certificado, de modo que cualquier entidad que reconozca a la CA como autoridad de confianza pueda confiar en él. A continuación, el certificado emitido se envía de vuelta a la entidad solicitante, donde puede instalarse en un servidor o dispositivo.

Una vez instalado, el certificado X.509 se utiliza para establecer comunicaciones seguras al habilitar el cifrado SSL/TLS. Cuando un cliente (por ejemplo, un navegador web) se conecta al servidor, el servidor presenta el certificado. A continuación, el cliente verifica la autenticidad del certificado comprobando la firma de la CA con su lista de certificados raíz de confianza. Si la

verificación es correcta, se establece un canal de comunicación cifrado, lo que garantiza que todos los datos intercambiados entre el cliente y el servidor permanezcan confidenciales y protegidos contra interceptaciones.

Certificados X.509 en SSL/TLS

Los certificados X.509 desempeñan un papel fundamental en el protocolo SSL/TLS, que se utiliza para proteger las comunicaciones entre clientes y servidores a través de Internet. A continuación, se muestra un ejemplo paso a paso de cómo generar una solicitud de firma de certificado (CSR) para un dominio mediante OpenSSL, una biblioteca criptográfica muy utilizada.

Cuando un usuario se conecta a un sitio web seguro, el servidor presenta su certificado X.509 al navegador del usuario como parte del protocolo de enlace SSL/TLS. A continuación, el navegador verifica la autenticidad del certificado comprobando la cadena de confianza con una CA raíz de confianza. Si el certificado es válido y de confianza, el navegador continúa con el protocolo de enlace SSL/TLS y establece una conexión cifrada entre el usuario y el servidor.

Los certificados X.509 también se utilizan en otras aplicaciones, como el cifrado de correo electrónico y las firmas digitales, para verificar la identidad del remitente y garantizar la integridad del mensaje.

Let’s Encrypt

Existen docenas de CA en todo el mundo, la mayoría de las cuales ofrecen servicios de emisión de certificados pagos. Entre las CA más conocidas se encuentra Let’s Encrypt, que ofrece certificados SSL/TLS gratuitos y automatizados y promueve la adopción generalizada de HTTPS.

Let’s Encrypt ha transformado el proceso de obtención y gestión de certificados X.509 al ofrecer certificados SSL/TLS automatizados y gratuitos. Esta iniciativa promueve la adopción generalizada de HTTPS, lo que hace que Internet sea más segura al reducir las barreras para el cifrado.

Antes de Let’s Encrypt, obtener certificados SSL/TLS solía ser un proceso costoso y técnicamente complejo. Let’s Encrypt simplifica este proceso automatizando el proceso de emisión y renovación de certificados, lo que permite a los sitios web proteger sus comunicaciones de forma sencilla y sin coste alguno.

Let’s Encrypt ha desempeñado un papel importante en el aumento de la adopción de HTTPS, mejorando la seguridad y la privacidad en la web. Sin embargo, es importante tener en cuenta que Let’s Encrypt emite certificados validados por dominio (DV), que verifican la propiedad del dominio, pero no brindan el mismo nivel de seguridad que los certificados validados por organización (OV) o los certificados de validación extendida (EV).

Los certificados Let's Encrypt tienen una validez de solo 90 días. Este breve período de validez garantiza que los certificados se actualicen periódicamente, lo que reduce el riesgo de uso indebido en caso de vulneración. Debido a la corta duración de los certificados Let's Encrypt, la renovación automática es crucial para mantener la seguridad.

 | Esta obra está bajo la licencia CC BY-NC-ND 4.0. |

Ejercicios guiados

1. Describa cómo la infraestructura de clave pública (PKI) establece la confianza en las comunicaciones digitales.

2. ¿Cuál es el papel de los certificados X.509 en los protocolos SSL/TLS?

3. Explique el concepto de cadena de confianza en PKI. ¿Por qué es importante la cadena de confianza para establecer comunicaciones seguras y cómo garantiza que se pueda confiar en los certificados digitales?

Ejercicios exploratorios

1. Investigue la función de los certificados de validación extendida (EV) en la seguridad web y explique en qué se diferencian de los certificados validados por dominio (DV) y por organización (OV).

2. Genere una CSR para el dominio *www.example.com* mediante OpenSSL. Proporcione el comando que utilizaría y explique cada parte del comando.

Resumen

En esta lección se analiza la infraestructura de clave pública (PKI), y se profundiza en las funciones de las autoridades de certificación (CA), los certificados X.509 y la cadena de confianza que sustenta las comunicaciones digitales seguras. Además, se analiza la aparición de Let's Encrypt y su impacto en la adopción generalizada de HTTPS.

Respuestas a los ejercicios guiados

1. Describa cómo la infraestructura de clave pública (PKI) establece confianza en las comunicaciones digitales.

   La PKI establece confianza a través de una cadena de confianza que involucra a las autoridades de certificación (CA). Las CA emiten certificados digitales que vinculan la clave pública de una entidad con su identidad verificada. Las CA raíz, en las que confían los navegadores y los sistemas operativos, anclan la cadena de confianza y validan los certificados emitidos por las CA intermedias. Esta estructura jerárquica garantiza comunicaciones seguras al verificar la autenticidad de los certificados digitales.

2. ¿Cuál es la función de los certificados X.509 en los protocolos SSL/TLS?

   Los certificados X.509 se utilizan en los protocolos SSL/TLS para autenticar la identidad de los servidores y establecer una comunicación segura. Durante el protocolo de enlace SSL/TLS, el servidor presenta su certificado X.509 al cliente, que verifica la autenticidad del certificado a través de la cadena de confianza. Si el certificado es válido, se realiza el protocolo de enlace y se establece una conexión cifrada.

3. Explique el concepto de la cadena de confianza en PKI. ¿Por qué es importante la cadena de confianza para establecer comunicaciones seguras y cómo garantiza que se pueda confiar en los certificados digitales?

   La cadena de confianza en PKI se refiere a la relación jerárquica entre la autoridad de certificación raíz (CA raíz), las autoridades de certificación intermedias (CA) y los certificados de entidad final. La CA raíz, en la parte superior de la jerarquía, es inherentemente confiable para los sistemas operativos y los navegadores. Emite certificados a las CA intermedias, que a su vez emiten certificados a entidades finales como sitios web y servidores. Esta estructura garantiza que cada certificado pueda ser validado por el que está por encima de él, y en última instancia se vincula de nuevo con la CA raíz de confianza.

   La cadena de confianza es crucial para las comunicaciones seguras porque permite a los usuarios y sistemas verificar la autenticidad de los certificados digitales. Si la cadena se rompe o un certificado se ve comprometido, el sistema marca la comunicación como insegura, protegiendo a los usuarios de posibles amenazas.

Respuestas a los ejercicios exploratorios

1. Investigue el papel de los certificados de validación extendida (EV) en la seguridad web y explique en qué se diferencian de los certificados validados por dominio (DV) y los certificados validados por organización (OV).

   Los certificados de validación extendida (EV) brindan el mayor nivel de seguridad entre los certificados digitales. A diferencia de los certificados validados por dominio (DV) y los certificados validados por organización (OV), que verifican principalmente el control del dominio y los detalles básicos de la organización, los certificados EV implican procesos de investigación rigurosos. Las autoridades de certificación (CA) deben verificar la existencia legal, la ubicación física y el estado operativo de la entidad solicitante antes de emitir un certificado EV. Si bien los certificados DV son más fáciles de obtener y suficientes para las necesidades básicas de cifrado, los certificados EV se centran en brindar capas adicionales de verificación de identidad, lo que mejora la confianza del usuario durante transacciones confidenciales como la banca en línea o las compras.

2. Genere una CSR para el dominio *www.example.com* mediante OpenSSL. Proporcione el comando que usaría y explique cada parte del comando.

   Para generar una CSR para *www.example.com* mediante OpenSSL, debe utilizar el siguiente comando:

   ```
   openssl req -new -key private.key -out example.csr
   ```

   `req -new` inicia la creación de una nueva CSR.

   `-key private.key` especifica el archivo de clave privada que se utilizará para generar la CSR. Debe haber creado previamente esta clave privada.

   `-out example.csr` indica el nombre del archivo CSR que se creará.

   Después de ejecutar el comando, se le solicitará que ingrese información como el nombre de dominio, la organización y la ubicación, que se incluirán en la CSR. Luego, este archivo se puede enviar a una Autoridad de certificación para solicitar un certificado X.509.

022.2 Cifrado web

Referencia al objetivo del LPI

Security Essentials version 1.0, Exam 020, Objective 022.2

Peso

2

Áreas de conocimiento clave

- Comprensión de las principales diferencias entre los protocolos de texto simple y de transporte
- Comprensión de los conceptos de HTTPS
- Comprensión de los campos importantes en certificados X.509 para el uso de HTTPS
- Comprensión de cómo se asocian los certificados X.509 con un sitio web específico
- Comprensión de las comprobaciones de validez que realizan los navegadores web en los certificados X509
- Determinar si un sitio web está encriptado o no, incluidos los mensajes comunes del navegador

Lista parcial de archivos, términos y utilidades

- HTTPS, TLS, SSL
- Campos del certificado X.509: asunto, validez, subjectAltName

Linux Professional Institute

Lección 1

Certificado:	Fundamentos de seguridad
Versión:	1.0
Tema:	022 Cifrado
Objetivo:	022.2 Cifrado web
Lección:	1 de 1

Introducción

El cifrado web desempeña un papel fundamental en la seguridad de los datos intercambiados entre los sitios web y sus visitantes, garantizando la privacidad y la protección contra el acceso no autorizado. El protocolo principal utilizado para este fin es el *Protocolo de transferencia de hipertexto seguro* (HTTPS). HTTPS no solo cifra los datos, sino que también verifica la identidad de los servidores web mediante certificados digitales. Esta doble funcionalidad permite a los visitantes interactuar con confianza en sitios web legítimos.

Es importante comprender cómo funciona HTTPS, el papel de las autoridades de certificación (CA) en la verificación del servidor y cómo se utilizan las advertencias del navegador para alertar a los visitantes sobre posibles riesgos de seguridad. Al dominar estos conceptos, las personas pueden garantizar interacciones web seguras y protegidas.

En esta lección se exploran los principios básicos de HTTPS, con especial atención a la verificación del servidor, el cifrado y la importancia de los certificados digitales. También se tratarán los mensajes de error más comunes de los navegadores, como los certificados vencidos o no confiables, y se brindará información sobre cómo estas advertencias ayudan a proteger a los visitantes de amenazas como los ataques de intermediarios.

Diferencias principales entre los protocolos de texto simple y el cifrado de transporte

En las comunicaciones web, es fundamental distinguir entre los protocolos de texto simple y los protocolos de cifrado de transporte. Los protocolos de texto simple envían datos en un formato legible, lo que significa que los actores maliciosos pueden interceptar y ver fácilmente la información. HTTP (*protocolo de transferencia de hipertexto*) es un protocolo de texto simple, en el que todos los datos se transmiten sin ningún tipo de cifrado, lo que los deja vulnerables a escuchas y manipulaciones.

HTTP define cómo los clientes web (por ejemplo, los navegadores) se comunican con los servidores web. Como protocolo de capa de aplicación, HTTP es independiente de los protocolos subyacentes de capa de transporte o de capa de sesión (<<fig.22.2.1> >). Sin embargo, en su forma original, HTTP transmite datos como texto simple, encapsulado en segmentos de transporte (como TCP) sin cifrado, lo que lo hace susceptible a la interceptación.

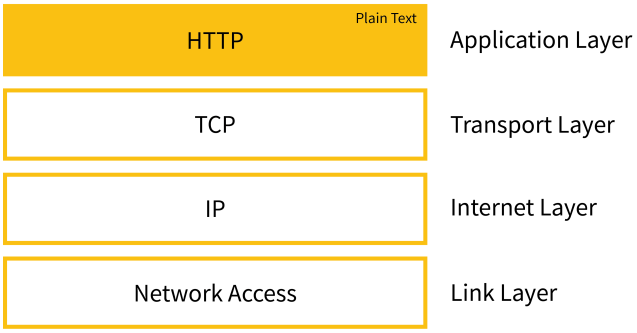

Figure 3. HTTP como parte de la pila de Internet

El *cifrado de transporte* ofrece una solución codificando los datos durante la transmisión y convirtiéndolos en un formato ilegible. Incluso si los datos son interceptados, ya que no se pueden decodificar sin las claves de descifrado correctas. Este enfoque garantiza la confidencialidad e integridad de los datos, evitando el acceso y la modificación no autorizados. El protocolo de seguridad de la capa de transporte (TLS) es el más utilizado para el cifrado de transporte y proporciona la base para la versión segura de HTTP, conocida como HTTPS.

TLS

A medida que Internet evolucionó para gestionar transacciones comerciales y confidenciales, surgió la necesidad de un protocolo que protegiera estos datos. El protocolo *Secure Sockets Layer* (SSL), introducido en la década de 1990, cumplía esa función, pero desde entonces ha sido reemplazado por su sucesor, el protocolo *Transport Layer Security* (TLS). TLS sigue siendo el estándar para proteger la comunicación entre clientes y servidores a través de canales inseguros.

TLS se compone de varios elementos clave, incluidos protocolos de cifrado, certificados digitales para la verificación de la identidad del servidor y dos protocolos TLS principales: el protocolo *TLS handshake* y el protocolo *TLS record*. Estos componentes funcionan juntos para proporcionar una conexión segura entre el cliente y el servidor (<<fig.22.2.2> >).

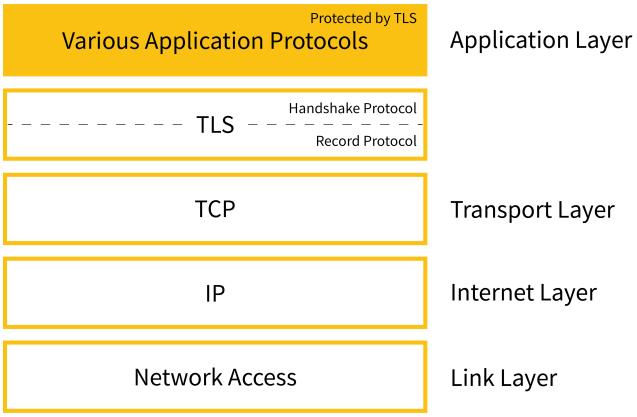

Figure 4. Protocolos TLS como parte de la pila de Internet.

El protocolo de enlace TLS es responsable de la autenticación inicial entre el cliente y el servidor, durante la cual intercambian claves criptográficas y acuerdan un algoritmo de cifrado. El protocolo de enlace TLS garantiza que la conexión sea segura antes de que se intercambien datos de la aplicación. Para que la autenticación sea correcta, el servidor debe presentar un certificado digital firmado por una autoridad de certificación (CA) de confianza, que confirme su identidad.

TLS también incluye el protocolo de registro TLS, que encapsula protocolos de nivel superior y proporciona privacidad e integridad de los datos. La privacidad se logra mediante el cifrado simétrico, mientras que la integridad de los datos se garantiza mediante la incorporación de un *Código de autenticación de mensajes* (MAC) para detectar manipulaciones durante la transmisión. Este enfoque de doble capa garantiza que las comunicaciones sigan siendo privadas y seguras.

Conceptos detrás de HTTPS

HTTPS, o Protocolo seguro de transferencia de hipertexto, es simplemente HTTP que se ejecuta sobre TLS (<<fig.22.2.3> >). El propósito de HTTPS es proteger los datos transmitidos entre el navegador de un visitante y un servidor web; cifrándolos y verificando la identidad del servidor.

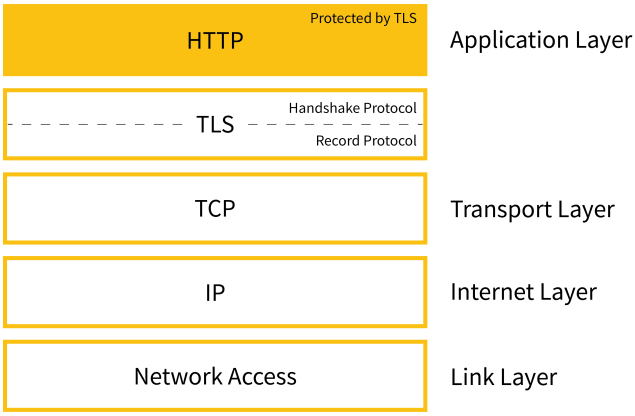

Figure 5. HTTPS como parte de la pila de Internet

Cuando un visitante solicita acceso a un sitio web mediante HTTPS, el servidor presenta un certificado digital X.509 al navegador. Este certificado, emitido por una autoridad de certificación (CA) de confianza, autentica la identidad del servidor. Una vez verificado, el navegador establece una conexión segura mediante cifrado simétrico, a menudo facilitado por métodos de intercambio de claves como Diffie-Hellman o Elliptic Curve Diffie-Hellman (ECDH).

La principal ventaja de HTTPS es que proporciona confidencialidad, integridad y autenticación para las comunicaciones web. Los datos transmitidos a través de HTTPS están protegidos contra la interceptación o la manipulación, y la identidad del servidor se verifica para evitar que los visitantes interactúen sin saberlo con sitios web maliciosos.

Los navegadores modernos ofrecen indicadores visuales, como un icono de candado en la barra de direcciones, para mostrar que un sitio web utiliza HTTPS. Sin embargo, si el certificado está vencido, mal configurado o no es de confianza, los navegadores pueden mostrar mensajes de advertencia para informar a los visitantes sobre posibles riesgos de seguridad. Estas advertencias ayudan a prevenir ataques como las intercepciones de intermediarios, ya que alertan a los visitantes cuando la conexión puede verse comprometida.

El cambio de HTTP a HTTPS ha sido impulsado por la creciente demanda de privacidad y seguridad en la web. La mayoría de los navegadores y motores de búsqueda ahora priorizan los sitios web habilitados para HTTPS, lo que refleja la importancia de la comunicación segura en el panorama digital actual.

El puerto predeterminado para la comunicación HTTPS es TCP 443, mientras que HTTP utiliza TCP 80. La diferencia en los números de puerto permite a los servidores distinguir entre tráfico seguro e inseguro. Cuando un navegador solicita una página web a través de HTTPS, la conexión inicial implica el protocolo de enlace TLS, durante el cual se autentica la identidad del servidor y se intercambian las claves de cifrado.

Una vez que se completa el protocolo de enlace TLS, el navegador envía la primera solicitud HTTP y todos los intercambios de datos posteriores se cifran, lo que garantiza que la información confidencial, como las credenciales de inicio de sesión o los detalles de pago, permanezca segura durante toda la sesión.

Muchos sitios web están configurados para redirigir automáticamente a los visitantes de HTTP a HTTPS para garantizar conexiones seguras. Por ejemplo, si un visitante solicita `http://www.example.com`, el servidor puede redirigirlo a `https://www.example.com`, lo que garantiza que la comunicación esté cifrada y sea segura.

Campos importantes en certificados X.509 para uso de HTTPS

La autenticación del servidor HTTPS se basa en certificados digitales, específicamente certificados X.509, para verificar la identidad del servidor. Cuando un visitante ingresa una URL, el navegador recupera el certificado digital del servidor, que contiene la clave pública y la información de identidad. Este certificado está firmado por una autoridad de certificación (CA) confiable, lo que garantiza que el servidor sea legítimo.

Los certificados X.509, también conocidos como certificados SSL o TLS, vinculan una clave pública a la identidad del servidor, denominada `Sujeto` (o Subject en inglés) del certificado. La firma digital de la CA confirma la validez de esta vinculación, que se almacena en el campo "signatureValue" del certificado.

El estándar X.509 define la estructura de los certificados digitales. La versión 3 (X.509v3) introdujo la posibilidad de agregar extensiones a los certificados, lo que permite incluir información adicional, como nombres alternativos para el servidor.

Cómo se asocian los certificados X.509 con un sitio web específico

La extensión de Nombre alternativo del sujeto o *Subject Alternative Name* (SAN) en inglés, permite que un certificado asocie varias identidades, como nombres DNS o direcciones IP, con el mismo servidor. Esta flexibilidad es crucial para los servidores que operan bajo varios nombres de dominio o direcciones IP, ya que permite que un certificado cubra todas las identidades relevantes.

El proceso de verificación de un certificado implica comparar el `Asunto` o el `Nombre alternativo del sujeto` con la identidad del servidor. Si se encuentra una coincidencia, el certificado se considera válido. También se pueden utilizar comodines, como `*.example.com`, para hacer coincidir varios subdominios, lo que proporciona una mayor flexibilidad en la gestión

de certificados.

Los certificados son emitidos por CA intermedios, que forman parte de una cadena de confianza que conduce a una CA raíz de confianza. El navegador verifica la cadena de confianza haciendo coincidir el campo `Emisor`(Issuer) de cada certificado con el `Asunto` del siguiente certificado de la cadena, y llega finalmente a una CA raíz de confianza.

Los certificados tienen un *período de validez* definido, que indica el tiempo que el certificado es válido. Si un certificado se ve comprometido antes de su vencimiento, la CA puede revocarlo y publicar su número de serie en una *Lista de revocación de certificados* (CRL). Los navegadores utilizan las CRL para verificar el estado del certificado y asegurarse de que no haya sido revocado.

Los servidores HTTPS suelen estar configurados para redirigir automáticamente el tráfico HTTP a HTTPS. Por ejemplo, si un navegador de Internet envía una solicitud a la siguiente URL, especificando HTTP:

```
http://www.example.com/~carol/home.html
```

El servidor HTTPS redirigiría al cliente a una URI que especifique HTTPS, como:

```
https://www.example.com/~carol/home.html
```

Comprobaciones de validez que realizan los navegadores web en los certificados X.509

Cuando un navegador web se conecta a un sitio web mediante HTTPS, realiza varias comprobaciones de validez esenciales en el certificado X.509 del sitio web para garantizar que la conexión sea segura y confiable. Estas comprobaciones verifican la autenticidad del certificado, confirman la identidad del sitio web y protegen a los visitantes de posibles amenazas de seguridad, como ataques de intermediarios (man-in-the-middle). El navegador realiza una serie de pasos para evaluar la validez del certificado.

El formato de los certificados de clave pública está definido por el estándar X.509, que se publicó por primera vez en 1988. El formato de certificado X.509 versión 3 (v3), que se desarrolló en 1996, extiende el formato agregando disposiciones para campos de "Extensiones" adicionales (<<fig.22.2.4> >).

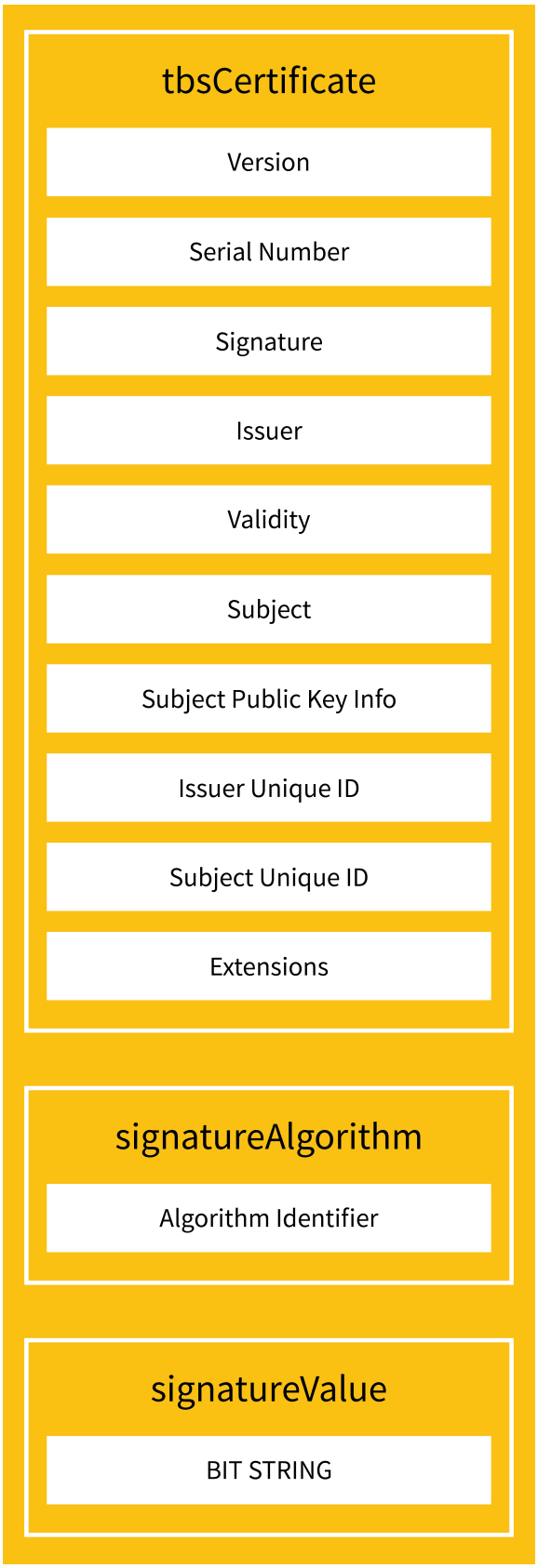

Figure 6. Certificado X.509 v3

El campo `Asunto` del certificado de clave pública identifica el servidor HTTPS asociado con la clave pública almacenada en el campo `Información de clave pública del sujeto` (Subject Public Key Info). El campo `Extensiones` puede transmitir datos como información adicional de identificación del sujeto.

La extensión Subject Alternative Name de la especificación X. 509 permite vincular identidades adicionales al sujeto del certificado. Las opciones de Subject Alternative Name pueden incluir un nombre de host DNS, una dirección IP y más.

El nombre del sujeto puede incluirse en el campo `Sujeto`, en la extensión Nombre alternativo del sujeto o en ambos. Si hay una extensión SAN de tipo `Nombre DNS`, se utiliza como identificador del servidor. De lo contrario, se utiliza como identidad el campo `Nombre común` (Common Name) más específico del campo `Sujeto` del certificado.

Si hay más de una identidad de un tipo específico en el certificado (por ejemplo, más de un campo `Nombre DNS`), se considera aceptable una coincidencia en cualquier campo del conjunto. Los nombres pueden contener el carácter comodín `*` (asterisco) para que coincida con cualquier componente o fragmento de componente de nombre de dominio. Por lo tanto, si el URI es `https://www.example.com/~carol/home.html` y el certificado del servidor contiene `*.basket.com`, `abcd.com` y `*.example.com` como opciones de `Nombre DNS`, hay una coincidencia aceptable: el nombre `*.example.com` coincide con `www.example.com`. Ese nombre comodín no coincidiría con `basket.carol.example.com` porque este último nombre de dominio contiene un componente adicional.

De manera similar, `c*.com` coincide con `carol.com` porque el asterisco puede coincidir con un fragmento de un componente, pero no coincide con `basket.com`.

Si el campo de host del URI incluye una dirección IP, como `https://8.8.8.8`, en lugar de un nombre de host, el cliente verifica el campo `Dirección IP` de la extensión Nombre alternativo del sujeto. El campo `Dirección IP` debe estar presente en el certificado y debe coincidir exactamente con la dirección IP del URI.

A continuación, el navegador comprueba la cadena de confianza del certificado. Verifica que el certificado haya sido emitido y firmado por una autoridad de certificación (CA) de confianza. Esto implica rastrear la cadena del certificado desde el certificado del sitio web, pasando por los certificados intermedios, hasta una CA raíz de confianza, que está incluida en el almacén de certificados raíz preinstalado del navegador. Si algún certificado de esta cadena no es válido o ha sido emitido por una CA no confiable, el navegador marca la conexión como insegura y advierte al visitante.

Otra comprobación crítica es la relativa al período de validez del certificado. Cada certificado X.509 especifica un período de validez, definido por los campos `notBefore` y `notAfter`. El

navegador compara la fecha y la hora actuales con este período de validez. Si el certificado ha expirado o aún no es válido, el navegador alerta al visitante sugiriendo que la conexión puede no ser segura. Este proceso garantiza que los certificados se renueven periódicamente para mantener una comunicación segura.

Además, los navegadores realizan comprobaciones para determinar si la CA ha revocado el certificado. Esto se hace a través de métodos como consultar una lista de revocación de certificados (CRL) o usar el protocolo de estado de certificados en línea (OCSP). Si el certificado ha sido revocado debido a razones como una clave comprometida o una emisión incorrecta, el navegador advierte al visitante que el certificado ya no es confiable y que la conexión puede ser insegura.

El navegador también valida la firma digital del certificado para confirmar que no ha sido alterado desde su emisión. Esto implica verificar la firma criptográfica de la CA emisora. Si la firma no se verifica, sugiere que el certificado puede haber sido alterado o falsificado, lo que lleva al navegador a bloquear la conexión para garantizar la seguridad del visitante.

Por último, los navegadores revisan los campos de extensión o uso de claves dentro del certificado. Estos campos especifican los propósitos previstos del certificado, como la autenticación del servidor o la firma de código. El navegador se asegura de que el certificado se esté utilizando de acuerdo con estos propósitos definidos. Si el certificado se está utilizando para un propósito fuera del ámbito permitido, el navegador emite una advertencia al visitante.

Estas comprobaciones garantizan colectivamente la seguridad de las comunicaciones web al validar la autenticidad, la integridad y el uso adecuado de los certificados X.509. Si alguna de estas comprobaciones falla, el navegador muestra una advertencia de seguridad o un mensaje de error, que aconseja al visitante proceder con precaución o evitar el sitio web por completo. Este riguroso proceso de validación desempeña un papel fundamental en el mantenimiento de la fiabilidad de las interacciones en línea y ayuda a evitar que entidades maliciosas se hagan pasar por sitios web legítimos.

Cómo determinar si un sitio web está encriptado

Determinar si un sitio web está encriptado es un paso crucial para garantizar una comunicación segura entre el navegador del visitante y el servidor del sitio web. Los sitios web encriptados utilizan HTTPS, que proporciona encriptación a través del protocolo TLS, lo que garantiza que los datos intercambiados entre el visitante y el sitio permanezcan privados y protegidos contra escuchas o manipulaciones.

Para determinar si un sitio web está encriptado, los visitantes pueden basarse en algunas señales visuales que ofrecen los navegadores web. El indicador más común es el icono del candado que

aparece en la barra de direcciones del navegador a la izquierda de la URL. Si el sitio web utiliza HTTPS, el candado aparecerá cerrado o bloqueado, lo que indica que la conexión es segura. En algunos navegadores, al hacer clic en el icono del candado se mostrará información más detallada sobre el cifrado del sitio web, como el tipo de cifrado que se utiliza y la autoridad de certificación que lo emite.

Además del candado, la URL en sí es otro indicador de si un sitio está cifrado. Los sitios web seguros comienzan con `https://`, mientras que los sitios no cifrados usan `http://`. La presencia de `https://` indica que la conexión está protegida por cifrado TLS. Algunos navegadores también pueden resaltar esto cambiando el color de la barra de direcciones cuando se establece una conexión segura.

Cuando un sitio web no utiliza cifrado, los navegadores modernos suelen mostrar un mensaje de advertencia para informar a los visitantes de los posibles riesgos. Por ejemplo, cuando un visitante intenta acceder a un sitio mediante HTTP simple (sin cifrado), el navegador puede mostrar un mensaje como “No seguro” en la barra de direcciones. En algunos casos, los navegadores pueden mostrar una advertencia más destacada, alertando al visitante de que la “conexión no es privada” y aconsejándole que evite introducir información confidencial, como contraseñas o números de tarjetas de crédito. Los navegadores como Google Chrome, Mozilla Firefox y Microsoft Edge han sido cada vez más estrictos a la hora de marcar los sitios web no cifrados, especialmente en las páginas en las que se pide a los visitantes que envíen información personal.

Si la configuración HTTPS de un sitio web no es válida o está configurada de forma incorrecta, los navegadores muestran mensajes de advertencia adicionales. Por ejemplo, si un sitio tiene un certificado “vencido”, “mal configurado” o “no confiable”, el navegador puede mostrar un mensaje de advertencia de página completa con una descripción del problema. Mensajes como “Su conexión no es privada” o “Potencial riesgo de seguridad a futuro” indican que el certificado ha vencido, ha sido revocado o está firmado por una CA no confiable. Estas advertencias suelen recomendar que los visitantes regresen a un lugar seguro y no continúen visitando el sitio, aunque a menudo ofrecen una opción para continuar por cuenta y riesgo del visitante.

Para determinar si un sitio web está cifrado, es necesario comprobar los indicadores visuales como el icono del candado y la URL con el símbolo `https://`. Los navegadores también muestran advertencias claras cuando un sitio no es seguro, lo que garantiza que los visitantes estén informados de los posibles riesgos asociados con las conexiones no cifradas o mal configuradas. Comprender estos mensajes del navegador es esencial para navegar de forma segura y evitar la exposición a amenazas de seguridad.

Ejercicios guiados

1. ¿Qué características pertenecen al protocolo HTTP y cuáles al protocolo HTTPS?

Característica	**HTTP**	**HTTPS**
Los datos web se encapsulan directamente mediante un protocolo de capa de transporte, normalmente TCP.		
Los atacantes pueden espiar la comunicación.		
Los datos cifrados se transmiten por Internet.		
El puerto 80 es el puerto TCP predeterminado.		
El puerto 443 es el puerto TCP predeterminado.		
Los datos de texto sin formato se transmiten por Internet.		
Los datos web se encapsulan mediante el protocolo TLS.		
Los datos web pueden ser modificados por un “intermediario”.		
Se verifica la identidad del servidor web.		
El protocolo proporciona integridad de los datos.		

2. ¿En cuál de los siguientes casos se consideraría válida o no válida la identidad de un servidor web?

URI	Contenido del sujeto y nombre alternativo del sujeto del certificado del servidor	Validez de la identidad del servidor
`https://www.example1.com/penguin.html`	`*.penguin.com`, `www.example.com`	
`https://hotlinux.org`	`www.xyz.com`, `hot*.com`	
`https://www.securityessent.com`	`*.security.com`, `security*.org`	
`https://www.certsun.com/`	`ohlala.com`, `cert*.com`	
`https://www.justaparadigm.com/`	`www.carol.com`, `www.justaparadigm.com`	
`https://www.128.263.5.98/`	`www.carol.com`, `128.263.6.98`	
`https://251.32.75.42/`	`www.abc.com`, `251.32.75.42`	

Ejercicios exploratorios

1. ¿Cómo verifica un cliente HTTPS la identidad del emisor del certificado X.509?

2. ¿Qué información contienen los siguientes campos de un certificado X.509v3 de un servidor web?

`Issuer`	
`Validity`	
`Subject`	
`Extensions`	
`SignatureValue`	

3. Describa una situación que puede provocar que un certificado X.509 se vuelva inválido antes de que expire su período de validez.

Resumen

En esta lección se analiza la importancia del cifrado web, centrándose en cómo HTTPS protege la comunicación entre los visitantes y los sitios web mediante el cifrado de datos y la verificación de la identidad del servidor mediante certificados digitales. HTTPS, que se ejecuta sobre el protocolo Transport Layer Security (TLS), desempeña un papel fundamental a la hora de garantizar la confidencialidad e integridad de las comunicaciones web. En la lección se explican las diferencias entre los protocolos de texto sin formato como HTTP, que exponen los datos a escuchas no autorizadas, y el cifrado de transporte, que protege los datos durante la transmisión.

La lección profundiza más en el funcionamiento de HTTPS, haciendo hincapié en el papel de los certificados X.509 en la autenticación de servidores web. Describe el proceso de verificación mediante el cual los navegadores web validan la confiabilidad del certificado, incluidas las comprobaciones de coincidencia de nombres de dominio, cadena de confianza de certificados, período de validez, estado de revocación y uso adecuado en función de las extensiones de clave. Además, los visitantes aprenden cómo los navegadores advierten sobre posibles riesgos de seguridad cuando los certificados están vencidos, no son confiables o están mal configurados. Estas advertencias desempeñan un papel importante en la protección de los visitantes contra ataques de intermediarios y otras amenazas.

 | Esta obra está bajo la licencia CC BY-NC-ND 4.0. |

Respuestas a los ejercicios guiados

1. ¿Qué características pertenecen al protocolo HTTP y cuáles al protocolo HTTPS?

Característica	HTTP	HTTPS
Los datos web se encapsulan directamente mediante un protocolo de capa de transporte, normalmente TCP.	X	
Los atacantes pueden espiar la comunicación.	X	
Los datos cifrados se transmiten por Internet.		X
El puerto 80 es el puerto TCP predeterminado.	X	
El puerto 443 es el puerto TCP predeterminado.		X
Los datos de texto sin formato se transmiten por Internet.	X	
Los datos web se encapsulan mediante el protocolo TLS.		X
Los datos web pueden ser modificados por un "intermediario".	X	
Se verifica la identidad del servidor web.		X
El protocolo proporciona integridad de los datos.		X

2. ¿En cuál de los siguientes casos se consideraría válida o no válida la identidad de un servidor web?

URI	Contenido del sujeto y nombre alternativo del sujeto del certificado del servidor	Validez de la identidad del servidor
`https://www.example1.com/penguin.html`	`*.penguin.com`, `www.example.com`	Not valid
`https://hotlinux.org`	`www.xyz.com`, `hot*.com`	Not valid
`https://www.securityessent.com`	`*.security.com`, `security*.org`	Not valid
`https://www.certsun.com/`	`ohlala.com`, `cert*.com`	Valid
`https:///www.justaparadigm.com/`	`www.carol.com`, `www.justaparadigm.com`	Valid
`https://www.128.263.5.98/`	`www.carol.com`, `128.263.6.98`	Not valid
`https://251.32.75.42/`	`www.abc.com`, `251.32.75.42`	Valid

Respuestas a los ejercicios exploratorios

1. ¿Cómo verifica un cliente HTTPS la identidad del emisor del certificado X.509?

   Los clientes HTTPS procesan los campos que enumeran el nombre distinguido del emisor y el nombre distinguido del sujeto para realizar el encadenamiento de nombres para la validación de la ruta de certificación. El encadenamiento de nombres se realiza haciendo coincidir el nombre distinguido del emisor en un certificado con el nombre del sujeto en otro certificado. Por último, el nombre distinguido del emisor en el certificado raíz debe tener una coincidencia en el almacén raíz del cliente.

2. ¿Qué información contienen los siguientes campos de un certificado X.509v3 de un servidor web?

`Issuer`	Nombre común de la CA y otra información sobre la CA
`Validity`	Fechas que especifican la vida útil válida del certificado
`Subject`	Nombre común del sujeto y otra información sobre el sujeto
`Extensions`	Nombre DNS del sujeto, dirección IP y otros datos extendidos
`SignatureValue`	Firma de la CA

3. Describa una situación que puede provocar que un certificado X.509 se vuelva inválido antes de que expire su período de validez.

   Un compromiso o sospecha de compromiso de la clave privada correspondiente.

022.3 Cifrado de correo electrónico

Referencia al objetivo del LPI

Security Essentials version 1.0, Exam 020, Objective 022.3

Peso

2

Áreas de conocimiento clave

- Comprensión del cifrado de correo electrónico y las firmas de correo
- Comprensión de OpenPGP
- Comprensión de S/MIME
- Comprensión del rol de las claves OpenPGP
- Comprensión del rol de los certificados para S/MIME
- Comprensión de cómo las claves PGP y los certificados S/MIME se asocian con una dirección de correo electrónico
- Uso de Mozilla Thunderbird para enviar y recibir correo electrónicos cifrados mediante OpenPGP y S/MIME

Lista parcial de archivos, términos y utilidades

- GnuPGP, claves GPG, servidores de claves
- Certificados S/MIME y S/MIME

Lección 1

Certificado:	Fundamentos de seguridad
Versión:	1.0
Tema:	022 Cifrado
Objetivo:	022.3 Cifrado de correo electrónico
Lección:	1 de 1

Introducción

En el panorama actual, el correo electrónico sigue siendo una herramienta de comunicación fundamental, pero también es vulnerable a la interceptación y al acceso no autorizado. Para proteger la información confidencial intercambiada por correo electrónico, las tecnologías de cifrado como *OpenPGP* y *S/MIME* brindan confidencialidad, integridad y autenticidad. Comprender estos dos estándares de cifrado es esencial para cualquier persona involucrada en comunicaciones seguras.

Open Pretty Good Privacy (OpenPGP) y Secure/Multipurpose Internet Mail Extensions (S/MIME) son dos protocolos ampliamente adoptados para cifrar y firmar digitalmente mensajes de correo electrónico. OpenPGP se basa en un modelo de confianza descentralizado, que permite a los usuarios generar y gestionar sus propias claves de cifrado, mientras que S/MIME funciona con un modelo de confianza centralizado, que utiliza certificados digitales emitidos por autoridades de certificación (CA) de confianza. Ambos estándares ofrecen cifrado para proteger el contenido de un mensaje de correo electrónico y evitar que lo lean destinatarios no deseados, así como firmas digitales para verificar la identidad del remitente y garantizar que el mensaje no haya sido alterado.

Exploraremos Mozilla Thunderbird, un cliente de correo electrónico multiplataforma conocido por admitir e integrar OpenPGP y S/MIME, lo que permite el cifrado de extremo a extremo. La configuración generalmente implica configurar OpenPGP y S/MIME, generar pares de claves públicas y privadas, importar certificados X.509 y administrar el envío y la recepción seguros de mensajes cifrados.

Cifrado de correo electrónico y firmas digitales

Para cifrar el correo electrónico, los sistemas utilizan criptografía de clave pública o criptografía asimétrica. A diferencia de la criptografía simétrica, que se basa en la misma clave para cifrar y descifrar, la criptografía de clave pública proporciona a cada usuario un par de claves que consta de una clave pública y una clave privada.

Como lo indica el nombre, la clave pública se comparte abiertamente y es accesible para cualquier persona que desee participar en una comunicación por correo electrónico cifrada. Sin embargo, la clave privada permanece confidencial y el usuario nunca la comparte ni la transmite.

El proceso de cifrado funciona de la siguiente manera: el remitente utiliza la clave pública del destinatario para cifrar el mensaje de texto sin formato, lo que da como resultado un *texto cifrado* que no se puede leer sin la clave privada correspondiente. Solo el destinatario, que la posee, puede descifrar el texto y acceder al formato original.

La criptografía de clave pública se emplea en una variedad de aplicaciones, como la navegación web segura a través de HTTPS (Protocolo seguro de transferencia de hipertexto), el correo electrónico seguro con S/MIME o PGP y las firmas digitales, que garantizan la autenticidad e integridad de los documentos digitales.

Dos algoritmos ampliamente utilizados en criptografía de clave pública son RSA y DSA. RSA recibe su nombre de sus creadores (Ron Rivest, Adi Shamir y Leonard Adleman), mientras que DSA significa *Digital Signature Algorithm*. Un desarrollo más reciente es la criptografía de curva elíptica, que incluye el *Elliptic Curve Digital Signature Algorithm* (ECDSA).

OpenPGP

Como puede ver en el sitio web de OpenPGP, esta tecnología se derivó originalmente del software PGP creado por Phil Zimmermann. Hoy en día, OpenPGP es el estándar de cifrado de correo electrónico más utilizado. Para mostrar cómo funciona, utilizaremos *GNU Privacy Guard* (GnuPG o GPG para abreviar), una implementación gratuita de OpenPGP para cifrar y firmar digitalmente sus datos y comunicaciones. GPG se publica bajo los términos de la Licencia Pública General de GNU.

GPG puede utilizar criptografía de clave simétrica y de clave asimétrica. De todos los algoritmos admitidos, AES es quizás el más conocido para el cifrado simétrico, mientras que RSA y ECDSA son los que utiliza GPG con más frecuencia para el cifrado asimétrico.

Comencemos abriendo una terminal y cifrando simétricamente un archivo que contiene un mensaje en texto plano:

```
$ echo "Hello world" > message_file.txt
$ gpg --symmetric message_file.txt
```

Se le solicitará una contraseña dos veces y se generará el archivo cifrado `message_file.txt.gpg`. Si intenta leer el texto ahora, obtendrá un texto sin sentido como el siguiente:

```
$ cat message_file.txt.gpg
???_?#?[??Qw?h:0???V?)??z/LBzL>?□Q$?□?#U.srm[?.3?O??V?p!\@!J?w?|??90?,R??
```

Para desencriptarlo, simplemente use la opción `--decrypt` y proporcione la contraseña cuando se le solicite:

```
$ gpg --decrypt message_file.txt.gpg
gpg: AES256.CFB encrypted data
gpg: encrypted with 1 passphrase
Hello world
```

También puedes firmar y cifrar el mensaje con un solo comando (siempre que hayas creado una clave privada previamente):

```
$ gpg --sign --symmetric message_file.txt
```

Puedes subir un nivel y usar GPG de una manera más sofisticada cifrando asimétricamente un mensaje para un destinatario en particular. Para eso, tendrás que crear un par de claves. Aunque aprenderemos a generar fácilmente un par de claves usando Mozilla Thunderbird más adelante en la lección, es interesante notar que también puedes usar `gpg` en la línea de comandos para hacerlo:

```
$ gpg --full-generate-key
gpg (GnuPG) 2.2.27; Copyright (C) 2021 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
```

```
There is NO WARRANTY, to the extent permitted by law.

gpg: directory '/home/carol/.gnupg' created
gpg: keybox '/home/carol/.gnupg/pubring.kbx' created
Please select what kind of key you want:
   (1) RSA and RSA (default)
   (2) DSA and Elgamal
   (3) DSA (sign only)
   (4) RSA (sign only)
  (14) Existing key from card
Your selection?
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (3072)
Requested keysize is 3072 bits
Please specify how long the key should be valid.
         0 = key does not expire
      <n>  = key expires in n days
      <n>w = key expires in n weeks
      <n>m = key expires in n months
      <n>y = key expires in n years
Key is valid for? (0)
Key does not expire at all
Is this correct? (y/N) y

You need a user ID to identify your key; the software constructs the user ID
from the Real Name, Comment and Email Address in this form:
    "Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"

Real name: Carol Doe
E-mail address: carol.doe@example.com
Comment: Generating keys is fun!
You selected this USER-ID:
    "Carol Doe (Generating keys is fun!) <carol.doe@example.com>"

Change (N)ame, (C)omment, (E)-mail or (O)kay/(Q)uit? O

We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilise the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
gpg: /home/carol/.gnupg/trustdb.gpg: trustdb created
gpg: key 683714AD69979321 marked as ultimately trusted
gpg: directory '/home/carol/.gnupg/openpgp-revocs.d' created
gpg: revocation certificate stored as '/home/carol/.gnupg/openpgp-
```

```
revocs.d/FFA136F2E1B69CAA35DE55CE683714AD69979321.rev'
public and secret key created and signed.

pub   rsa3072 2023-05-03 [SC]
      FFA136F2E1B69CAA35DE55CE683714AD69979321
uid                      Carol Doe (Generating keys is fun!) <carol.doe@example.com>
sub   rsa3072 2023-05-03 [E]
```

¡Listo! Tu par de claves ya está listo. Otras opciones más rápidas para crear un par de claves son `--quick-generate-key` y `--generate-key`.

NOTE Quizás la opción `gpg` más importante es `--help`, porque le brinda todas las opciones y la información necesaria.

El cifrado asimétrico implica cifrar el mensaje utilizando su clave privada junto con la clave pública del destinatario, de modo que el mensaje pueda descifrarse únicamente con la clave privada del destinatario. Para ello, necesitará la clave pública del destinatario. Puede pedir que la compartan con usted o, más a menudo, buscarla en servidores de clave pública. Este tema nos lleva directamente a la siguiente sección.

El rol de los servidores de claves OpenPGP

La función principal de los servidores de claves OpenPGP es almacenar claves públicas y ponerlas a disposición de cualquier persona que desee comunicarse de forma segura con el propietario de la clave. Cuando un usuario desea enviar un mensaje de correo electrónico cifrado o verificar una firma digital, puede buscar la clave pública del destinatario en un servidor de claves, lo que garantiza que el proceso de cifrado pueda continuar sin necesidad de un intercambio manual de claves.

Los servidores de claves almacenan y sirven claves públicas criptográficas que se utilizan para intercambiar claves públicas. El procedimiento estándar es el siguiente (supondremos que hay dos usuarios llamados Carol y John):

1. Carol crea un par de claves (pública y privada) utilizando GPG.
2. Carol conserva la clave privada.
3. Carol exporta (carga) su clave pública a un servidor de claves públicas para que John pueda usarla.
4. John importa (descarga) la clave pública de Carol en su llavero.

Ahora John puede firmar asimétricamente un mensaje que sólo puede descifrarse con la clave privada de Carol.

NOTE La clave pública normalmente se incluye en un archivo de certificado criptográfico que contiene no solo la clave sino también información sobre su propietario.

S/MIME

Compatible con la gran mayoría de los clientes de correo electrónico (como Apple Mail, Microsoft Outlook y Mozilla Thunderbird), S/MIME es un protocolo estándar para proteger y autenticar mensajes de correo electrónico mediante criptografía de clave pública: cifrado y firmas digitales. De este modo, S/MIME garantiza la confidencialidad, integridad y autenticidad del correo electrónico.

Los siguientes términos a menudo se confunden, por lo que es importante tener una idea clara de lo que significa cada uno:

Confidencialidad

El mensaje debe ser descifrado y leído únicamente por el destinatario previsto. Esto se logra mediante el cifrado.

Integridad

El mensaje debe llegar a su destino exactamente como fue escrito (sin modificaciones). Esto se logra mediante firmas digitales.

Autenticidad

Se deben verificar las identidades del remitente y del destinatario. Esto se logra firmando y verificando digitalmente los mensajes de correo electrónico utilizando la clave privada del remitente y la clave pública del destinatario, respectivamente.

S/MIME proporciona seguridad de extremo a extremo para la comunicación por correo electrónico. El remitente cifra el mensaje de correo electrónico utilizando la clave pública del destinatario para que pueda descifrarse únicamente utilizando la clave privada del destinatario. Esto es extremadamente importante, ya que garantiza que el mensaje pueda ser leído únicamente por el destinatario previsto y que no sea alterado durante el envío por terceros no autorizados.

Además, S/MIME proporciona firmas digitales, que permiten a los remitentes firmar digitalmente sus mensajes utilizando sus claves privadas y a los destinatarios verificar que el mensaje proviene del supuesto remitente. Esto se hace de la siguiente manera: el remitente crea una firma digital cifrando un hash del mensaje utilizando su clave privada. El destinatario puede verificar la firma descifrando el hash con la clave pública del remitente y comparándolo con el hash que ha calculado él mismo.

NOTE Una función hash toma algunos datos de entrada o un mensaje y les aplica un

> conjunto de algoritmos para generar una salida única de longitud fija: una secuencia de caracteres o bits conocida como *resumen del mensaje*, *código hash* o simplemente *hash*. El hash resultante se utiliza normalmente para validar la integridad de los datos de entrada. Una de las ventajas del hash es que permite comparar los datos de forma rápida y eficiente sin tener que comparar todo el contenido de los datos.

El rol de los certificados para S/MIME

Para utilizar S/MIME, tanto el remitente como el destinatario deben tener un cliente de correo electrónico compatible con S/MIME y un certificado digital emitido por una autoridad de certificación de confianza. Además de la clave pública del propietario, el certificado contiene otra información de identificación importante y se utiliza para demostrar la identidad del propietario, así como la autenticidad de la clave pública.

Algunas CA ofrecen certificados digitales S/MIME gratuitos por un período de un año. También puedes generar tu propio certificado autofirmado con OpenSSL.

Cómo se asocian las claves PGP y los certificados S/MIME con una dirección de correo electrónico

Como ya se ha mencionado, tanto PGP como S/MIME se utilizan para el cifrado de correo electrónico y las firmas digitales. Sin embargo, difieren en la forma en que asocian las claves o los certificados con una dirección de correo electrónico.

PGP requiere que el usuario genere un par de claves PGP y asocie la clave pública con su dirección de correo electrónico en el cliente de correo electrónico. Esto normalmente se hace compartiendo la clave pública en un servidor de claves. Luego, otros usuarios pueden buscar la clave pública asociada con la dirección de correo electrónico del usuario en el servidor de claves y usarla para enviarle mensajes cifrados.

Por otro lado, S/MIME utiliza certificados para asociar la clave pública a una dirección de correo electrónico. El certificado digital es emitido por una CA de confianza, que verifica la identidad del usuario y la autenticidad de la clave pública. El usuario debe tener el certificado digital instalado en su cliente de correo electrónico. El certificado contiene la clave pública del usuario, así como otros datos de identificación, incluida la dirección de correo electrónico. Otros usuarios pueden verificar la firma digital del usuario y cifrar los mensajes que le envían utilizando la clave pública asociada a su dirección de correo electrónico.

Cómo usar Mozilla Thunderbird para enviar y recibir correo electrónico cifrado

Mozilla Thunderbird es un cliente de correo electrónico multiplataforma, gratuito y de código abierto que realiza el cifrado de correo electrónico de extremo a extremo e integra tanto OpenPGP como S/MIME, así como una funcionalidad de administración de claves incorporada. Las siguientes subsecciones demuestran cómo configurar Thunderbird para cifrar y descifrar correo electrónico de forma asimétrica.

Las instrucciones asumen que Thunderbird está instalado en su sistema y que ya hay una cuenta de correo electrónico configurada.

Configuración de OpenPGP y generación de un par de claves

Una vez creada la cuenta, vaya a la pestaña “Bandeja de entrada” y haga clic en el icono de la rueda dentada (“Configuración”) en la esquina inferior izquierda. Luego, desde la pestaña “Configuración”, haga clic en “Configuración de la cuenta” y, por último, en “Cifrado de extremo a extremo”. Encontrará la pantalla que se muestra en Pantalla de cifrado de extremo a extremo.

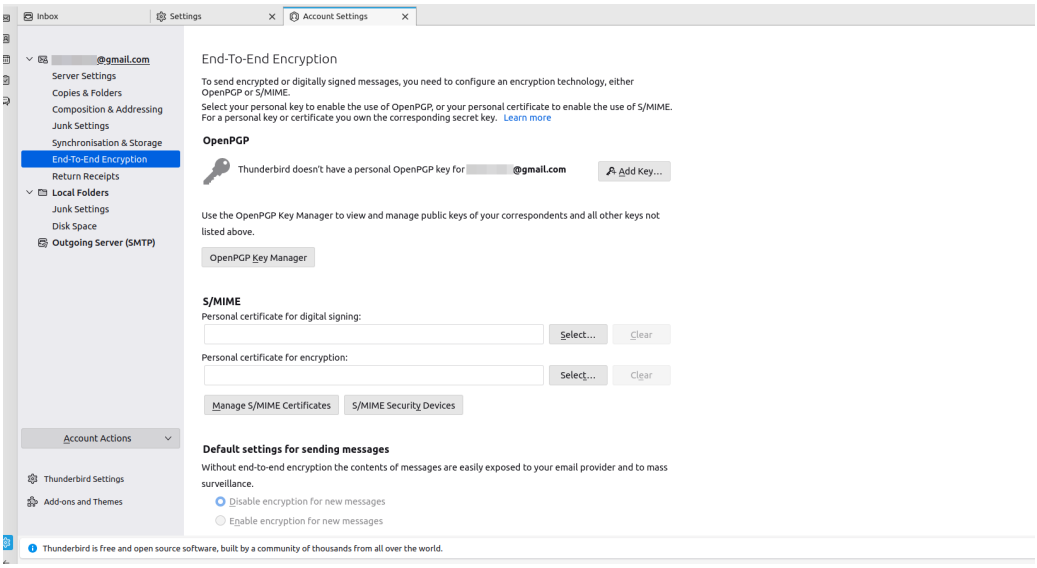

Figure 7. Pantalla de cifrado de extremo a extremo

Actualmente, no hay claves disponibles para su cuenta (ni tampoco certificados personales S/MIME), por lo que debe hacer clic en el botón “Agregar clave...”. Ahora puede elegir entre importar una clave OpenPGP existente para su dirección de correo electrónico o crear una nueva clave OpenPGP desde cero. Optaremos por la segunda opción (Creación de un nuevo par de claves PGP).

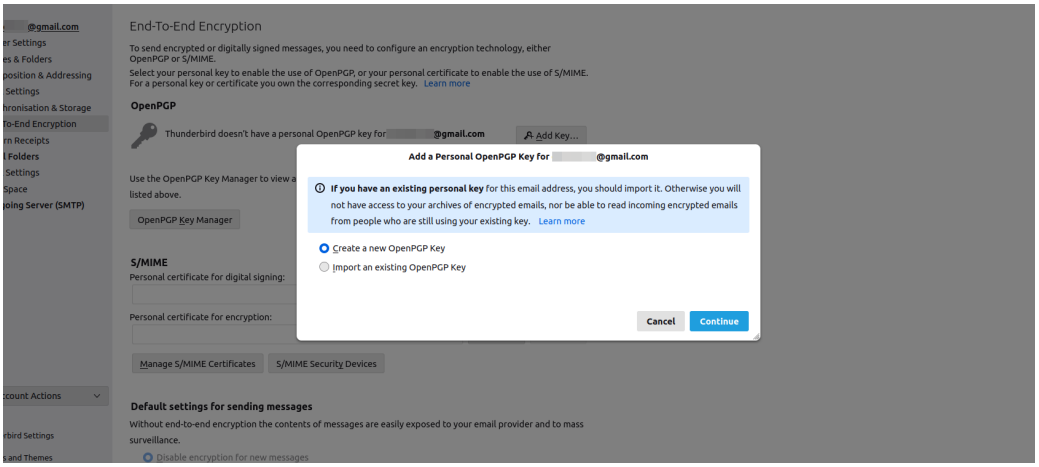

Figure 8. Creación de un nuevo par de claves PGP

A continuación debes realizar algunas configuraciones, como seleccionar el tiempo de expiración, el tipo y el tamaño de la clave (Configuración de su par de claves).

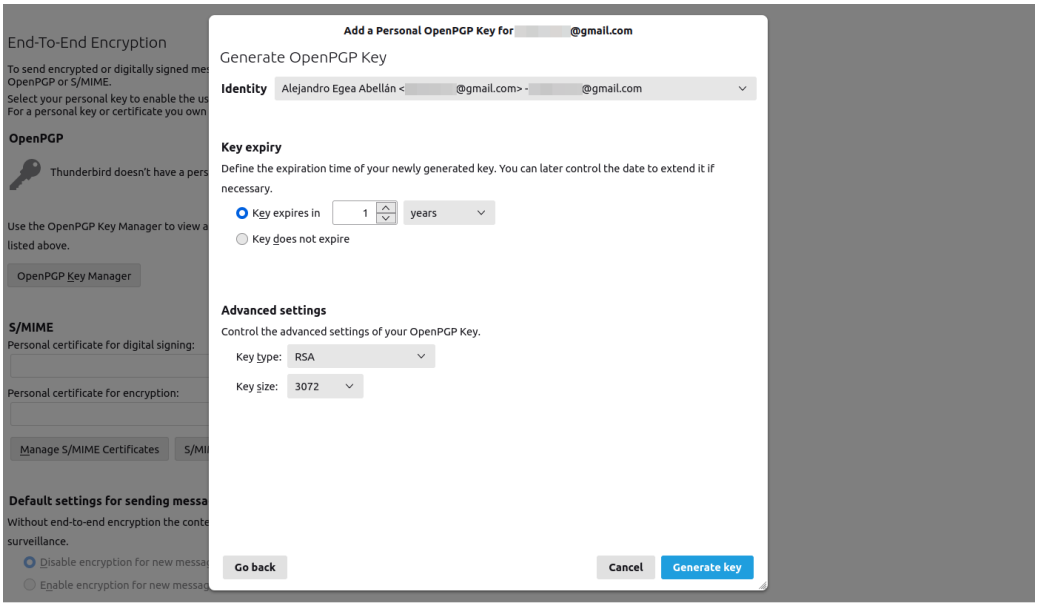

Figure 9. Configuración de su par de claves

Por último, se le informa sobre el tiempo necesario para la generación de la clave y se le solicita que confirme la operación (Confirmando la creación del par de claves).

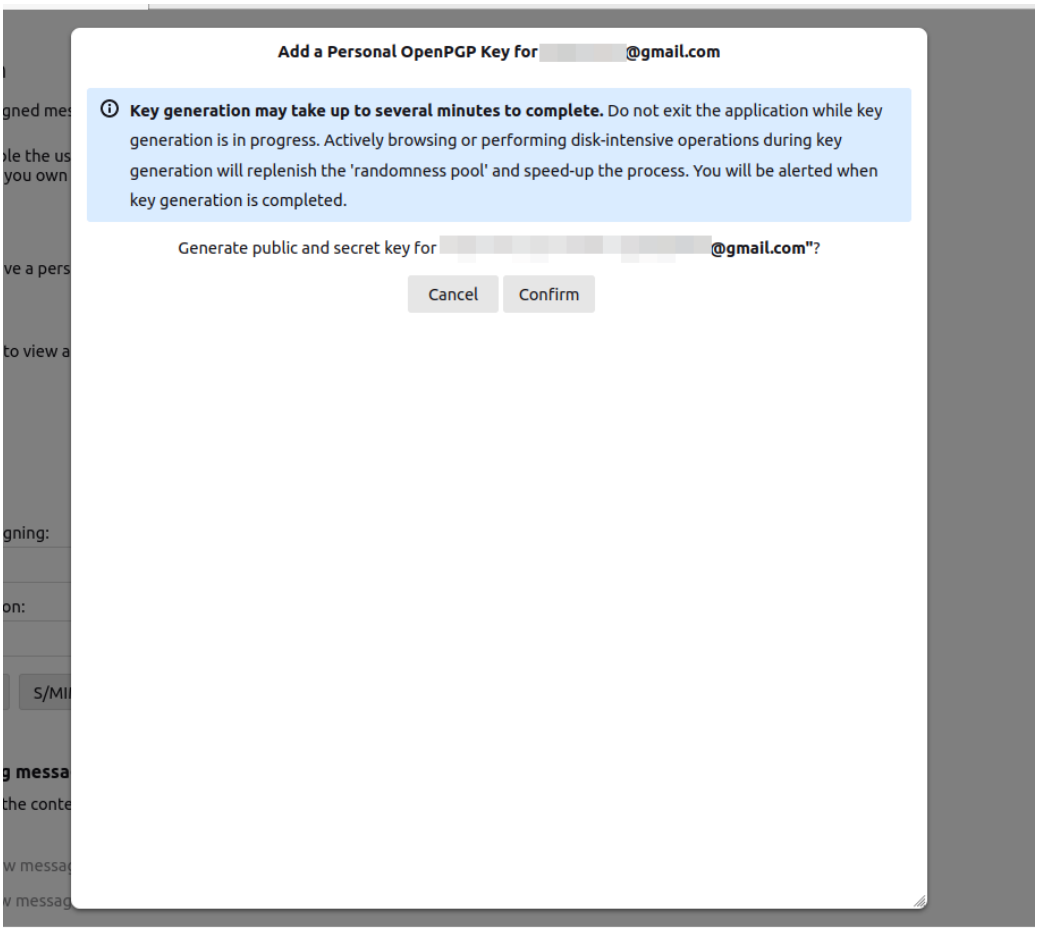

Figure 10. Confirmando la creación del par de claves

El par de claves ahora debería haberse creado correctamente (Par de claves generadas correctamente).

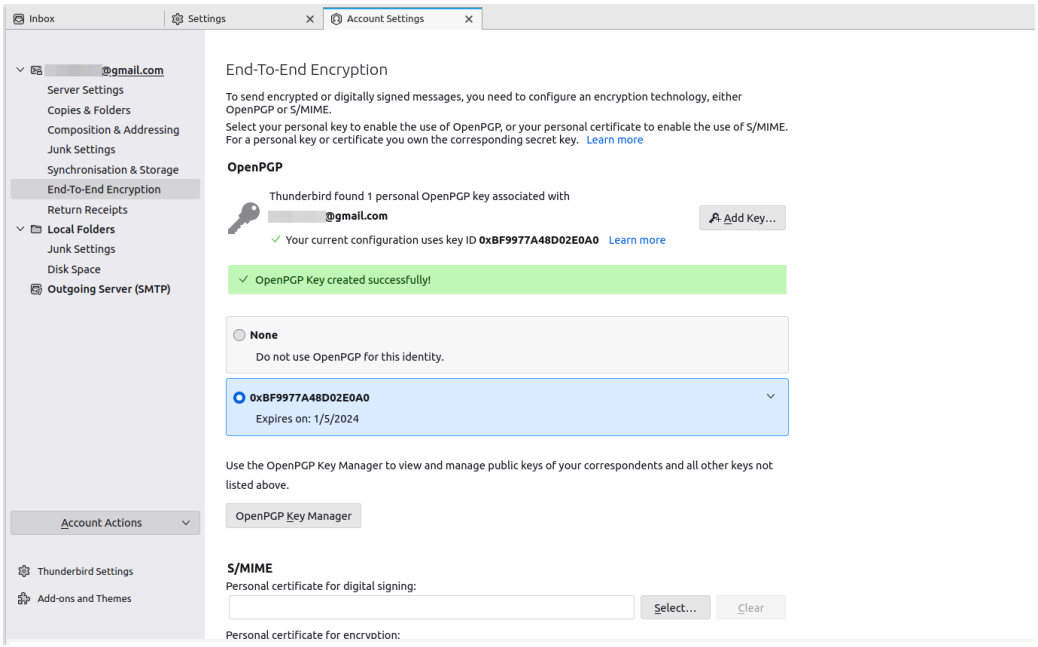

Figure 11. Par de claves generadas correctamente

Ahora puede hacer clic en “Administrador de claves OpenPGP” para configurar una serie de cosas, como un keyserver para buscar claves públicas de sus destinatarios potenciales (Interfaz del administrador de claves).

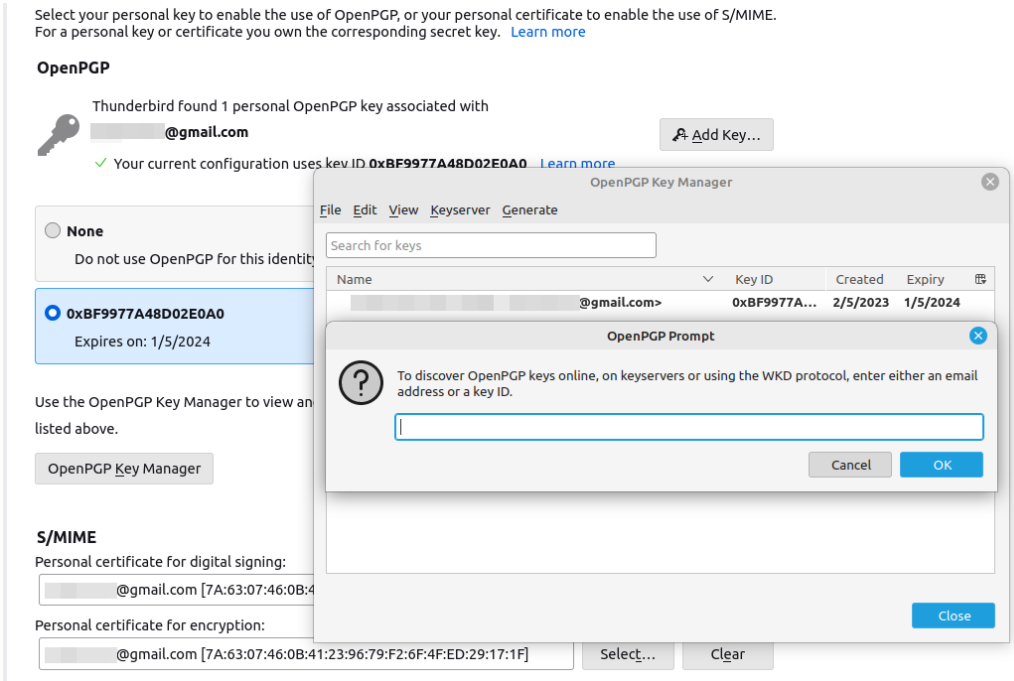

Figure 12. Interfaz del administrador de claves

Configuración de S/MIME e importación de un certificado

Ahora nos centraremos en S/MIME. Comenzaremos obteniendo e importando un certificado X.509 válido para firmar y cifrar digitalmente el correo con S/MIME. Para simplificar el proceso, puede obtener un certificado gratuito de una CA de confianza. (La generación de su propio certificado autofirmado queda fuera del alcance de esta lección). Una vez que lo haga, haga clic en "Administrar certificados S/MIME", busque su certificado en su unidad local e impórtelo. Si se le solicita una contraseña, proporciónela como se muestra en Cómo proporcionar una contraseña al importar un certificado.

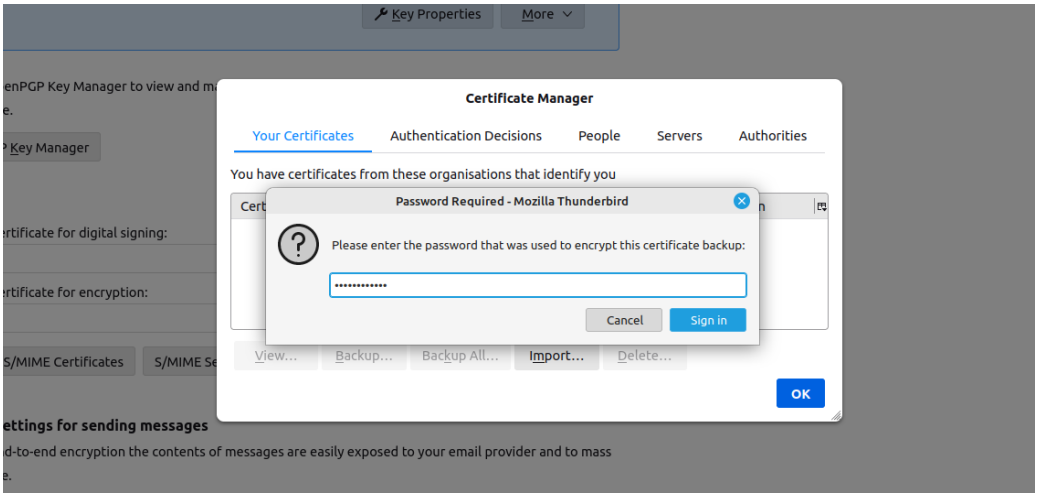

Figure 13. Cómo proporcionar una contraseña al importar un certificado

Luego seleccione su certificado (Selección de una imagen de certificado).

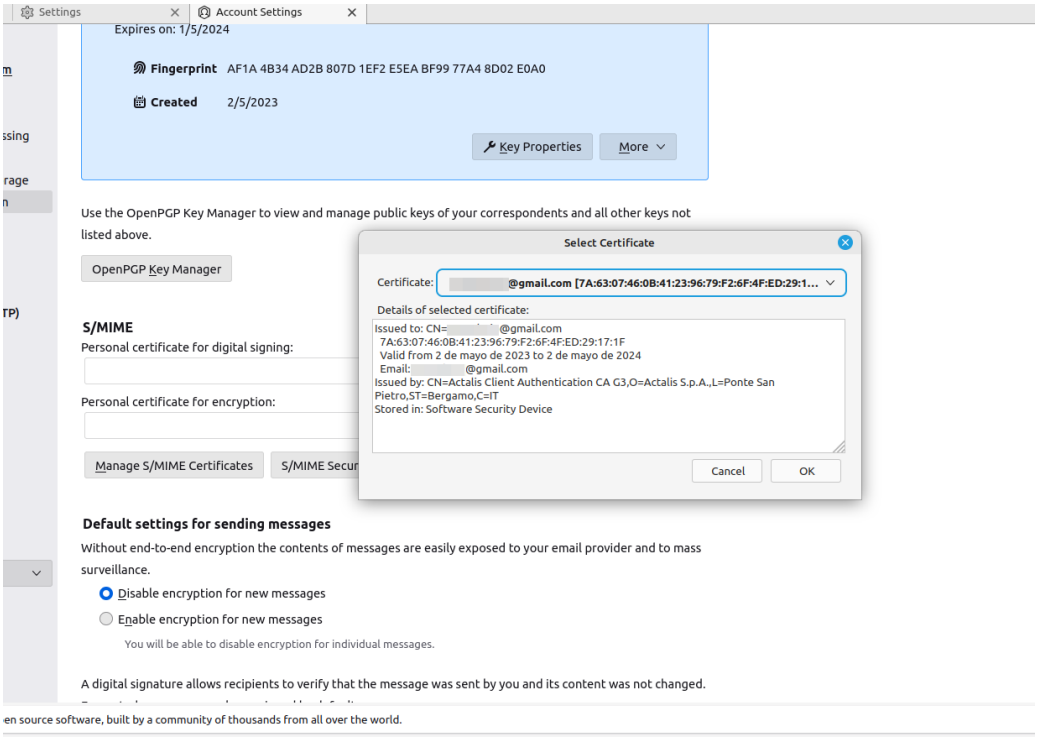

Figure 14. Selección de una imagen de certificado

A continuación se le solicitará un segundo certificado que será utilizado por otras personas al enviar sus mensajes cifrados. Puede elegir el mismo certificado (Seleccionar una segundo certificado).

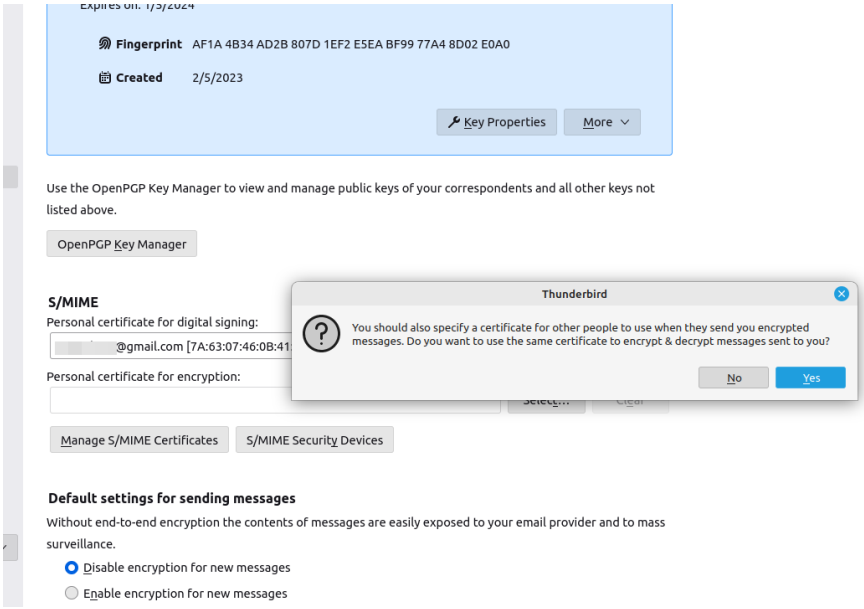

Figure 15. Seleccionar una segundo certificado

Por último, puedes verificar que tu certificado esté seleccionado tanto para firma digital como

para cifrado (Los certificados están listos para usar).

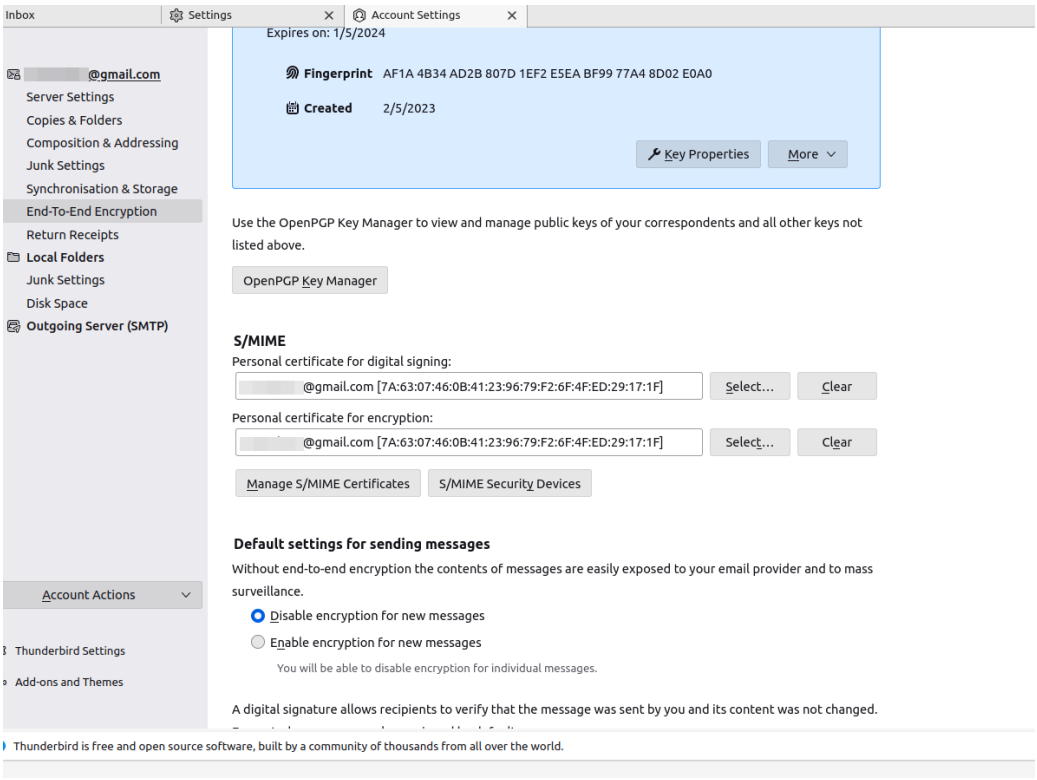

Figure 16. Los certificados están listos para usar

Ahora que ha configurado tanto OpenPGP como S/MIME, puede ir a la parte inferior de la página y elegir su tecnología de cifrado preferida: OpenPGP, S/MIME o selección automática basada en claves o certificados disponibles (Tecnología de cifrado preferida).

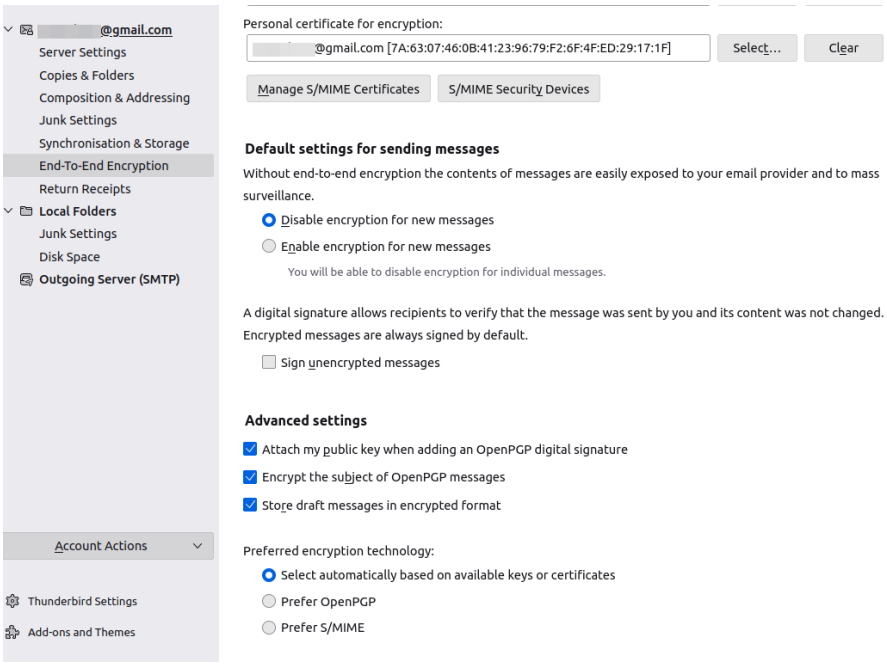

Figure 17. Tecnología de cifrado preferida

Enviar y recibir correo electrónico cifrado con OpenPGP

Si intenta enviar un mensaje a alguien cuya clave pública posee, Thunderbird le informa que el cifrado de correo electrónico está disponible y puede proceder a utilizarlo. El cifrado es posible cuando se posee la clave pública del destinatario muestra el mensaje que aparece en la parte inferior del mensaje de correo electrónico. La interfaz es bastante fácil de usar.

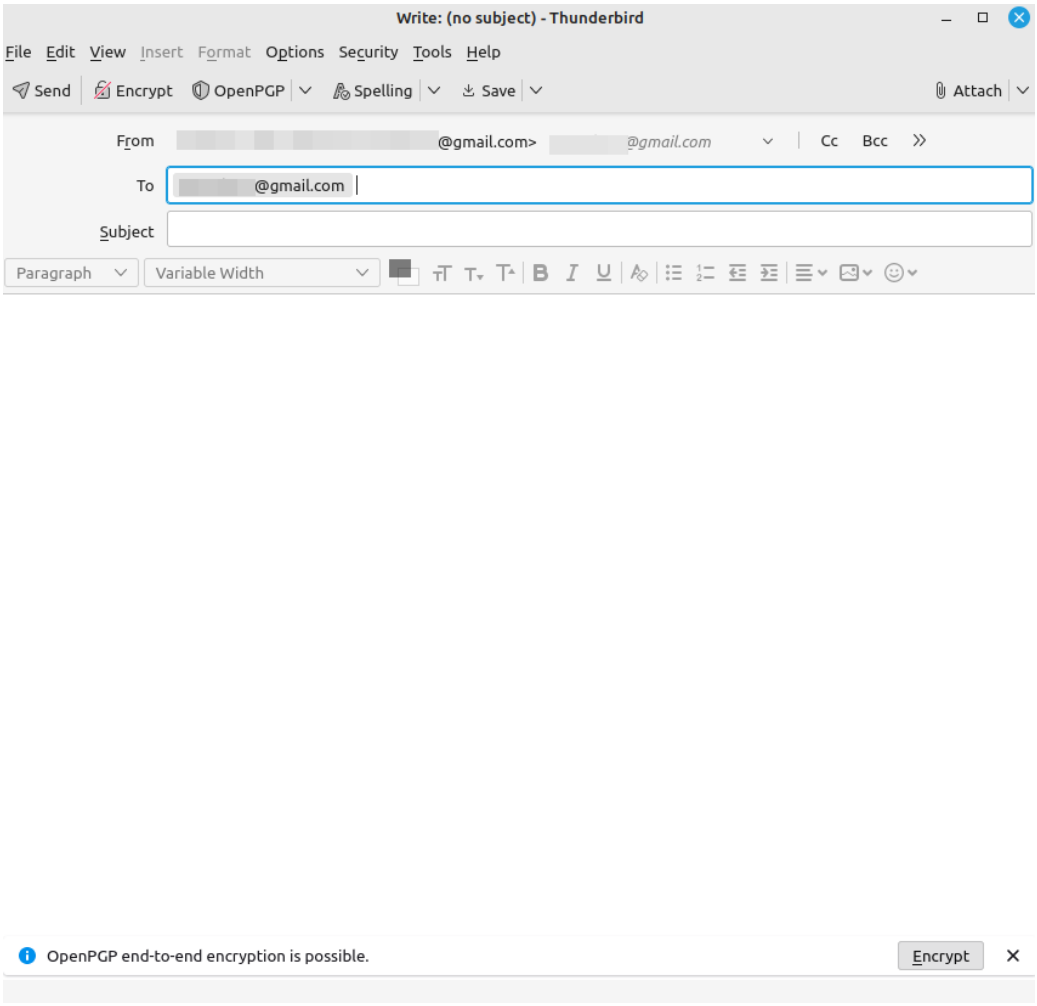

Figure 18. El cifrado es posible cuando se posee la clave pública del destinatario

De esta forma, si te envías un mensaje a ti mismo con el asunto “Prueba de cifrado de correo electrónico” y el cuerpo “¡Hola! ¡Adiós!”, podrás abrirlo y leerlo. En el lado derecho de la pantalla, haz clic en el botón “OpenPGP” para obtener información sobre la clave (Envío y recepción de correo electrónico cifrado mediante PGP).

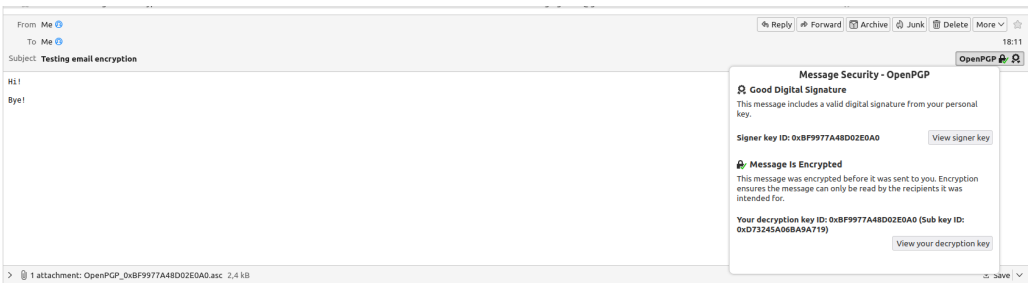

Figure 19. Envío y recepción de correo electrónico cifrado mediante PGP

Por otro lado, si intentas enviar un mensaje a un destinatario cuya clave pública no tienes en tu servidor, recibirás un mensaje alertándote de que el cifrado no es posible (El cifrado no es posible

a menos que tenga una clave utilizable para el destinatario).

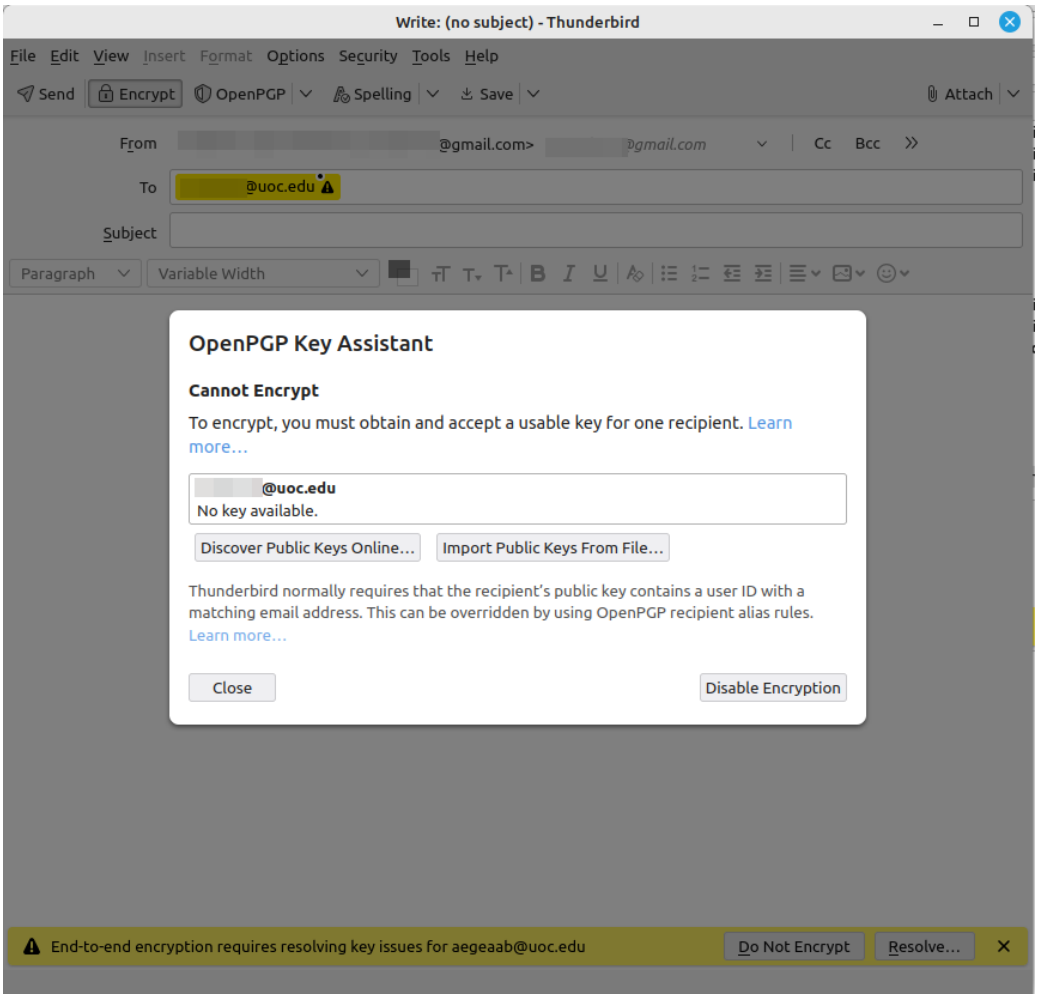

Figure 20. El cifrado no es posible a menos que tenga una clave utilizable para el destinatario

Puede importar claves públicas desde archivos o buscarlas en el servidor de claves.

Envío y recepción de correo electrónico cifrado con S/MIME

De manera similar a lo que hemos visto en la sección anterior, Thunderbird te permite enviar correo electrónico cifrado a alguien que tenga el certificado (El cifrado es posible si tiene un certificado válido del destinatario).

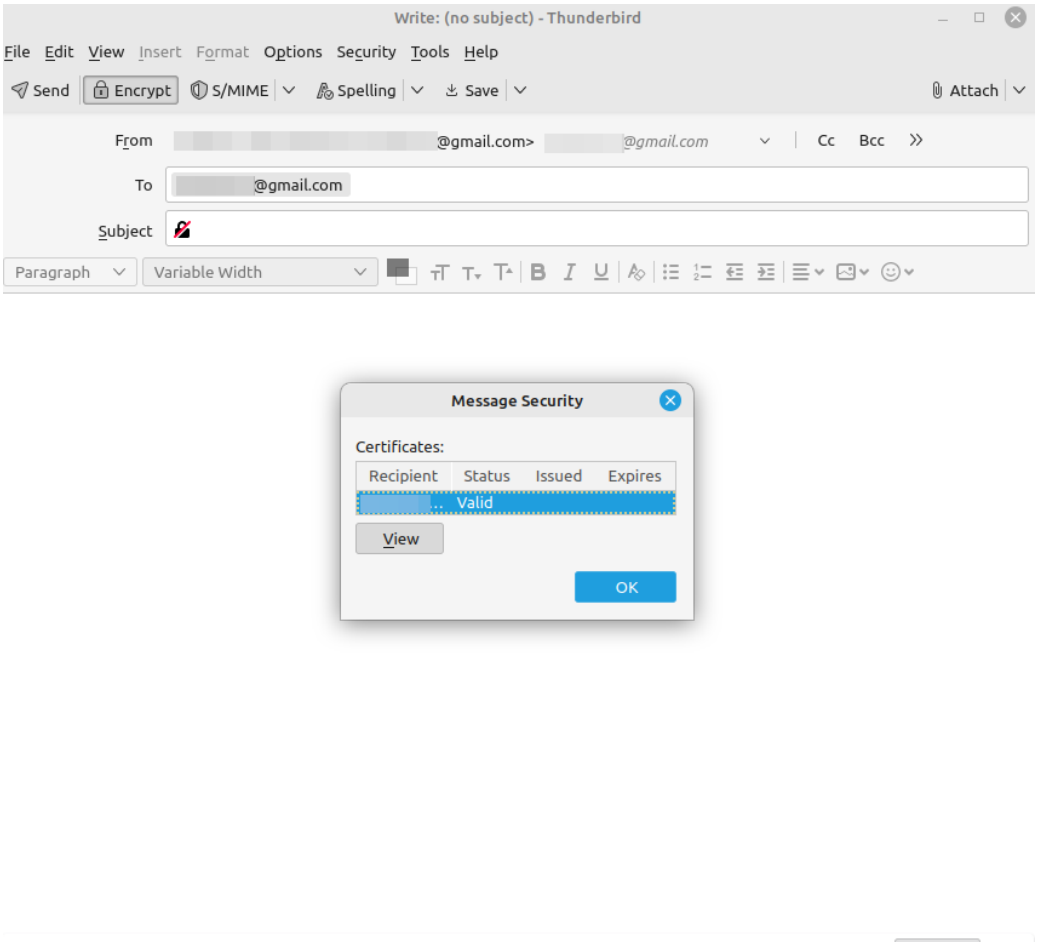

Figure 21. El cifrado es posible si tiene un certificado válido del destinatario

Puedes enviarte un mensaje a ti mismo con el asunto “Retesting email encrypted” y el mismo cuerpo que antes. Nuevamente, podrás abrirlo, leerlo y ver la información de seguridad S/MIME haciendo clic en el botón “S/MIME” a la derecha (Envío y recepción de correo electrónico cifrado mediante S/MIME).

Figure 22. Envío y recepción de correo electrónico cifrado mediante S/MIME

Si intenta enviar un mensaje a un destinatario que no tiene certificado, un mensaje de alerta le informará al respecto (El cifrado de extremo a extremo requiere resolver problemas de clave para el destinatario).

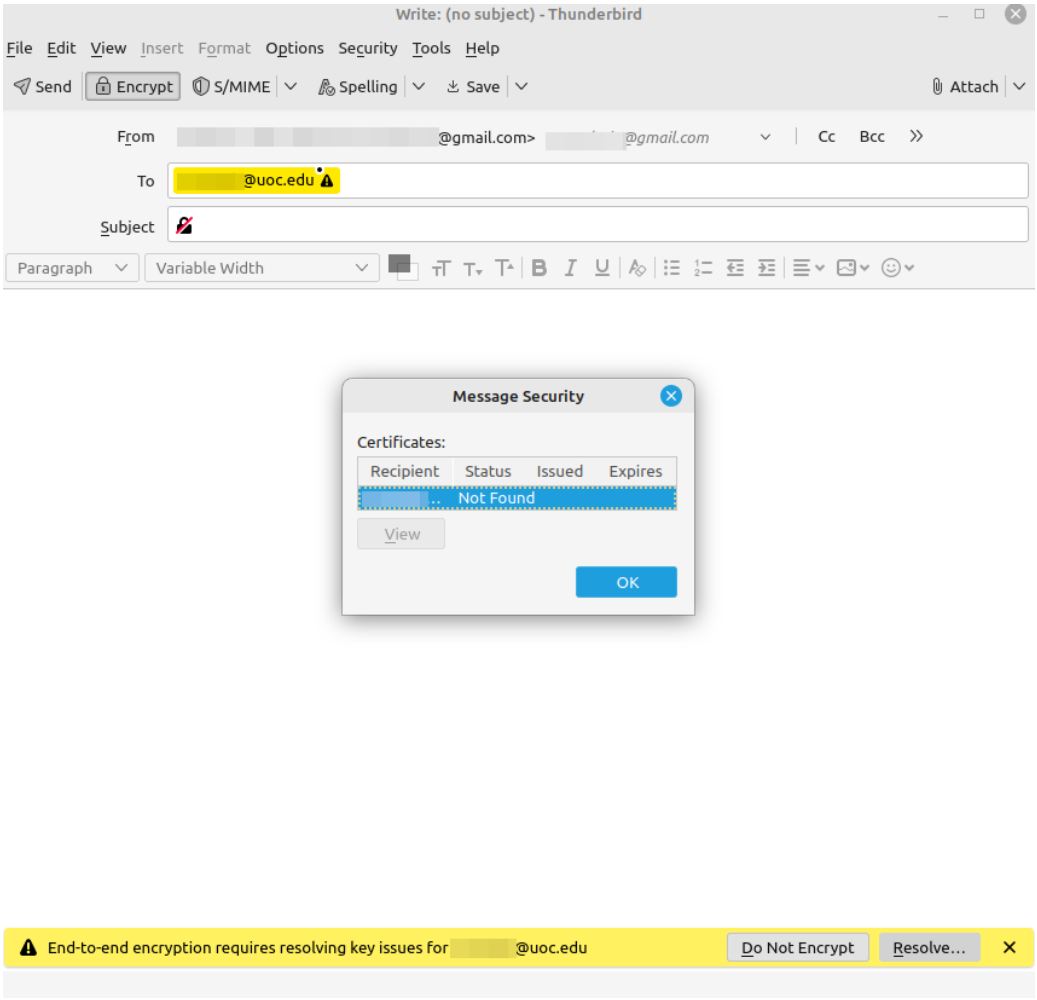

Figure 23. El cifrado de extremo a extremo requiere resolver problemas de clave para el destinatario

Ejercicios guiados

1. La criptografía de clave pública se basa en un par de claves formado por una clave pública y una clave privada. Indique a qué tipo de clave corresponden las siguientes afirmaciones:

Enunciado	**¿Clave pública o clave privada?**
Disponible para cualquiera que quiera enviar correo electrónico cifrado	
No debe compartirse con nadie	
Se aplica a un mensaje en texto simple para obtener un texto cifrado	
Se utiliza para descifrar correo electrónico	
Se puede importar a su llavero	

2. Indique a cuál de los siguientes conceptos corresponden las siguientes afirmaciones: criptografía simétrica, texto cifrado, autoridad de certificación, firma digital, Mozilla Thunderbird, ECDSA, confidencialidad, claves pares, GPG, S/MIME.

Afirmación	**Concepto**
Una clave pública y su clave privada correspondiente	
La misma clave se utiliza tanto para el cifrado como para el descifrado	
Un tercero de confianza que emite, revoca y gestiona certificados digitales	
Se utiliza para verificar la autenticidad e integridad de un documento digital	
Una implementación gratuita de OpenPGP	
Un algoritmo criptográfico para generar y verificar firmas digitales	
Un mensaje que se ha vuelto ininteligible	
Un protocolo de seguridad que garantiza el cifrado de extremo a extremo	

Afirmación	**Concepto**
Garantiza que un mensaje sea leído solo por el destinatario previsto	
Un cliente de correo electrónico multiplataforma gratuito y de código abierto que admite el cifrado de extremo a extremo	

Ejercicios exploratorios

1. Aparte de los tres casos de uso mencionados en el último ejercicio de la sección anterior, nombre dos protocolos de intercambio de datos que utilicen criptografía asimétrica. Explique brevemente cómo funcionan.

2. ¿Qué protocolos pueden garantizar un intercambio seguro de correo electrónico?

3. ¿Qué protocolos pueden garantizar una navegación web segura?

 | Esta obra está bajo la licencia CC BY-NC-ND 4.0. |

Resumen

Esta lección profundiza en la importancia crítica del cifrado de correo electrónico en el mundo digital actual, centrándose en dos protocolos ampliamente utilizados: OpenPGP y S/MIME. Estos estándares de cifrado garantizan la confidencialidad, integridad y autenticidad de las comunicaciones por correo electrónico, brindando protección contra el acceso no autorizado. OpenPGP opera con un modelo de confianza descentralizado en el que los usuarios administran sus propias claves de cifrado, mientras que S/MIME utiliza un modelo de confianza centralizado respaldado por certificados digitales emitidos por autoridades de certificación (CA) confiables. Ambos protocolos permiten el cifrado para evitar que los destinatarios no autorizados lean el contenido del correo electrónico y ofrecen firmas digitales para verificar la identidad del remitente.

La lección también analiza la configuración práctica de Mozilla Thunderbird, un popular cliente de correo electrónico que admite OpenPGP y S/MIME para el cifrado de extremo a extremo.

Respuestas a los ejercicios guiados

1. La criptografía de clave pública se basa en un par de claves formado por una clave pública y una clave privada. Indique a qué tipo de clave corresponden las siguientes afirmaciones:

Enunciado	**¿Clave pública o clave privada?**
Disponible para cualquiera que quiera enviar correo electrónico cifrado	clave pública
No debe compartirse con nadie	clave privada
Se aplica a un mensaje en texto simple para obtener un texto cifrado	clave pública
Se utiliza para descifrar correo electrónico	clave privada
Se puede importar a su llavero	clave pública

2. Indique a cuál de los siguientes conceptos corresponden las siguientes afirmaciones: criptografía simétrica, texto cifrado, autoridad de certificación, firma digital, Mozilla Thunderbird, ECDSA, confidencialidad, claves pares, GPG, S/MIME.

Afirmación	**Concepto**
Una clave pública y su clave privada correspondiente	claves pares
La misma clave se utiliza tanto para el cifrado como para el descifrado	criptografía simétrica
Un tercero de confianza que emite, revoca y gestiona certificados digitales	autoridad de certificación
Se utiliza para verificar la autenticidad e integridad de un documento digital	firma digital
Una implementación libre de OpenPGP	GPG
Un algoritmo criptográfico para generar y verificar firmas digitales	ECDSA
Un mensaje que se ha vuelto ininteligible	texto cifrado
Un protocolo de seguridad que garantiza el cifrado de extremo a extremo	S/MIME

Afirmación	**Concepto**
Garantiza que un mensaje sea leído solo por el destinatario previsto	confidencialidad
Un cliente de correo electrónico multiplataforma gratuito y de código abierto que admite el cifrado de extremo a extremo	Mozilla Thunderbird

Respuestas a los ejercicios exploratorios

1. Además de los tres casos de uso mencionados en el último ejercicio de la sección anterior, nombre dos protocolos de intercambio de datos que utilicen criptografía asimétrica. Explique brevemente cómo funcionan.

   El Protocolo de transferencia segura de archivos (SFTP) y Secure Shell (SSH) aseguran las transferencias de archivos entre un cliente y un servidor.

   Una red privada virtual (VPN) proporciona una comunicación segura y autenticada entre dispositivos remotos a través de una red insegura como Internet.

2. ¿Qué protocolos pueden garantizar un intercambio seguro de correo electrónico?

   PGP, S/MIME.

3. ¿Qué protocolos pueden garantizar una navegación web segura?

   SSL, TLS.

022.4 Cifrado de almacenamiento de datos

Referencia al objetivo del LPI

Security Essentials version 1.0, Exam 020, Objective 022.4

Peso

2

Áreas de conocimiento clave

- Comprensión de los conceptos de cifrado de datos, archivos y dispositivos de almacenamiento
- Uso de VeraCrypt para almacenar datos en un contenedor cifrado o en un dispositivo de almacenamiento cifrado
- Comprender las características principales de BitLocker
- Uso de Cryptomator para cifrar archivos en servicios de almacenamiento de archivos en la nube

Lista parcial de archivos, términos y utilidades

- VeraCrypt
- BitLocker
- Cryptomator

Linux Professional Institute

Lección 1

Certificado:	Fundamentos de seguridad
Versión:	1.0
Tema:	022 Cifrado
Objetivo:	022.4 Cifrado de almacenamiento de datos
Lección:	1 de 1

Introducción

En el ámbito de la ciberseguridad, proteger los datos en reposo es tan importante como proteger los datos en tránsito. El cifrado de archivos y el de dispositivos de almacenamiento son prácticas clave que se utilizan para garantizar que la información confidencial permanezca segura, ya sea almacenada en dispositivos locales o en la nube. Estos métodos de cifrado transforman los datos en formatos ilegibles, de modo que solo puedan acceder quienes tengan las claves de descifrado correctas. Este proceso no solo protege los datos del acceso no autorizado en caso de robo o pérdida, sino que también garantiza el cumplimiento de las normas de privacidad y seguridad.

En esta lección se exploran los conceptos fundamentales del cifrado de archivos y dispositivos de almacenamiento, y se detalla cómo se pueden almacenar datos de forma segura en dispositivos locales y en la nube. También se tratan métodos prácticos para cifrar archivos y dispositivos de almacenamiento completos, lo que ofrece una comprensión integral de las herramientas y técnicas necesarias para proteger la información confidencial en el entorno digital cada vez más interconectado de la actualidad.

Cifrado de datos, archivos y dispositivos de almacenamiento

La información confidencial, ya sea personal, financiera o empresarial, debe protegerse contra el acceso no autorizado. El cifrado de datos es uno de los métodos más fiables para garantizar esta seguridad, ya que convierte los datos en un formato codificado que solo pueden descifrar los usuarios autorizados que poseen la clave de descifrado correcta.

El cifrado de datos implica transformar datos legibles (texto simple) en un formato ilegible (texto cifrado). Esto garantiza que, incluso si los datos son interceptados o accedidos por actores maliciosos, no podrán descifrar su contenido sin la clave de descifrado. El cifrado se puede aplicar en diferentes niveles, incluidos archivos individuales, dispositivos de almacenamiento completos e incluso servicios de almacenamiento en la nube.

El *cifrado de archivos* se aplica a los archivos individuales, haciéndolos seguros incluso si se transfieren entre dispositivos o se envían a través de redes no seguras. Las herramientas y el software diseñados para el cifrado de archivos garantizan que solo las personas que tengan la clave de cifrado o la llaves correctas puedan acceder a los archivos. Este método es particularmente útil para proteger documentos sensibles o información confidencial que puede ser necesario compartir o respaldar en unidades externas o servicios de almacenamiento en la nube.

Por otro lado, el *cifrado de dispositivos de almacenamiento* implica cifrar todo el dispositivo, como discos duros, SSD, unidades flash USB y dispositivos de almacenamiento externo. En esta forma, todos los datos del dispositivo se cifran automáticamente a medida que se escriben en la unidad y se descifran cuando se leen. Este método garantiza que si el dispositivo físico se pierde o es robado, los datos que contiene permanecerán seguros. El cifrado de dispositivos de almacenamiento se utiliza habitualmente en portátiles, ordenadores de sobremesa y dispositivos móviles para protegerlos contra el acceso no autorizado en caso de robo o intentos de piratería.

El *cifrado de disco completo* (FDE) es un subconjunto del cifrado de dispositivos de almacenamiento que encripta todo el contenido de un dispositivo, incluido el sistema operativo. Esto garantiza que todos los datos del dispositivo estén protegidos sin necesidad de que el usuario intervenga para cifrar archivos individuales. El FDE se utiliza habitualmente en entornos corporativos donde el riesgo de vulneraciones de datos a causa de portátiles perdidos o robados es alto. Al requerir autenticación antes de que el sistema operativo pueda arrancar, el FDE proporciona una capa integral de seguridad.

Uno de los aspectos críticos del cifrado de archivos y dispositivos de almacenamiento es el uso de algoritmos de cifrado fuertes, como el *Estándar de cifrado avanzado* (AES), para garantizar que los atacantes no puedan descifrar fácilmente los datos. Estos métodos de cifrado proporcionan altos niveles de seguridad, pero solo son eficaces si las claves o contraseñas de cifrado se administran

correctamente. Las prácticas de administración de claves deficientes, como contraseñas débiles o no realizar copias de seguridad de las claves de cifrado, pueden socavar la eficacia del cifrado y provocar la pérdida de datos.

A medida que el almacenamiento de datos se traslada cada vez más a la nube, el *cifrado del almacenamiento en la nube* se ha convertido en una parte esencial de la seguridad de los datos. Los proveedores de almacenamiento en la nube suelen ofrecer cifrado integrado para proteger los datos de los usuarios durante la transmisión (cifrado en tránsito) y mientras se almacenan en servidores en la nube (cifrado en reposo). Sin embargo, algunos usuarios prefieren cifrar sus archivos ellos mismos antes de subirlos a la nube, lo que garantiza que solo ellos tengan acceso a las claves de cifrado.

Comprender cómo y cuándo aplicar el cifrado de archivos y dispositivos de almacenamiento es fundamental para mantener la seguridad de los datos tanto en entornos personales como profesionales. La correcta implementación del cifrado garantiza que los datos confidenciales permanezcan seguros, protegidos del acceso no autorizado y cumplan con las normas de privacidad.

Exploraremos la aplicación práctica de herramientas de cifrado como *VeraCrypt*, *BitLocker* y *Cryptomator*. Estas herramientas ofrecen soluciones sólidas para el cifrado de archivos, dispositivos de almacenamiento y la nube. Cada herramienta ofrece características únicas adaptadas a necesidades de cifrado específicas.

Uso de VeraCrypt para almacenar datos en un contenedor cifrado o en un dispositivo de almacenamiento cifrado

VeraCrypt es multiplataforma y compatible con Windows, macOS y Linux, lo que lo convierte en una solución versátil para personas y organizaciones que operan en múltiples entornos. Se puede acceder a los datos cifrados en un sistema operativo y descifrarlos en otro, siempre que se disponga de las credenciales de descifrado correctas. Esta flexibilidad es esencial para mantener el almacenamiento seguro de los datos en diferentes plataformas y dispositivos.

La función principal de VeraCrypt es la creación de contenedores cifrados. Un contenedor cifrado actúa como un disco virtual en el que se pueden almacenar datos de forma segura. Este contenedor aparece como un único archivo en el sistema, pero una vez montado en VeraCrypt, se comporta como un volumen de almacenamiento normal en el que se pueden añadir, editar y eliminar archivos. La principal ventaja de este método es que todo el contenido del contenedor está cifrado, lo que hace imposible que usuarios no autorizados accedan a los datos sin la clave de descifrado o la contraseña correctas.

Antes de que aparezcan los contenedores, la pantalla principal de VeraCrypt se parece a Pantalla

principal de VeraCrypt.

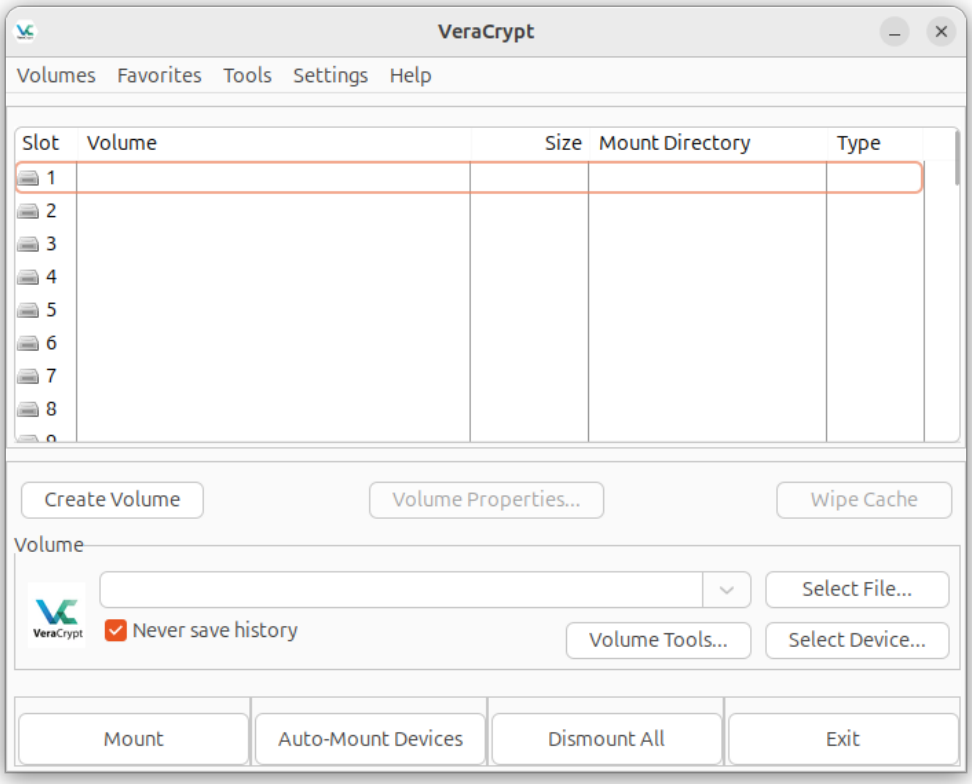

Figure 24. Pantalla principal de VeraCrypt

Para crear un contenedor cifrado en VeraCrypt, comience seleccionando un archivo o partición que actuará como contenedor (Un archivo de volumen seleccionado en VeraCrypt).

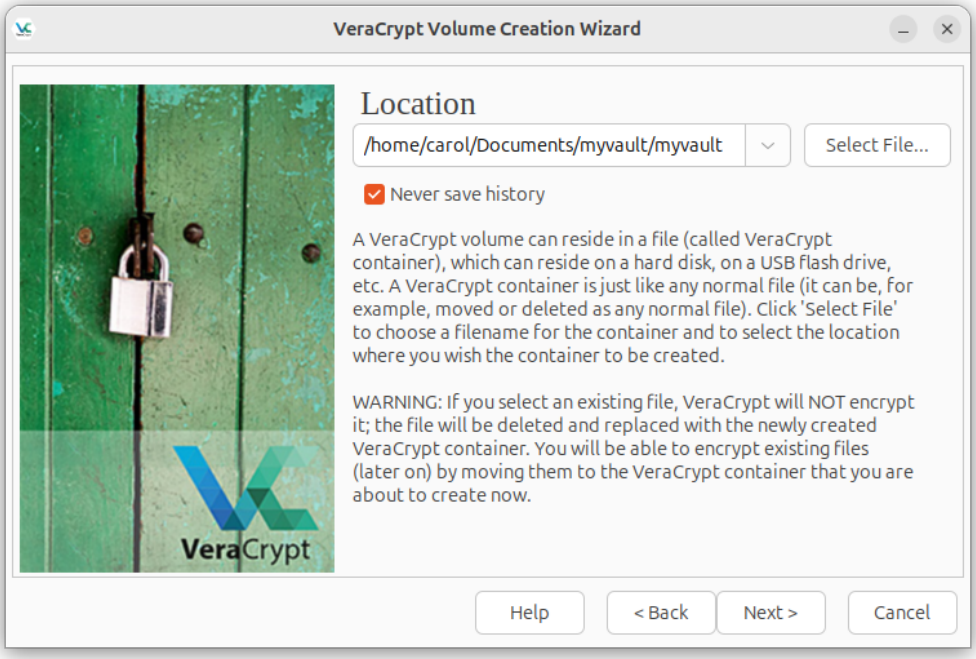

Figure 25. Un archivo de volumen seleccionado en VeraCrypt

Se le solicitará que elija el algoritmo de cifrado. AES es el algoritmo más recomendado, gracias a su alto nivel de seguridad (Selección de AES como algoritmo de cifrado de VeraCrypt).

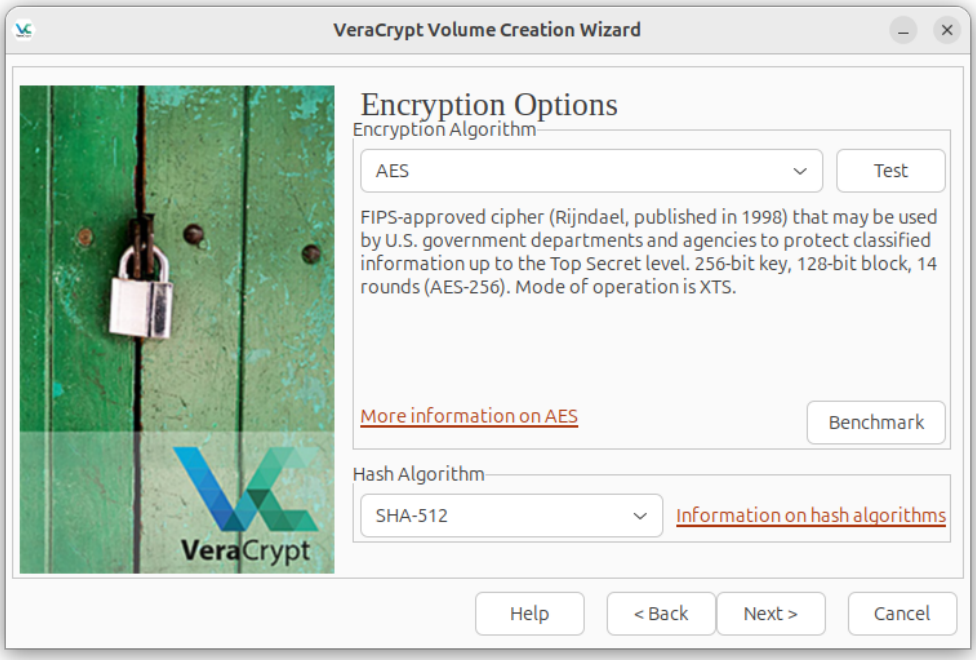

Figure 26. Selección de AES como algoritmo de cifrado de VeraCrypt

A continuación especifique el tamaño del volumen (Tamaño del volumen de VeraCrypt).

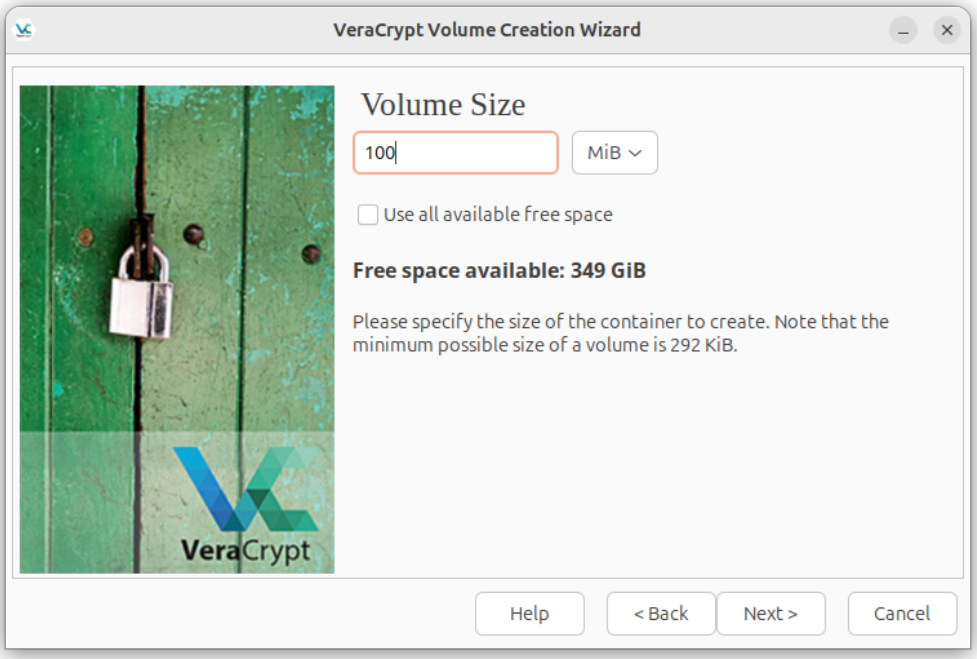

Figure 27. Tamaño del volumen de VeraCrypt

El último paso es crear una contraseña segura (Definir una contraseña en VeraCrypt).

Figure 28. Definir una contraseña en VeraCrypt

Ahora el contenedor está montado en VeraCrypt y listo para usar (Volumen cifrado montado en VeraCrypt). Funciona como cualquier otra unidad de almacenamiento, pero todos los datos almacenados dentro del contenedor se cifran automáticamente en tiempo real.

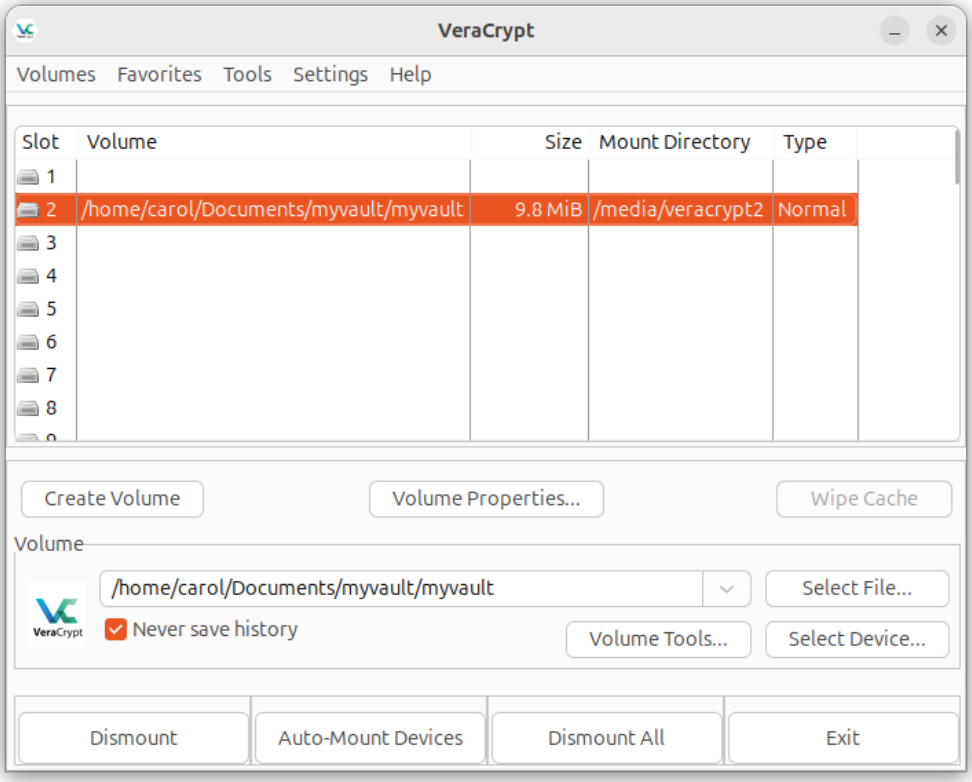

Figure 29. Volumen cifrado montado en VeraCrypt

VeraCrypt también admite el cifrado de disco completo, lo que permite a los usuarios cifrar dispositivos de almacenamiento completos, como unidades externas, unidades flash USB o incluso discos duros internos. Esto garantiza que todos los datos del dispositivo estén cifrados, incluidos los archivos del sistema y el propio sistema operativo, si así se desea. El cifrado de disco completo es especialmente útil para proteger información confidencial en caso de robo o pérdida del dispositivo físico. Al utilizar el cifrado de disco completo, los usuarios deben introducir una contraseña o utilizar un archivo de claves en el momento del arranque para descifrar la unidad y acceder a su contenido.

Para cifrar un dispositivo de almacenamiento con VeraCrypt, el usuario selecciona la unidad o partición que desea cifrar y elige un algoritmo de cifrado. De forma similar a los contenedores cifrados, se crea una contraseña o un archivo de claves seguro para garantizar la integridad de los datos. Una vez que se completa el proceso de cifrado, el dispositivo entero se vuelve inaccesible sin las credenciales de descifrado correctas. Este método proporciona una capa integral de protección para unidades portátiles que pueden contener información confidencial.

Uso de Cryptomator para cifrar archivos almacenados en servicios de almacenamiento en la nube

Cryptomator es una potente herramienta diseñada específicamente para cifrar archivos antes de que se carguen en servicios de almacenamiento en la nube. Su simplicidad y facilidad de uso la convierten en una solución ideal para proteger datos confidenciales en plataformas como Google Drive, Dropbox y OneDrive. Cryptomator crea una "`bóveda` o vault" cifrada en su sistema local, donde los archivos se pueden almacenar de forma segura antes de sincronizarlos con la nube. La bóveda garantiza que los datos se cifren en su dispositivo antes de que se carguen, lo que los hace ilegibles para usuarios no autorizados incluso si el servicio de almacenamiento en la nube se ve comprometido.

Cryptomator está disponible en varias plataformas, incluidas Windows, macOS, Linux y dispositivos móviles como iOS y Android. Una vez instalado, puedes crear una bóveda cifrada donde se almacenarán tus archivos. Esta bóveda se encuentra en una carpeta que se sincroniza con el servicio de almacenamiento en la nube que hayas elegido, lo que garantiza que los archivos cifrados se carguen automáticamente como parte del proceso de sincronización normal.

Después de la instalación, inicie Cryptomator y cree una nueva bóveda cifrada haciendo clic en el botón “Agregar” (<<022.4.fig7>).

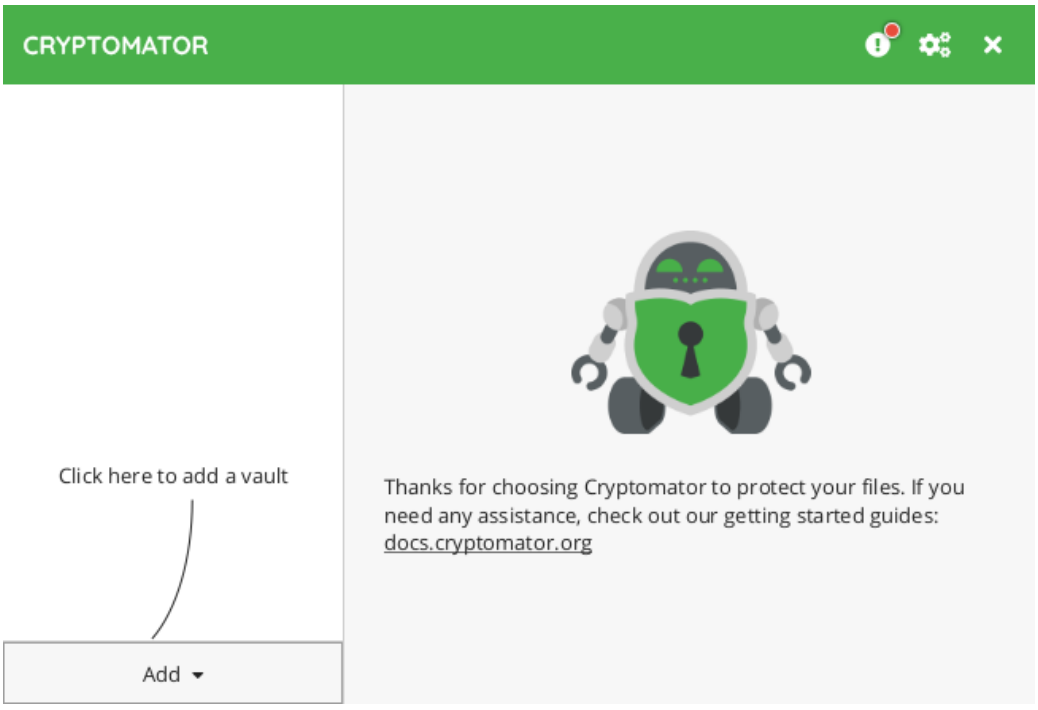

Figure 30. Pantalla principal de Cryptomator

Luego, seleccione “Crear nuevo almacén”, elija un nombre y una ubicación de almacenamiento

para su almacén (Selección de una ubicación de bóveda en Cryptomator). Este almacén puede ubicarse en una carpeta que esté sincronizada con su servicio de almacenamiento en la nube (por ejemplo, una carpeta en su directorio de Google Drive o Dropbox).

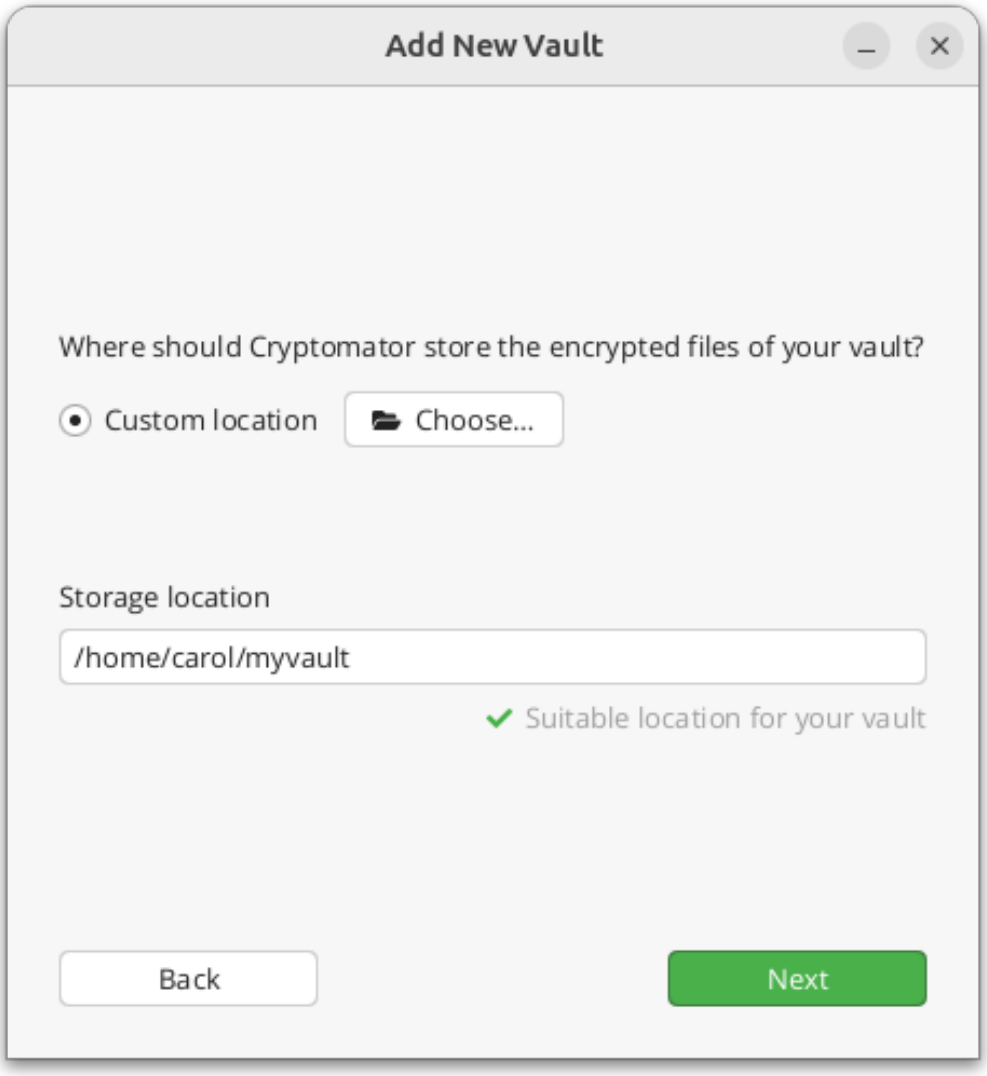

Figure 31. Selección de una ubicación de bóveda en Cryptomator

Ahora debe establecer una contraseña segura para la bóveda (Definir una contraseña en Cryptomator). Esta contraseña será necesaria para acceder a los archivos cifrados.

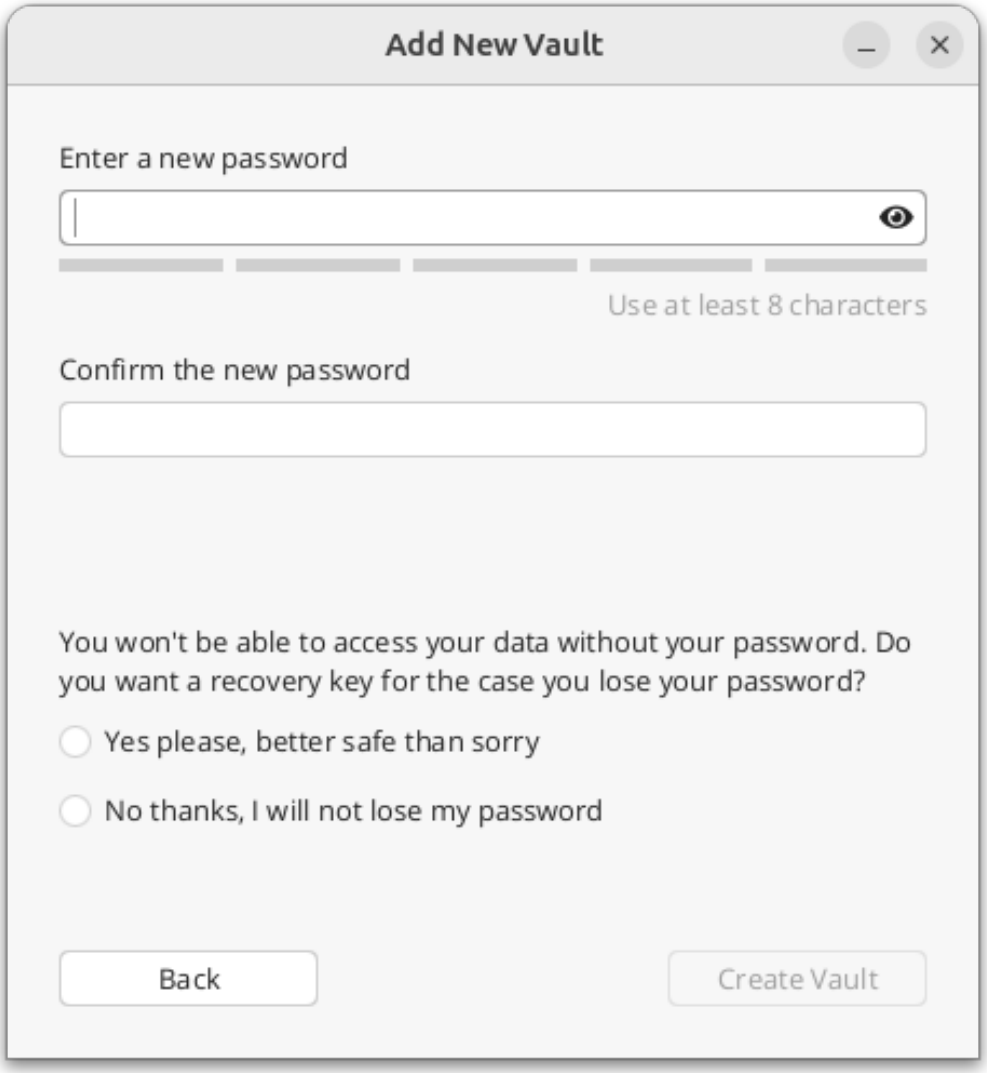

Figure 32. Definir una contraseña en Cryptomator

Una vez creada la bóveda, Cryptomator le solicitará que la desbloquee y la monte. Cuando la bóveda esté desbloqueada, se creará una unidad virtual en su sistema. Esta unidad virtual se comporta como una carpeta normal, lo que le permite mover archivos dentro y fuera de ella (Cryptomator - desbloquea y monta la bóveda).

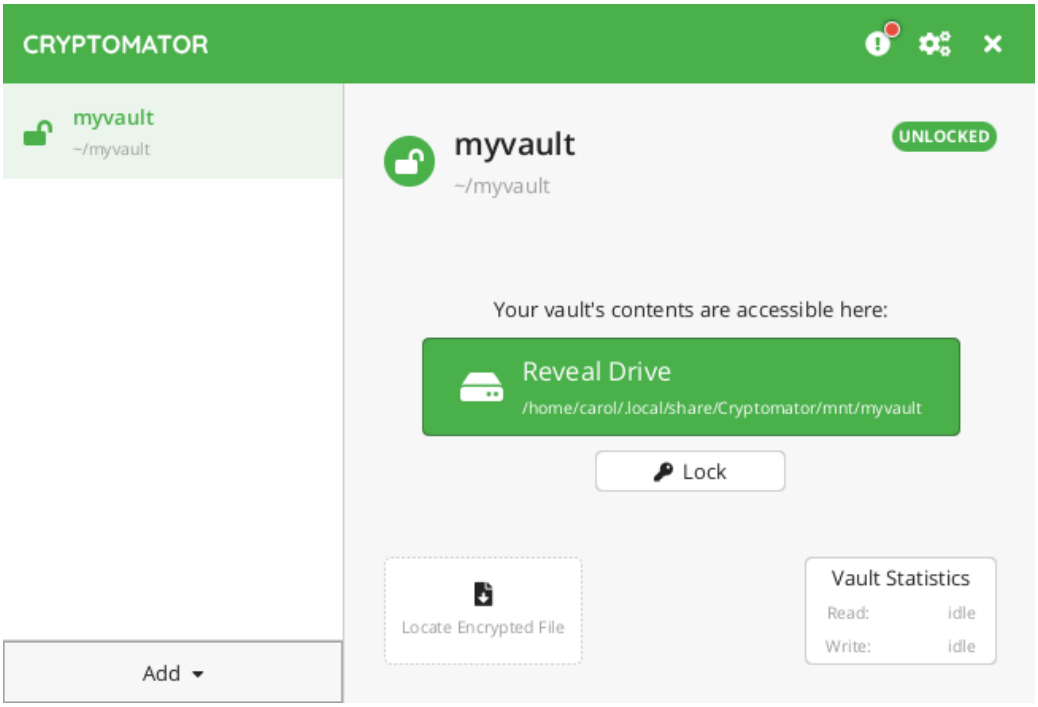

Figure 33. Cryptomator - desbloquea y monta la bóveda

Después de montarla, puede comenzar a agregar archivos. Simplemente arrastre y suelte o copie archivos en la bóveda. A medida que agrega archivos, Cryptomator los cifra automáticamente, lo que garantiza que los datos almacenados en la bóveda estén seguros.

Estos archivos aparecerán cifrados dentro de la carpeta de almacenamiento en la nube sincronizada (por ejemplo, Google Drive, Dropbox o OneDrive). Sin embargo, cuando se visualicen desde la unidad virtual, aparecerán como sus versiones originales, sin cifrar.

Dado que la bóveda se almacena en una carpeta que está sincronizada con un servicio de almacenamiento en la nube, todos los archivos cifrados se cargarán automáticamente en la nube. Estos archivos aparecerán en el almacenamiento en la nube como blobs cifrados, lo que hará imposible que usuarios no autorizados lean su contenido.

Una vez que haya terminado de trabajar con sus archivos, puede bloquear la bóveda, lo que desmonta la unidad virtual y garantiza que los archivos cifrados permanezcan seguros. La próxima vez que necesite acceder a la bóveda, simplemente desbloquéela ingresando su contraseña y la unidad virtual se volverá a montar con los archivos descifrados accesibles.

Cryptomator ofrece una sincronización perfecta con los servicios de almacenamiento en la nube, lo que garantiza que sus archivos cifrados se almacenen de forma segura sin necesidad de realizar ningún paso adicional. Por ejemplo, cuando agrega o modifica un archivo en la bóveda, este se cifra inmediatamente y se sincroniza con su servicio en la nube. Esto garantiza que los datos confidenciales estén protegidos en todo momento, incluso durante la sincronización.

El proceso de cifrado que utiliza Cryptomator es sólido y está diseñado para garantizar tanto la confidencialidad como la integridad. Los archivos almacenados en la bóveda se cifran mediante el algoritmo AES-256 y cada archivo se cifra individualmente, lo que permite una sincronización eficiente y garantiza que solo los archivos modificados se vuelvan a cargar en la nube.

Además de sus funciones de cifrado, Cryptomator ofrece indicaciones visuales para ayudarle a gestionar su bóveda. La bóveda aparece como una unidad virtual en su sistema, donde se puede acceder fácilmente a los archivos cifrados, y el proceso de bloqueo y desbloqueo es sencillo e intuitivo. Además, Cryptomator es de código abierto, lo que significa que su código está disponible públicamente para su revisión, lo que añade una capa adicional de transparencia y confianza en la seguridad de la herramienta.

Características principales de BitLocker

BitLocker es una función de cifrado de disco completo integrada en ciertas ediciones de Microsoft Windows y fue diseñada para proteger los datos mediante el cifrado de volúmenes enteros en el disco duro de una computadora. Al emplear algoritmos de cifrado potentes, BitLocker garantiza que los datos almacenados en el dispositivo estén protegidos contra el acceso no autorizado, incluso si el dispositivo de almacenamiento físico es robado o se pierde. BitLocker es particularmente útil en entornos donde la seguridad de los datos almacenados en dispositivos portátiles, como computadoras portátiles o unidades externas, es fundamental.

La función principal de BitLocker es proporcionar cifrado de disco completo (FDE). BitLocker utiliza el algoritmo AES con longitudes de clave de 128 o 256 bits, lo que ofrece una protección sólida contra los intentos de eludir la seguridad. BitLocker también admite el cifrado de unidades externas y dispositivos de almacenamiento extraíbles a través de su función *BitLocker To Go*.

Una de las características clave de BitLocker es su integración con el módulo de plataforma segura (TPM) del sistema, un componente de seguridad basado en hardware integrado en muchos ordenadores modernos. El TPM proporciona una capa adicional de protección al almacenar las claves de cifrado en un entorno seguro que está aislado del sistema operativo principal.

BitLocker ofrece *autenticación previa al arranque*, una función que mejora la seguridad al requerir que el usuario ingrese un PIN o use una memoria USB con una clave de inicio antes de que se inicie el sistema.

Como característica nativa de Windows, BitLocker está estrechamente integrado con el sistema operativo, lo que proporciona actualizaciones sin inconvenientes y compatibilidad con otras funciones de seguridad, como Windows Defender y Secure Boot. Esta integración garantiza que BitLocker funcione sin problemas para proteger los datos y, al mismo tiempo, mantener la estabilidad y la facilidad de uso generales del sistema.

Ejercicios guiados

1. Explique la diferencia principal entre el cifrado de archivos y de disco completo (FDE).

2. ¿Cuál es la función de un módulo de plataforma segura (TPM) en el cifrado de BitLocker?

3. ¿Cómo garantiza Cryptomator que los archivos almacenados en servicios en la nube permanezcan seguros?

4. Compare las características de seguridad de VeraCrypt y BitLocker. ¿Cuáles son las diferencias clave en la forma en que manejan el cifrado de disco completo y en qué situaciones preferiría uno sobre el otro?

 | Esta obra está bajo la licencia CC BY-NC-ND 4.0. |

Ejercicios exploratorios

1. BitLocker ofrece cifrado para los usuarios de Windows, pero no todos los usuarios querrán depender de una solución propietaria. Investigue alternativas de código abierto a BitLocker, como LUKS y eCryptfs, que se utilizan habitualmente en sistemas Linux. Compare estas herramientas en términos de solidez de cifrado, facilidad de uso y mecanismos de recuperación de claves. ¿Cuál recomendaría a un usuario que busca una solución de cifrado flexible y transparente, y por qué?

2. Explique cómo los proveedores de almacenamiento en la nube, como Google Drive y Dropbox, implementan el cifrado para los archivos almacenados en la nube. Compárelo con el cifrado que ofrece Cryptomator. ¿Cuáles son las ventajas de utilizar Cryptomator junto con estos servicios?

Resumen

Esta lección destaca la importancia de proteger los datos en reposo, haciendo énfasis en el cifrado de archivos y dispositivos de almacenamiento para garantizar la confidencialidad y seguridad de los datos. Profundiza en los conceptos esenciales del cifrado, que abarcan el cifrado de archivos, el cifrado de dispositivos de almacenamiento y el cifrado de disco completo (FDE). La lección explica cómo estos métodos convierten los datos legibles en formatos ilegibles a los que solo pueden acceder los usuarios autorizados con las claves de descifrado adecuadas. Esta protección se aplica tanto a los dispositivos locales como al almacenamiento en la nube, lo que garantiza la seguridad de los datos en caso de robo o pérdida.

La lección también explora VeraCrypt, una herramienta para crear contenedores cifrados y cifrado de disco completo, junto con Cryptomator, que protege los archivos almacenados en servicios en la nube. Por último, se analiza BitLocker, destacando características como el cifrado de disco completo y la integración con TPM para el almacenamiento seguro de claves.

Respuestas a los ejercicios guiados

1. Explique la diferencia principal entre el cifrado de archivos y el cifrado de disco completo (FDE).

   El cifrado de archivos protege los archivos individuales, lo que garantiza que solo los usuarios autorizados con la clave de descifrado o la contraseña correctas puedan acceder a ellos. El cifrado de disco completo (FDE), por otro lado, cifra todo el dispositivo de almacenamiento, incluido el sistema operativo, lo que hace que todos los datos del dispositivo sean inaccesibles sin autenticación. FDE protege todo lo que hay en el dispositivo, mientras que el cifrado de archivos se dirige a archivos específicos.

¿Cuál es la función de un módulo de plataforma segura (TPM) en el cifrado de BitLocker?

+ En el cifrado de BitLocker, el módulo de plataforma segura (TPM) es un componente de seguridad basado en hardware que almacena claves de cifrado en un entorno seguro. Mejora la seguridad al garantizar que las claves de cifrado estén aisladas del sistema operativo y puede desbloquear automáticamente las unidades cifradas durante el arranque, siempre que no se haya comprometido la integridad del sistema.

¿Cómo garantiza Cryptomator que los archivos almacenados en los servicios en la nube permanezcan seguros?

+ Cryptomator cifra los archivos localmente antes de que se carguen en los servicios de almacenamiento en la nube. Crea una bóveda cifrada donde los archivos se almacenan de forma segura y, una vez que se cargan, aparecen como blobs cifrados en el almacenamiento en la nube. Esto garantiza que, incluso si el servicio en la nube se ve comprometido, los usuarios no autorizados no puedan leer los archivos cifrados.

1. Compare las características de seguridad de VeraCrypt y BitLocker. ¿Cuáles son las diferencias clave en cómo manejan el cifrado de disco completo y en qué escenarios preferiría uno sobre el otro?

   VeraCrypt es una herramienta de código abierto que ofrece cifrado de disco completo multiplataforma y permite a los usuarios crear contenedores cifrados. Proporciona más opciones de personalización y transparencia porque es de código abierto. BitLocker, por otro lado, está integrado con Windows y ofrece una gestión perfecta con el Módulo de plataforma segura (TPM), que agrega seguridad basada en hardware. BitLocker generalmente se prefiere para entornos empresariales debido a su facilidad de integración y gestión a través de Active Directory, mientras que VeraCrypt puede ser preferido para usuarios que desean software de código abierto con un soporte de plataforma más amplio.

Respuestas a los ejercicios exploratorios

BitLocker ofrece cifrado para usuarios de Windows, pero no todos los usuarios querrán depender de una solución propietaria. Investigue alternativas de código abierto a BitLocker, como LUKS y eCryptfs, que se usan comúnmente en sistemas Linux. Compare estas herramientas en términos de solidez del cifrado, facilidad de uso y mecanismos de recuperación de claves. ¿Cuál recomendaría a un usuario que busca una solución de cifrado flexible y transparente, y por qué?

+ LUKS (Linux Unified Key Setup) y eCryptfs ofrecen un cifrado sólido. LUKS, el estándar para Linux, proporciona un cifrado sólido y admite varias claves por partición. eCryptfs es más fácil de usar, pero puede que no sea tan versátil para el cifrado de todo el disco. Según la investigación, LUKS sería la herramienta recomendada por su flexibilidad y compatibilidad con varias distribuciones de Linux, así como por su capacidad para cifrar unidades enteras.

1. Explique cómo los proveedores de almacenamiento en la nube, como Google Drive y Dropbox, implementan el cifrado para los archivos almacenados en la nube. Compárelo con el cifrado que ofrece Cryptomator. ¿Cuáles son las ventajas de utilizar Cryptomator junto con estos servicios?

   Los proveedores de almacenamiento en la nube como Google Drive y Dropbox suelen ofrecer cifrado del lado del servidor, donde los datos se cifran en reposo y en tránsito mediante claves administradas por el proveedor. Sin embargo, siguen teniendo el control sobre las claves de cifrado, lo que significa que podrían acceder a sus archivos o compartirlos si así lo exige la ley. Cryptomator, por el contrario, proporciona cifrado del lado del cliente, lo que significa que el usuario cifra los archivos localmente antes de que se carguen. Solo el usuario tiene las claves de descifrado, lo que ofrece más privacidad y seguridad. La ventaja de utilizar Cryptomator con estos servicios es que garantiza que los datos sigan siendo ilegibles incluso si el proveedor de la nube se ve comprometido o tiene que compartir datos con terceros.

 Esta obra está bajo la licencia CC BY-NC-ND 4.0.

Linux Professional Institute

Tema 023: Seguridad de dispositivos y almacenamiento

023.1 Seguridad de dispositivos y almacenamiento

Referencia al objetivo del LPI

Security Essentials version 1.0, Exam 020, Objective 023.1

Peso

2

Áreas de conocimiento clave

- Comprensión de los componentes principales de una computadora
- Comprensión de los dispositivos inteligentes e Internet de las cosas (IoT)
- Comprensión de las implicaciones de seguridad del acceso físico a una computadora
- Comprensión de los tipos de dispositivos USB, conexiones y aspectos de seguridad
- Comprensión de los dispositivos de tipo Bluetooth, conexiones y aspectos de seguridad
- Comprensión de los tipos de dispositivos RFID, conexiones y aspectos de seguridad
- Conocimiento de la computación confiable

Lista parcial de archivos, términos y utilidades

- Procesadores, memoria, almacenamiento, adaptadores de red
- Tabletas, teléfonos inteligentes, televisores, enrutadores, impresoras, hogares inteligentes, alarmas, dispositivos IoT (por ejemplo, bombillas, termostatos, televisores)
- USB
- Bluetooth
- RFID

Linux Professional Institute

Lección 1

Certificado:	Fundamentos de seguridad
Versión:	1.0
Tema:	023 Seguridad de dispositivos y almacenamiento
Objetivo:	023.1 Seguridad de hardware
Lección:	1 de 1

Introducción

La ciberseguridad ya no se limita a las vulnerabilidades del software o a las infracciones de la red. La seguridad del hardware desempeña un papel fundamental a la hora de garantizar la protección general de los sistemas informáticos. Un conocimiento básico de la seguridad del hardware es crucial para identificar y mitigar los riesgos que pueden comprometer la integridad y la confidencialidad de los sistemas informáticos.

Componentes principales de una computadora

Comprender los componentes principales de una computadora es fundamental para saber cómo pueden surgir vulnerabilidades de seguridad a nivel de hardware. Cada sistema informático está compuesto por varios elementos clave que trabajan juntos para realizar tareas y administrar datos, y cada uno de estos componentes tienen sus propios desafíos de seguridad.

En el corazón de cualquier computadora se encuentra el *procesador* (*unidad central de procesamiento o CPU*), que es responsable de ejecutar instrucciones y realizar cálculos. Como cerebro del sistema, el rendimiento y la seguridad de la CPU son cruciales. Las vulnerabilidades

en un procesador pueden dar lugar a ataques de canal lateral, en los que los atacantes pueden obtener acceso a datos confidenciales al monitorear el comportamiento de la CPU durante sus operaciones.

La *memoria* de una computadora, conocida principalmente como *memoria de acceso aleatorio* (RAM), es otro componente fundamental. La RAM almacena temporalmente datos e instrucciones a los que la CPU necesita acceder rápidamente. Sin embargo, dado que la RAM es volátil y pierde sus datos cuando se apaga el sistema, puede convertirse en un objetivo como los ataques de arranque en frío, en los que un atacante podría intentar recuperar datos confidenciales después de apagar el sistema.

Los *dispositivos de almacenamiento*, como los discos duros y las unidades de estado sólido (SSD), son responsables de la retención permanente de datos. Almacenan todo, desde el sistema operativo y las aplicaciones hasta archivos personales e información confidencial. A diferencia de la RAM, el almacenamiento conserva sus datos incluso después de que se apaga el sistema, lo que lo convierte en un objetivo principal para los ataques. El cifrado de los dispositivos de almacenamiento y las prácticas de borrado seguro son esenciales para proteger los datos del acceso no autorizado, especialmente en casos de robo o pérdida.

Por último, los *adaptadores de red* permiten que el ordenador se conecte a redes locales e Internet, lo que facilita la transmisión de datos entre dispositivos. Estos adaptadores son fundamentales para la comunicación, pero también abren numerosas vulnerabilidades de seguridad, como la posible exposición a ataques de intermediarios, rastreo de paquetes o acceso no autorizado a través de redes poco seguras.

Dispositivos inteligentes e Internet de las cosas (IoT)

Comprender los dispositivos inteligentes y el Internet de las cosas (IoT) es fundamental para reconocer los posibles riesgos de seguridad que plantea la rápida proliferación de dispositivos interconectados. A diferencia de las computadoras tradicionales, los dispositivos de IoT suelen integrarse en entornos cotidianos, desde hogares y oficinas hasta espacios públicos, lo que crea nuevas vulnerabilidades que pueden explotarse si los dispositivos no están protegidos adecuadamente.

Los dispositivos inteligentes, como las tabletas, los teléfonos y los televisores inteligentes, están a la vanguardia de la interacción digital personal y profesional. Estos dispositivos han evolucionado hasta convertirse en herramientas poderosas capaces de ejecutar aplicaciones complejas, almacenar datos confidenciales y conectarse a una variedad de redes. Sin embargo, su uso generalizado también los convierte en objetivos principales de los ciberataques.

La expansión de la IoT también ha introducido una gama de dispositivos domésticos inteligentes,

como termostatos, bombillas, cámaras y asistentes de voz. Si bien estos dispositivos ofrecen comodidad y automatización, también presentan desafíos de seguridad únicos. La mayoría de los dispositivos IoT están diseñados para ser "plug and play", lo que significa que son fáciles de instalar, pero a menudo carecen de sólidos protocolos de seguridad integrados. Por ejemplo, muchos dispositivos IoT se envían con nombres de usuario y contraseñas predeterminados, que los usuarios pueden olvidarse de cambiar, lo que deja a los dispositivos vulnerables a ataques como botnets o control no autorizado. Los dispositivos como los enrutadores, que sirven como puertas de enlace entre los sistemas IoT e Internet, deben configurarse correctamente con contraseñas seguras, cifrado y segmentación de red para evitar el acceso no autorizado.

En el caso de televisores inteligentes, impresoras y enrutadores, los riesgos van más allá del simple secuestro de dispositivos. La aplicación periódica de parches, la desactivación de funciones no utilizadas y el control de la actividad anormal pueden ayudar a mitigar estos riesgos.

Implicaciones de seguridad del acceso físico a una computadora

Al considerar la ciberseguridad, es esencial reconocer que el acceso físico a una computadora puede debilitar significativamente incluso las defensas digitales más sólidas. Un sistema al que personas no autorizadas pueden acceder físicamente es vulnerable a una variedad de ataques directos, muchos de los cuales pasan por alto las medidas de seguridad tradicionales basadas en software.

Uno de los riesgos más directos asociados al acceso físico es la posibilidad de manipular componentes de hardware. Un atacante con acceso físico puede manipular elementos clave de hardware, como reemplazar o modificar el disco duro del sistema, agregar dispositivos maliciosos como *keyloggers* o instalar hardware no autorizado para interceptar comunicaciones o transferencias de datos.

Otro riesgo crítico surge del acceso físico a los datos del sistema. Incluso si los datos están cifrados, un atacante que obtenga acceso físico a un dispositivo podría extraer o copiar los medios de almacenamiento para intentar descifrarlos más tarde.

El acceso físico también puede hacer que un atacante arranque el sistema desde un medio externo, como una unidad USB o un CD. Al hacerlo, el atacante puede eludir por completo el sistema operativo y los mecanismos de seguridad del sistema, obteniendo acceso a archivos, contraseñas y otra información confidencial sin tener que descifrar las credenciales de inicio de sesión existentes. Este tipo de ataque resalta la importancia de configurar los ajustes de BIOS (sistema básico de entrada/salida) o UEFI (interfaz de firmware extensible unificada) para deshabilitar el arranque desde dispositivos externos y garantizar que dichos ajustes estén protegidos con contraseña. Además, configurar una contraseña en el administrador de arranque, como GRUB, agrega una capa adicional de seguridad, lo que dificulta que un atacante eluda los

controles de seguridad del sistema operativo.

USB

Comprender los *dispositivos USB* (Universal Serial Bus), sus tipos, conexiones y aspectos de seguridad, es fundamental debido a su ubicuidad en la informática moderna. Los dispositivos USB se utilizan para una amplia gama de propósitos, desde almacenamiento hasta conectividad periférica, lo que los convierte en una parte común de las interacciones cotidianas con computadoras y redes. Sin embargo, su conveniencia también presenta riesgos de seguridad que deben gestionarse con cuidado.

Los dispositivos USB vienen en varios tipos, incluidos USB-A, USB-B y USB-C, cada uno diseñado para diferentes casos de uso. USB-A es el tipo más común y se encuentra en la mayoría de las computadoras para conectar periféricos como teclados, ratones y dispositivos de almacenamiento. USB-B se usa a menudo para dispositivos más grandes, como impresoras o discos duros externos, y USB-C es un estándar más nuevo, conocido por su diseño más pequeño y reversible y sus velocidades de transferencia de datos más rápidas.

Además de los conectores físicos, existen distintas versiones de USB que sirven para distintos propósitos. Por ejemplo, USB 2.0, 3.0 y 3.1 varían en cuanto a la velocidad de transferencia de datos; el USB 3.1 ofrece un rendimiento significativamente más rápido que el USB 2.0. Una transferencia de datos más rápida puede beneficiar el rendimiento, pero también significa que los datos maliciosos pueden transferirse más rápidamente, lo que representa un riesgo para la seguridad.

Desde el punto de vista de la seguridad, los dispositivos USB son propensos a una serie de ataques y vulnerabilidades. Una de las amenazas más comunes es el uso de dispositivos USB maliciosos. Los atacantes pueden utilizar unidades USB cargadas con malware para comprometer los sistemas cuando el dispositivo se conecta a una computadora. Estos ataques pueden ocurrir a través de técnicas como la ejecución automática de archivos maliciosos o la explotación de vulnerabilidades en el manejo de conexiones USB por parte del sistema operativo.

Los dispositivos USB también se utilizan a menudo para la *exfiltración de datos*, donde se copian datos confidenciales en una unidad USB y se eliminan de un entorno seguro. Este tipo de ataque puede ser perpetrado por personas malintencionadas internas o atacantes externos que obtienen acceso físico al sistema. Implementar *controles de puertos USB* o deshabilitar los puertos por completo es una práctica común para evitar que se conecten dispositivos no autorizados.

Para mitigar los riesgos de seguridad asociados con los dispositivos USB, es fundamental implementar varias prácticas recomendadas. El cifrado de datos en las unidades USB es esencial, especialmente cuando se maneja información confidencial. Además, el uso exclusivo de

dispositivos de confianza, garantizando que todos los dispositivos USB provengan de fuentes fiables, ayuda a reducir la probabilidad de ataques maliciosos. Por último, las organizaciones deben aplicar políticas que limiten el uso de dispositivos USB en entornos de alta seguridad y educar a los empleados sobre los posibles peligros de conectar dispositivos desconocidos.

Bluetooth

La tecnología Bluetooth es compatible con varios tipos de dispositivos en diferentes industrias. Los tipos más comunes de dispositivos Bluetooth incluyen dispositivos personales como teléfonos inteligentes, tabletas, auriculares inalámbricos y relojes inteligentes. Estos dispositivos se comunican entre sí a corta distancia, lo que convierte a Bluetooth en una tecnología esencial para crear ecosistemas inalámbricos tanto en entornos personales como profesionales. Además de la electrónica de consumo, Bluetooth también se utiliza en dispositivos médicos, sistemas automotrices y equipos industriales, donde la comunicación inalámbrica confiable es esencial. Comprender los tipos de dispositivos Bluetooth y sus aplicaciones es importante para reconocer las implicaciones de seguridad que conllevan.

Los dispositivos Bluetooth funcionan con diferentes conexiones, que se clasifican principalmente en *Bluetooth Classic* y *Bluetooth Low Energy* (BLE). Bluetooth Classic se utiliza para dispositivos que requieren conexiones continuas de alta velocidad, como la transmisión de audio a altavoces inalámbricos o la transferencia de archivos grandes entre teléfonos y computadoras. BLE, por otro lado, está optimizado para dispositivos que necesitan una comunicación intermitente con un bajo consumo de energía, lo que lo hace ideal para dispositivos IoT, rastreadores de actividad física y dispositivos domésticos inteligentes. Cada tipo de conexión viene con su propio conjunto de desafíos de seguridad. Por ejemplo, Bluetooth Classic puede ser más vulnerable a las *espionaje* durante la transferencia de datos, mientras que los dispositivos BLE, debido a su menor peso, pueden carecer de mecanismos de seguridad avanzados.

Desde el punto de vista de la seguridad, los dispositivos Bluetooth son propensos a diversos ataques. Una de las amenazas más comunes es el *bluejacking*, en el que un atacante envía mensajes o archivos no solicitados a un dispositivo habilitado con Bluetooth que se encuentre dentro del alcance. Si bien esto puede parecer inofensivo, puede dar lugar a ataques de phishing o a la difusión de enlaces maliciosos. Otro riesgo es el *bluesnarfing*, un ataque más grave en el que un atacante obtiene acceso no autorizado a los datos de un dispositivo, como contactos, mensajes u otra información confidencial, sin el consentimiento del usuario.

Un ataque más grave es la suplantación de identidad de un dispositivo Bluetooth, una variante del *ataque de intermediario* (man-in-the-middle). En este escenario, un atacante intercepta la comunicación entre dos dispositivos Bluetooth y se hace pasar por una de las partes. Esto le permite acceder, manipular o robar los datos que se transmiten entre los dispositivos. Dado que el alcance del Bluetooth es de aproximadamente diez metros, estos ataques suelen ocurrir en lugares

muy próximos, lo que los convierte en una amenaza importante en espacios públicos como aeropuertos, cafeterías y oficinas.

Otra vulnerabilidad importante en las conexiones Bluetooth está relacionada con el *emparejamiento*. Cuando los dispositivos se emparejan, intercambian claves de seguridad para establecer una conexión segura. Sin embargo, si el proceso de emparejamiento no está protegido adecuadamente, los atacantes pueden interceptar o manipular estas claves, obteniendo acceso no autorizado a los dispositivos. El emparejamiento público, en el que los dispositivos se emparejan en entornos abiertos o no seguros, es especialmente vulnerable a este tipo de ataque. Garantizar el uso de métodos de emparejamiento seguros, como la autenticación con *clave de acceso*, puede mitigar este riesgo.

Para protegerse contra estos riesgos, es importante seguir las mejores prácticas para proteger los dispositivos Bluetooth. En primer lugar, deshabilitar el Bluetooth cuando no se utiliza es una forma eficaz de evitar el acceso no autorizado.

Para las organizaciones, supervisar la actividad de Bluetooth en los dispositivos corporativos es un paso necesario para evitar el acceso no autorizado a datos confidenciales. Al restringir el uso de Bluetooth en entornos seguros e implementar herramientas que supervisen las comunicaciones inalámbricas, las empresas pueden minimizar los posibles riesgos asociados con los dispositivos Bluetooth. De manera similar, educar a los empleados sobre la importancia de proteger sus dispositivos Bluetooth personales en espacios públicos ayuda a reducir la exposición a ataques.

RFID

Comprender los dispositivos de identificación por radiofrecuencia (RFID), sus tipos, conexiones y aspectos de seguridad, es fundamental, ya que la tecnología RFID se utiliza ampliamente en sectores como el comercio minorista, la atención sanitaria, la logística y el control de acceso. Los dispositivos RFID facilitan la transferencia inalámbrica de datos entre una etiqueta y un lector, utilizando ondas de radio para identificar y rastrear objetos o personas. Si bien la RFID ofrece muchas ventajas en términos de eficiencia y automatización, también presenta riesgos de seguridad que deben abordarse.

Los dispositivos RFID se pueden clasificar en tres tipos principales: *pasivos*, *activos* y *semipasivos*. Las etiquetas RFID pasivas no tienen una fuente de alimentación interna; dependen de la energía transmitida por el lector RFID para encenderse y enviar sus datos. Este tipo de RFID se utiliza comúnmente en la gestión de inventario, el seguimiento minorista y el control de acceso. Las etiquetas RFID activas tienen una batería interna y pueden transmitir señales a distancias más largas. Suelen utilizarse cuando se requiere el seguimiento en tiempo real de activos o vehículos de alto valor, como en operaciones de logística o de almacén. Las etiquetas RFID semipasivas

también tienen una batería, pero la utilizan solo para alimentar circuitos internos; siguen dependiendo del lector RFID para la comunicación. Este tipo se utiliza cuando se necesita una lectura más fiable, especialmente en entornos con mucha interferencia.

Las conexiones entre dispositivos RFID se establecen de forma inalámbrica. El lector RFID emite ondas de radio que activan la etiqueta dentro de su alcance. A continuación, la etiqueta envía los datos al lector, que los procesa y los transmite a un sistema informático para su interpretación. Según la frecuencia utilizada, las conexiones RFID pueden variar desde unos pocos centímetros hasta varios metros. Los rangos de frecuencia más comunes incluyen *baja frecuencia* (LF), *alta frecuencia* (HF) y *ultra alta frecuencia* (UHF). La LF se utiliza normalmente para aplicaciones de corto alcance y baja cantidad de datos, como el seguimiento de animales, mientras que la HF se utiliza en tarjetas de proximidad y dispositivos habilitados para NFC. La UHF es el tipo más común para aplicaciones industriales y logísticas debido a su mayor alcance y capacidad para transmitir mayores cantidades de datos.

Al considerar los aspectos de seguridad de los dispositivos RFID, surgen varias vulnerabilidades potenciales. Uno de los riesgos más conocidos es la interceptación de comunicaciones. Debido a que las comunicaciones RFID se realizan de forma inalámbrica, un atacante con un receptor adecuado puede interceptar las señales transmitidas entre la etiqueta y el lector, lo que le permite capturar información confidencial, como números de tarjetas de crédito o datos de identificación personal. Esto es particularmente preocupante en aplicaciones como los sistemas de pago sin contacto, donde el acceso no autorizado a la información financiera puede dar lugar a fraudes.

Otra amenaza de seguridad común es la clonación. En un ataque de clonación, un atacante duplica los datos de una etiqueta RFID y crea una nueva etiqueta con la misma información. Esta etiqueta clonada puede utilizarse para obtener acceso no autorizado a áreas o sistemas restringidos, en particular en entornos en los que se utiliza RFID para el control de acceso.

El *skimming RFID* es otro método de ataque, en el que un atacante lee datos de una etiqueta sin el conocimiento o consentimiento del propietario. Los dispositivos de skimming suelen ser pequeños y portátiles, lo que permite a los atacantes leer etiquetas RFID en espacios concurridos, como el transporte público o los centros comerciales, sin ser detectados. Este riesgo es especialmente significativo para las tarjetas de crédito y los documentos de identificación habilitados con RFID, que pueden aprovecharse para el robo de identidad o el fraude financiero.

Para mitigar estos riesgos, se deben adoptar varias medidas de seguridad. Una de las más importantes es cifrar los datos que se transmiten entre las etiquetas RFID y los lectores. Esto garantiza que, incluso si los datos son interceptados, no puedan ser leídos ni utilizados fácilmente por un atacante.

Otra medida de seguridad eficaz es el uso de *escudos RFID* o *jaulas de Faraday* para bloquear las

señales RFID cuando las etiquetas no se utilizan. Estos escudos se utilizan a menudo en carteras o tarjeteros para proteger las tarjetas de crédito o los documentos de identidad con RFID de ser pirateados.

Por último, es fundamental actualizar y supervisar periódicamente los sistemas RFID. Al igual que cualquier otra tecnología, los dispositivos y lectores RFID deben mantenerse actualizados con los últimos parches de seguridad. El seguimiento de la actividad RFID, especialmente en entornos sensibles como almacenes, centros sanitarios y edificios seguros, ayuda a detectar comportamientos inusuales o intentos de acceso no autorizado en tiempo real.

Computación confiable

La computación confiable es un conjunto de tecnologías y estándares que mejoran la seguridad de los sistemas informáticos al garantizar que funcionen de manera fiable y predecible. La idea central es crear un entorno informático en el que los usuarios puedan confiar en que sus dispositivos están protegidos contra manipulaciones, accesos no autorizados y malware. La principal tecnología que permite esto es el módulo de *plataforma de confianza* (TPM), un componente de hardware especializado integrado en los dispositivos modernos que desempeña un papel fundamental en la protección del sistema desde su base.

Una de las funciones más importantes de computación confiable es el arranque seguro. El arranque seguro garantiza que el sistema se inicie utilizando únicamente software verificado y confiable. Durante el proceso de arranque, cada componente, desde el firmware hasta el sistema operativo, se verifica con una firma criptográfica. Si alguna parte del software ha sido alterada o reemplazada con código malicioso, el sistema se negará a arrancar.

La computación confiable también permite la *certificación remota*, que permite que un dispositivo demuestre a una parte remota que se encuentra en un estado confiable. Por ejemplo, en un escenario de computación en la nube, un servidor remoto puede usar la certificación para confirmar que un dispositivo cliente o una máquina virtual está ejecutando una versión confiable de software antes de otorgar acceso a recursos confidenciales.

Además de proteger la integridad del sistema y garantizar procesos de arranque seguros, la computación confiable desempeña un papel fundamental en la protección de datos confidenciales mediante el cifrado de datos. El TPM puede generar y gestionar claves de cifrado, lo que garantiza que las claves nunca abandonen el entorno de hardware seguro.

La computación confiable es un enfoque poderoso para proteger los sistemas informáticos modernos, proporcionando mecanismos para garantizar que los dispositivos y el software sean confiables y estén libres de manipulaciones.

Ejercicios guiados

1. Explique las posibles vulnerabilidades de seguridad del procesador, la memoria (RAM), los dispositivos de almacenamiento y los adaptadores de red. Para cada componente, proporcione un ejemplo real de una amenaza a la seguridad y sugiera una estrategia o solución para mitigar el riesgo.

2. Describa tres riesgos de seguridad comunes asociados con los dispositivos IoT. Además, explique dos prácticas recomendadas para mitigar estos riesgos. Por último, analice cómo la computación confiable y el módulo plataforma de confianza (TPM) pueden mejorar la seguridad de los dispositivos IoT.

Ejercicios exploratorios

1. Investiga cómo los diferentes sistemas operativos, como Windows, Linux y macOS, implementan mecanismos de arranque seguro.

2. Investigue un ejemplo real de un ataque de botnet de IoT, como el botnet Mirai.

Resumen

Esta lección destaca aspectos clave de la seguridad de hardware y dispositivos, centrándose en los componentes principales de computadoras, dispositivos inteligentes, IoT, USB, Bluetooth, RFID y computación confiable. Cada una de estas tecnologías presenta desafíos de seguridad únicos, desde vulnerabilidades del procesador y accesos no autorizados al almacenamiento hasta los riesgos asociados con los dispositivos inteligentes y de IoT, que a menudo están mal protegidos. Además, los dispositivos USB y Bluetooth son susceptibles a inyecciones de malware, transferencias de datos no autorizadas y ataques de intermediarios, mientras que los sistemas RFID enfrentan riesgos como la clonación y el skimming. La computación confiable a través del uso de tecnologías como el Módulo de plataforma segura (TPM), ayuda a garantizar la integridad del sistema, proteger los procesos de arranque y proteger los datos.

Respuestas a los ejercicios guiados

1. Explique las posibles vulnerabilidades de seguridad del procesador, la memoria (RAM), los dispositivos de almacenamiento y los adaptadores de red. Para cada componente, proporcione un ejemplo real de una amenaza de seguridad y sugiera una estrategia o solución para mitigar el riesgo.

   Los procesadores son vulnerables a los ataques de canal lateral, donde un atacante puede extraer datos confidenciales analizando el comportamiento del procesador. Estos ataques se pueden mitigar aplicando parches de hardware y actualizando el firmware del sistema. La memoria (RAM) enfrenta riesgos como los ataques de arranque en frío, donde los datos se recuperan después del apagado. Esto se puede mitigar utilizando el cifrado de memoria y borrando la RAM al apagar. Los dispositivos de almacenamiento, como los discos duros y SSD, son susceptibles al robo de datos, en particular cuando los datos no están cifrados. El cifrado de disco completo y las prácticas de borrado seguro son clave para proteger los datos de almacenamiento. Los adaptadores de red se pueden explotar en ataques de intermediario o mediante el rastreo de paquetes, donde se interceptan los datos transmitidos a través de las redes. El cifrado de las comunicaciones y la habilitación de firewalls son métodos efectivos para prevenir este tipo de ataques.

2. Describa tres riesgos de seguridad comunes asociados con los dispositivos IoT. Además, explique dos prácticas recomendadas para mitigar estos riesgos. Por último, analice cómo la computación confiable y el módulo de plataforma confiable (TPM) pueden mejorar la seguridad de los dispositivos IoT.

   Los dispositivos IoT enfrentan riesgos de seguridad, incluido el acceso no autorizado debido a la preservación de credenciales predeterminadas, ataques de botnet que utilizan dispositivos comprometidos en ataques DDoS a gran escala y violaciones de la privacidad de los datos causadas por transmisiones de datos inseguras. Para mitigar estos riesgos, es importante cambiar los nombres de usuario y las contraseñas predeterminadas en los dispositivos IoT y actualizar regularmente su firmware para corregir las vulnerabilidades. La computación confiable, en particular a través del uso del módulo de plataforma confiable (TPM), ayuda a proteger los dispositivos IoT al garantizar que inicien solo software confiable y al almacenar de forma segura las claves criptográficas, lo que protege los datos confidenciales y permite la certificación remota segura.

Respuestas a los ejercicios exploratorios

1. Investigue cómo los diferentes sistemas operativos, como Windows, Linux y macOS, implementan mecanismos de arranque seguro.

   Los mecanismos de arranque seguro varían según los sistemas operativos, pero generalmente dependen de componentes de hardware como TPM o UEFI para verificar la integridad del proceso de arranque. En Windows, el arranque seguro usa UEFI para garantizar que solo se cargue software confiable durante el inicio, empleando el TPM para almacenar claves criptográficas para la autenticación. Este enfoque es particularmente eficaz en entornos empresariales, ya que protege contra cargadores de arranque no autorizados y rootkits. Las distribuciones de Linux, como Ubuntu, también admiten el arranque seguro mediante UEFI, aunque la implementación puede diferir según la distribución. Es posible que los usuarios de Linux deban configurar manualmente los ajustes de arranque seguro para lograr compatibilidad con ciertos controladores o kernels personalizados. macOS usa un enfoque similar con su función de arranque seguro, que está estrechamente integrada con el chip de seguridad T2 de Apple. Esto garantiza que solo se pueda cargar software confiable firmado por Apple durante el inicio, lo que proporciona una capa sólida de seguridad contra la manipulación o el malware.

2. Investigue un ejemplo real de un ataque de botnet de IoT, como el botnet Mirai.

   El botnet Mirai es un ejemplo bien conocido de un ciberataque basado en IoT. Comprometió miles de dispositivos IoT, como cámaras y enrutadores, al explotar contraseñas débiles o predeterminadas. Mirai buscó dispositivos vulnerables en Internet, los infectó y formó un botnet capaz de lanzar ataques masivos de denegación de servicio distribuido (DDoS). El botnet interrumpió importantes sitios web y servicios, incluido Dyn, un proveedor de DNS, y afectó a plataformas importantes como Twitter, Netflix y Reddit.

023.2 Seguridad de aplicaciones

Referencia al objetivo del LPI

Security Essentials version 1.0, Exam 020, Objective 023.2

Peso

2

Áreas de conocimiento clave

- Comprensión de los tipos comunes de software
- Comprensión de diversas fuentes de aplicaciones y formas de adquirir e instalar software de forma segura
- Comprensión de las actualizaciones de firmware, sistemas operativos y aplicaciones
- Comprensión de fuentes para aplicaciones móviles
- Comprensión de las vulnerabilidades de seguridad comunes en el software
- Comprensión de los conceptos de software de protección local

Lista parcial de archivos, términos y utilidades

- Firmware, sistemas operativos, aplicaciones
- Tiendas de aplicaciones
- Filtros de paquetes locales, firewalls perimetrales y de capa de aplicación
- Desbordamientos de búfer, inyecciones SQL

Linux Professional Institute

Lección 1

Certificado:	Fundamentos de seguridad
Versión:	1.0
Tema:	023 Seguridad de dispositivos y almacenamiento
Objetivo:	023.2 Seguridad de aplicaciones
Lección:	1 de 1

Introducción

La seguridad del software es fundamental para mantener la integridad de los sistemas y los datos. Comienza por garantizar la instalación segura del software mediante la obtención de aplicaciones de proveedores confiables y evitando la introducción de código malicioso durante el proceso de instalación. Ya sea en una computadora de escritorio, un servidor o plataformas móviles. Cumplir con las mejores prácticas para la adquisición de software es esencial para evitar el acceso no autorizado o el malware. Además, la gestión de las actualizaciones de software es crucial, porque las actualizaciones y los parches regulares abordan las vulnerabilidades que podrían explotarse si no se aplican los parches.

Otro aspecto clave es la protección del software contra conexiones de red no deseadas. Esto implica el uso de herramientas como cortafuegos, filtros de paquetes y protección de puntos finales para garantizar que el software se comunique únicamente con redes y entidades autorizadas. Al proteger las instalaciones, garantizar actualizaciones oportunas y administrar las conexiones de red, las organizaciones pueden minimizar eficazmente los riesgos y mantener la integridad del software.

Tipos comunes de software y sus actualizaciones

En el campo de la informática y la ciberseguridad, es esencial comprender las categorías clave de software que forman la columna vertebral de los sistemas digitales. Estas categorías incluyen *firmware*, *sistemas operativos* y *aplicaciones*. Cada tipo cumple una función distinta para garantizar la funcionalidad, la facilidad de uso y la seguridad de un dispositivo o sistema.

El firmware es un software de bajo nivel integrado directamente en los dispositivos de hardware. Funciona como interfaz entre los componentes de hardware y el software de nivel superior, lo que garantiza que el hardware del sistema funcione correctamente. El firmware se almacena normalmente en una memoria no volátil y es esencial para arrancar el sistema y administrar los componentes de hardware, como la placa base, los discos duros y las interfaces de red.

Las actualizaciones de firmware son particularmente importantes porque una vulnerabilidad puede comprometer todo el dispositivo, ya que controla la comunicación entre el hardware y el software de nivel superior. Los fabricantes de hardware suelen publicar estas actualizaciones para solucionar problemas de seguridad, mejorar la compatibilidad con otros componentes de hardware o admitir nuevas funciones. Dado que el firmware es fundamental para el funcionamiento de un dispositivo, mantenerlo actualizado garantiza la integridad y la seguridad continua del sistema.

Un sistema operativo (SO) es el software principal que administra los recursos de hardware y software de una computadora. Algunos ejemplos son Windows, macOS y Linux, que proporcionan una interfaz de usuario y permiten que las aplicaciones se ejecuten en el sistema. El SO es responsable de administrar la memoria, la potencia de procesamiento, los sistemas de archivos y los dispositivos periféricos. La seguridad en los sistemas operativos es crucial, ya que actúan como la primera línea de defensa contra el acceso no autorizado y el malware.

Las actualizaciones del sistema operativo suelen incluir parches de seguridad para corregir vulnerabilidades conocidas, como las relacionadas con los protocolos de red, la gestión de la memoria o el control de acceso. Al garantizar que el sistema operativo esté actualizado, los usuarios reducen el riesgo de que sus sistemas sean explotados por malware u otros ataques. También es importante supervisar el ciclo de vida de un sistema operativo, ya que los sistemas más antiguos pueden dejar de recibir actualizaciones de seguridad críticas, lo que los deja vulnerables a los ataques.

Las aplicaciones son programas de software diseñados para realizar tareas específicas para el usuario, que van desde herramientas de productividad como procesadores de texto hasta navegadores web y plataformas de entretenimiento. Las aplicaciones dependen del sistema operativo para funcionar y ofrecen una amplia variedad de funcionalidades. Debido a su uso generalizado, las aplicaciones son un objetivo común de los ciberataques.

Las actualizaciones de aplicaciones se centran en corregir errores, mejorar la usabilidad y reparar vulnerabilidades en el software con el que los usuarios interactúan directamente. Estas actualizaciones pueden evitar riesgos de seguridad, como ataques de inyección, desbordamientos de búfer de memoria o acceso no autorizado a datos confidenciales. Mantener las aplicaciones actualizadas reduce la probabilidad de que se exploten estas vulnerabilidades.

Adquiera e instale software de forma segura

En la era digital, las aplicaciones de software se obtienen de una amplia gama de fuentes, por lo que es fundamental comprender dónde y cómo adquirir e instalar software de forma segura. La diversidad de fuentes, desde tiendas de aplicaciones oficiales hasta sitios web de terceros, puede presentar importantes riesgos de seguridad si no se maneja adecuadamente. Saber cómo verificar la legitimidad de una fuente de software y garantizar prácticas de instalación seguras son esenciales para prevenir infecciones de malware, violaciones de datos y acceso no autorizado.

Las *tiendas de aplicaciones* son una de las fuentes más comunes y confiables de aplicaciones de software, especialmente para dispositivos móviles. Plataformas como Apple App Store, Google Play Store y Microsoft Store ofrecen a los usuarios acceso a una gran colección de aplicaciones que han pasado por algún nivel de verificación de seguridad por parte del proveedor de la plataforma. Estas tiendas suelen emplear mecanismos para verificar la existencia de códigos maliciosos, lo que garantiza que las aplicaciones cumplan con ciertos estándares de seguridad antes de que estén disponibles al público. Sin embargo, si bien las tiendas de aplicaciones brindan un entorno más seguro para la adquisición de software, no son infalibles. Han habido casos en los que aplicaciones maliciosas se han escapado al proceso de verificación, por lo que es esencial que los usuarios verifiquen las calificaciones, las reseñas y los permisos de las aplicaciones antes de descargarlas.

En el caso de los entornos empresariales y de escritorio, el software se puede adquirir en sitios web de proveedores, distribuidores externos o sistemas de gestión de paquetes. Al descargar desde sitios web oficiales de proveedores, es importante verificar que la fuente sea legítima, a menudo comprobando los certificados HTTPS y las firmas digitales de los paquetes de software. El uso de gestores de paquetes confiables, como APT para sistemas Linux o el Administrador de paquetes de Windows de Microsoft, también puede garantizar que las aplicaciones provengan de repositorios confiables de forma segura.

Para instalar software de forma segura, los usuarios deben seguir las mejores prácticas, como evitar fuentes no confiables o desconocidas, verificar la integridad del software mediante hashes o firmas digitales y mantener actualizados sus sistemas y software de seguridad. Estos pasos ayudan a garantizar que no se instale software malicioso por accidente, lo que evita la posible vulneración de un sistema.

Fuentes para aplicaciones móviles

Las aplicaciones móviles se han convertido en una parte integral de nuestra vida diaria, desde herramientas de comunicación hasta aplicaciones de productividad y plataformas de entretenimiento. Sin embargo, el uso generalizado de aplicaciones móviles también genera importantes problemas de seguridad. Para garantizar que las aplicaciones que se instalan en los dispositivos móviles sean seguras y confiables, es fundamental comprender las distintas fuentes de aplicaciones móviles y los riesgos de seguridad asociados.

Las fuentes más comunes y seguras de aplicaciones móviles son las tiendas de aplicaciones oficiales, como Apple App Store y Google Play Store. Estas plataformas funcionan como repositorios centralizados donde los desarrolladores pueden distribuir sus aplicaciones, y ambas tiendas tienen procesos de verificación rigurosos para minimizar la distribución de software malicioso. Apple, en particular, mantiene un control estricto sobre la App Store, y exige que todas las aplicaciones pasen por un proceso de revisión que verifica el cumplimiento de los estándares de seguridad y las pautas de privacidad. De manera similar, Google Play Store analiza las aplicaciones en busca de malware y otras amenazas de seguridad mediante sistemas automatizados como Google Play Protect. Si bien estas tiendas de aplicaciones son generalmente seguras, ningún sistema es infalible y los usuarios siempre deben revisar las calificaciones de las aplicaciones, los permisos y la credibilidad del desarrollador antes de descargarlas.

Además de las tiendas de aplicaciones oficiales, las aplicaciones móviles pueden obtenerse de tiendas de aplicaciones o sitios web de terceros. Estas plataformas alternativas pueden ofrecer aplicaciones que no están disponibles en las tiendas oficiales, pero plantean riesgos de seguridad significativamente mayores. Las aplicaciones de fuentes de terceros a menudo no están sujetas al mismo nivel de escrutinio que las de las plataformas oficiales, lo que aumenta la probabilidad de descargar aplicaciones maliciosas o comprometidas. Los usuarios que eligen descargar desde estas fuentes deben ser conscientes de los posibles peligros y tomar precauciones adicionales, como analizar las aplicaciones con software antivirus y verificar la legitimidad de la fuente.

Otra forma de distribuir aplicaciones móviles es a través de tiendas de aplicaciones empresariales. Se trata de tiendas de aplicaciones privadas que suelen utilizarse dentro de las organizaciones para distribuir aplicaciones personalizadas desarrolladas para uso interno. Si bien las tiendas de aplicaciones empresariales pueden proporcionar acceso seguro a aplicaciones específicas de la empresa, requieren una gestión cuidadosa para garantizar que las aplicaciones se desarrollen, prueben y distribuyan de forma segura. Los empleados también deben recibir formación sobre cómo descargar e instalar estas aplicaciones de forma segura para evitar ataques accidentales.

 | Esta obra está bajo la licencia CC BY-NC-ND 4.0. |

Vulnerabilidades de seguridad comunes en el software

Las vulnerabilidades de software son fallas o debilidades en el código que los atacantes pueden explotar para comprometer la seguridad de un sistema. Dos de las vulnerabilidades más comunes y peligrosas son los desbordamientos de búfer y las inyecciones SQL. Estas vulnerabilidades han sido ampliamente explotadas y pueden tener consecuencias graves, como acceso no autorizado, violaciones de datos y fallas del sistema.

Un desbordamiento de búfer ocurre cuando un programa escribe más datos en un búfer (un área de almacenamiento de datos temporal) de los que esa área puede contener. Cuando esto sucede, los datos sobrantes pueden sobrescribir la memoria adyacente, lo que podría alterar el flujo de ejecución del programa. Los atacantes aprovechan los desbordamientos de búfer para inyectar código malicioso, obtener el control de un sistema o hacer que un programa se bloquee. Esta vulnerabilidad suele ser el resultado de una validación de entrada incorrecta o de la falta de comprobaciones de límites en el código. Para mitigar las vulnerabilidades de desbordamiento de búfer, los desarrolladores deben utilizar prácticas de codificación seguras, como la comprobación de límites y la validación de entrada, e implementar funciones de seguridad modernas como los canarios de pila y la aleatorización del diseño del espacio de direcciones (ASLR).

La inyección SQL es otra vulnerabilidad de seguridad común que ocurre en aplicaciones que interactúan con bases de datos. En este tipo de eventos, un atacante inyecta código SQL malicioso en un campo de entrada, manipulando la consulta de la aplicación a la base de datos. Si la entrada no se desinfecta correctamente, el atacante puede obtener acceso no autorizado a la base de datos, recuperar o alterar datos confidenciales o incluso ejecutar operaciones administrativas. Los ataques de inyección SQL son el resultado de una validación de entrada incorrecta y un uso insuficiente de declaraciones preparadas o consultas parametrizadas. Para defenderse contra la inyección SQL, los desarrolladores siempre deben desinfectar la entrada del usuario, utilizar consultas parametrizadas y evitar construir declaraciones SQL con entrada directa del usuario.

Software de protección local

El software de protección local desempeña un papel fundamental en la protección de los sistemas frente a una amplia gama de amenazas de seguridad, ya que controla el tráfico de red entrante y saliente, y filtra la actividad maliciosa. Esta protección suele proporcionarse mediante herramientas como *filtros de paquetes locales*, *cortafuegos (firewalls) perimetrales* y *de capa de aplicación*, cada uno de los cuales ofrece diferentes niveles de seguridad adaptados a las necesidades específicas de un sistema.

Los filtros de paquetes locales funcionan en la capa de red e inspeccionan los paquetes de datos individuales que se transmiten hacia o desde un sistema. Estos filtros deciden si permiten o bloquean los paquetes según reglas predefinidas, como direcciones IP, números de puerto o

protocolos. El filtrado de paquetes es una parte fundamental de la funcionalidad del firewall y ayuda a evitar el acceso no autorizado al detener los paquetes maliciosos antes de que puedan llegar a su destino. Si bien son eficaces para el control básico del tráfico, los filtros de paquetes pueden carecer de la capacidad de detectar ataques más sofisticados que ocurren en capas superiores de comunicación.

Los firewalls perimetrales están diseñados para proteger dispositivos individuales, como computadoras portátiles o de escritorio, actuando como una barrera entre el dispositivo y la red. Brindan una protección más integral que los filtros de paquetes básicos, ya que monitorean todo el tráfico que entra y sale del dispositivo, bloqueando la actividad maliciosa y evitando el acceso no autorizado. También pueden aplicar políticas de seguridad, como bloquear el acceso a la red de ciertas aplicaciones o evitar que se conecten dispositivos externos.

En el contexto del software de protección local, las funciones de un filtro de paquetes local y un firewall de punto final comúnmente se implementan juntas, proporcionando una capa integral de protección al filtrar el tráfico de red y aplicar políticas de seguridad directamente en dispositivos individuales.

Tanto Windows como macOS cuentan con firewalls integrados que proporcionan filtrado de paquetes y un firewall de punto final como parte de sus capacidades de seguridad generales. Esta doble funcionalidad garantiza que el acceso no autorizado y las actividades maliciosas se bloqueen de manera eficaz, lo que ofrece una defensa sólida.

Por ejemplo, *Windows Defender Firewall* supervisa y controla el tráfico en la capa de red, aplicando políticas de seguridad a nivel del dispositivo para evitar que las aplicaciones realicen acciones que violen esas políticas.

De manera similar, macOS cuenta con un firewall integrado que combina el filtrado de paquetes con las capacidades del firewall de punto final, lo que permite a los usuarios establecer reglas que regulen el tráfico entrante y saliente. macOS también proporciona opciones avanzadas como el registro y el modo oculto, que ayudan a evitar que el sistema sea detectado en una red, lo que mejora aún más la seguridad a nivel de dispositivo. Estas funciones brindan a los usuarios un mayor control sobre cómo sus dispositivos interactúan con la red, lo que garantiza una protección integral.

Iptables, ampliamente utilizado en sistemas Linux, funciona como una herramienta de filtrado de paquetes que permite a los usuarios definir reglas para administrar el tráfico de red entrante y saliente. Al operar en la capa de red, permite a los usuarios bloquear o permitir el tráfico en función de criterios como direcciones IP, números de puerto y protocolos. Iptables es altamente personalizable y ofrece opciones avanzadas para administrar la seguridad de la red, pero requiere una sólida comprensión de los conceptos de redes para una configuración adecuada.

Además, *SELinux* (Security-Enhanced Linux) desempeña un papel fundamental en la protección de los puntos finales en entornos Linux. Aunque no es un firewall tradicional, SELinux aplica *controles de acceso obligatorios* (MAC) que limitan las acciones que pueden realizar los procesos. Esto añade una capa adicional de seguridad al controlar cómo interactúan las aplicaciones con el sistema. Al gestionar estrictamente los permisos, SELinux ayuda a evitar que procesos no autorizados expongan en peligro el sistema, lo que lo convierte en un complemento valioso para los firewalls y otras herramientas de seguridad a la hora de garantizar la integridad del sistema.

Los *firewalls de capa de aplicación* funcionan a un nivel superior que los filtros de paquetes o los firewalls de punto final, inspeccionando el tráfico relacionado con aplicaciones o servicios específicos. Estos firewalls monitorean los datos intercambiados en la capa de aplicación, que es donde operan protocolos cruciales como HTTP, FTP o SMTP. Los firewalls de capa de aplicación brindan una inspección y un control más profundos, lo que permite a los administradores bloquear el tráfico según el tipo de aplicación o el contenido de los datos que se transmiten. Esto los hace muy efectivos contra ataques que apuntan a vulnerabilidades en las aplicaciones, como *cross-site scripting* (XSS), inyección SQL y desbordamiento de búfer.

Un ejemplo de un firewall de capa de aplicación es *ModSecurity*, que es un firewall de aplicación web (WAF) de código abierto que protege contra amenazas basadas en la web, como la inyección SQL y el ataque de secuencias de comandos entre sitios. Otro ejemplo es *F5 BIG-IP*, que incluye funciones avanzadas para gestionar el tráfico a nivel de aplicación y garantizar que las aplicaciones confidenciales estén protegidas contra ataques dirigidos.

Muchos proveedores de servicios en la nube ofrecen *firewalls de aplicaciones basados en la nube* para proteger las aplicaciones alojadas en sus plataformas.

Por ejemplo, AWS ofrece el *AWS Web Application Firewall* (AWS WAF), que brinda protección contra ataques web comunes al permitir que los usuarios definan reglas personalizadas para bloquear tipos específicos de tráfico. Google Cloud ofrece un servicio similar a través de su *Cloud Armor*, que ayuda a mitigar las vulnerabilidades de las aplicaciones y garantiza la protección contra ataques DDoS y de capa de aplicación. De manera similar, Microsoft Azure ofrece *Azure Web Application Firewall* (Azure WAF), que brinda protección centralizada para las aplicaciones alojadas en su plataforma en la nube al filtrar el tráfico malicioso antes de que llegue a la aplicación. Estos firewalls basados en la nube son altamente escalables, fáciles de integrar y ofrecen protección integral para aplicaciones web en entornos de nube.

Ejercicios guiados

1. ¿Cuál es la importancia de la instalación segura de software?

2. ¿Por qué es crucial para la seguridad la actualización periódica del software?

3. ¿Cómo la gestión de conexiones de red protege el software de amenazas?

 | Esta obra está bajo la licencia CC BY-NC-ND 4.0. |

Ejercicios exploratorios

1. ¿Qué sucede durante un desbordamiento de búfer?

2. ¿Cómo explotan los atacantes las vulnerabilidades de inyección SQL?

3. ¿En qué se diferencia un firewall de punto final de un filtro de paquetes?

Resumen

En esta lección se describen las prácticas esenciales para mantener la seguridad del software, centrándose en la instalación segura, las actualizaciones periódicas y la gestión de las conexiones de red. Se destaca la importancia de obtener el software de fuentes confiables para evitar el malware y garantizar que todo el software, incluidos el firmware, los sistemas operativos y las aplicaciones, se mantenga actualizado para corregir las vulnerabilidades. Además, la lección explica cómo los atacantes pueden explotar vulnerabilidades de software comunes, como desbordamientos de búfer e inyecciones SQL, y cómo las prácticas de codificación segura y la validación de entradas pueden mitigar estos riesgos.

La lección también examina el software de protección local, diferenciando entre filtros de paquetes locales, firewalls de puntos finales y firewalls de capa de aplicación, cada uno de los cuales ofrece distintos niveles de protección. Ejemplos como iptables, Firewall de Windows Defender y ModSecurity demuestran cómo estas herramientas protegen los sistemas filtrando el tráfico de red y evitando ataques específicos de la aplicación. También se analiza el papel de los firewalls basados en la nube, como los que ofrecen AWS, Google Cloud y Microsoft Azure, como elementos esenciales para proteger las aplicaciones alojadas en la nube de amenazas avanzadas.

 | Esta obra está bajo la licencia CC BY-NC-ND 4.0. |

Respuestas a los ejercicios guiados

1. ¿Cuál es la importancia de una instalación segura de software?

   Asegurarse de que el software se instala desde fuentes confiables ayuda a prevenir la introducción de código malicioso. Este proceso garantiza que el software que se instala sea legítimo y esté libre de amenazas de seguridad, lo que reduce el riesgo de acceso no autorizado o infecciones de malware.

2. ¿Por qué es fundamental para la seguridad la actualización periódica del software?

   Las actualizaciones y los parches de software son vitales porque solucionan vulnerabilidades que los atacantes podrían explotar. Las actualizaciones periódicas garantizan que se solucionen los fallos de seguridad, lo que ayuda a proteger los sistemas de amenazas conocidas.

3. ¿Cómo protege el software de amenazas la gestión de conexiones de red?

   Los firewalls, filtros de paquetes y protección de puntos finales garantizan que el software pueda comunicarse únicamente con redes autorizadas. Esto evita el acceso no autorizado y protege el software de ser comprometido por conexiones no deseadas, como tráfico entrante malicioso.

Respuestas a los ejercicios exploratorios

1. ¿Qué sucede durante un desbordamiento de búfer?

   Un desbordamiento de búfer ocurre cuando se escriben más datos en un búfer de los que puede contener, lo que provoca que se sobrescriba la memoria adyacente. Esto puede permitir que los atacantes inyecten código malicioso o bloqueen el sistema. Para evitarlo, los desarrolladores deben utilizar prácticas de codificación seguras, como la validación de entrada y las comprobaciones de límites, y emplear funciones de seguridad como los canarios de pila y ASLR.

2. ¿Cómo explotan los atacantes las vulnerabilidades de inyección SQL?

   La inyección SQL se produce cuando los atacantes insertan código SQL malicioso en los campos de entrada de una aplicación web, manipulando la base de datos para obtener acceso no autorizado a datos confidenciales o realizar operaciones destructivas. Esto se puede mitigar desinfectando las entradas del usuario y utilizando consultas parametrizadas, que evitan la manipulación directa de las instrucciones SQL.

3. ¿En qué se diferencia un firewall de punto final de un filtro de paquetes?

   Un firewall de punto final se diferencia de un filtro de paquetes en que proporciona una protección más integral para dispositivos individuales. Mientras que un filtro de paquetes solo inspecciona y filtra los paquetes de datos en función de reglas de capa de red predefinidas (por ejemplo, direcciones IP, puertos o protocolos), un firewall de punto final va más allá al monitorear y controlar todo el tráfico entrante y saliente específico del dispositivo. Los firewalls de punto final pueden aplicar políticas de seguridad más complejas, como bloquear aplicaciones no autorizadas, evitar que se conecten dispositivos externos y controlar a qué datos pueden acceder ciertos programas. Este nivel más profundo de inspección de tráfico y aplicación de políticas hace que los firewalls de punto final sean más efectivos para proteger sistemas individuales, en comparación con el control de tráfico más básico de los filtros de paquetes. Algunos ejemplos de firewalls de punto final incluyen el Firewall de Windows Defender y el firewall integrado de macOS.

023.3 Malware

Referencia al objetivo del LPI

Security Essentials version 1.0, Exam 020, Objective 023.3

Peso

3

Áreas de conocimiento clave

- Comprensión de los tipos comunes de malware
- Comprensión de los conceptos de rootkit y acceso remoto
- Comprensión de los escáneres de virus y malware
- Conocimiento del riesgo de malware utilizado para espionaje, exfiltración de datos y copias de libretas de direcciones

Lista parcial de archivos, términos y utilidades

- Virus, ransomware, malware troyano, adware, criptomineros
- Puertas traseras y acceso remoto
- Copia de archivos, registro de teclas, secuestro de cámara y micrófono

Lección 1

Certificado:	Fundamentos de seguridad
Versión:	1.0
Tema:	023 Seguridad de dispositivos y almacenamiento
Objetivo:	023.3 Malware
Lección:	1 de 1

Introducción

El término *malware* es una combinación de sílabas de las palabras *mal*-icious y soft-*ware*. Abarca una amplia gama de tipos de software cuyo objetivo final es comprometer un sistema informático o una red: virus, troyanos, ransomware, adware, etc. La mayoría de estos tipos (si no todos) también incluyen subtipos. Además, los ataques suelen ser más destructivos cuando contienen varias combinaciones de estos tipos de malware.

Las razones que se esconden detrás del malware son diversas y variadas: incluyen bromas y activismo, pero también espionaje, robo cibernético y otros delitos graves. En cualquier caso, la gran mayoría del malware está diseñado para ganar dinero de forma poco ética e ilegal. El malware puede entrar en su equipo o red a través de diversos medios: descargas de archivos, mensajes de correo electrónico con archivos adjuntos o enlaces sospechosos o visitas a un sitio web infectado, por nombrar solo algunos.

En esta lección se analizan los principios subyacentes de los diferentes tipos de malware (su *modus operandi*), el alcance de su daño potencial y cómo proteger sus máquinas contra ellos.

Tipos comunes de malware

Las siguientes subsecciones presentan algunos de los tipos más comunes de malware.

Virus

Tanto los virus biológicos como los virus informáticos necesitan un anfitrión para causar daño. Por lo tanto, un virus informático es un fragmento de código ejecutable malicioso que se instala en el equipo y tiene la capacidad de propagarse. A menudo, la propagación se lleva a cabo enviando un correo electrónico inicial que contiene el virus a todos los contactos de la libreta de direcciones de la víctima. Sin embargo, para causar estragos, el virus necesita la intervención humana. Por lo tanto, cuando el usuario desprevenido ejecuta el archivo host infectado, el virus se replica modificando programas o se propaga a otros equipos, lo que puede infectar una red completa.

El nivel de daño causado por los virus puede ser bastante devastador, ya que normalmente están diseñados para realizar prácticas desagradables como saturar una red con tráfico, corromper programas o eliminar archivos (o incluso el disco duro).

NOTE A diferencia de los virus, los gusanos no necesitan un archivo anfitrión infectado ni intervención humana para propagarse. Se los puede definir como un tipo de virus independiente.

Ransomware

Como su nombre indica, este tipo de malware consiste en retener la información del usuario como prisionera a cambio de un rescate. Normalmente, el malware funciona restringiendo el acceso de los usuarios a determinados archivos (o partes del ordenador) hasta que se le pague. A diferencia de los virus, los cibercriminales en un ataque de ransomware son claros con la víctima y le explican lo que ha ocurrido así como los pasos a seguir para recuperar la información perdida.

El ransomware suele utilizar criptografía de clave pública y una clave simétrica para cifrar los archivos afectados. Estos archivos se vuelven inaccesibles para sus legítimos propietarios; los archivos solo pueden descifrarse con la clave privada del atacante. La víctima recibe un mensaje con instrucciones sobre cómo pagar el rescate. Por lo tanto, los atacantes supuestamente entregarán la clave privada al usuario solo cuando pague el rescate. Al igual que ocurre con los virus, el ransomware puede escalar rápidamente y derribar organizaciones enteras al propagarse por las redes y atacar servidores de archivos y bases de datos.

NOTE Para proteger su identidad, los cibercriminales del ransomware normalmente piden el pago en forma de moneda virtual (por ejemplo, Bitcoin).

Criptomineros / Criptojacking

Los *criptomineros* maliciosos están diseñados para aprovecharse subrepticiamente de la actividad inactiva del CPU (o GPU). Como se ejecutan en segundo plano, pueden ser difíciles de detectar. Por lo tanto, el software malicioso se instala en secreto en su dispositivo (o navegador web) y comienza a minar criptomonedas. Aunque la minería se lleva a cabo sin que las víctimas se den cuenta, generalmente informan de un aumento de la actividad del ventilador u otros signos de trabajo intenso del procesador, como sobrecalentamiento o reducción del rendimiento.

Rootkits y acceso remoto

Los *rootkits* son una variedad de programas maliciosos que tienen como objetivo proporcionar a los cibercriminales acceso y control remotos sin que la víctima los detecte. Los rootkits suelen incluir un conjunto de herramientas para robar contraseñas, así como información bancaria o personal. De ahí el término: root (los atacantes obtienen acceso root) y kit (utilizan un conjunto de herramientas).

Existen distintos tipos de rootkits diseñados para atacar distintas partes del ordenador: el kernel, las aplicaciones, el firmware, el sistema de arranque (bootkits) o incluso la RAM.

Spyware

El término spyware se refiere a cualquier tipo de malware diseñado para monitorear la actividad de su computadora y, en la mayoría de los casos, también para robar información personal o confidencial: sus credenciales, información de pago, historial de navegación, etc. Los tipos más comunes de spyware incluyen adware, keylogger y secuestro de cámara y micrófono.

Adware

El término adware, que normalmente se produce en un navegador web, es un tipo de malware diseñado para bombardear su pantalla con anuncios. La mayoría de los programas espía su comportamiento en línea para dirigirse a usted con anuncios específicos. Para engañarlo y lograr que lo instale en su equipo, el adware puede camuflarse como software legítimo; sin embargo, también puede instalarse a través de una vulnerabilidad del navegador web.

Una vez instalado en su sistema, el adware generalmente se reconoce por signos como los siguientes: aparecen nuevas barras de herramientas en su navegador, los enlaces a sitios web lo llevan websites equivocados, su navegador web es más lento, la página de inicio de su navegador web cambia, etc.

Keylogging

El término keylogging se explica por sí solo. Un keylogger es un tipo de malware que registra las pulsaciones del teclado en un archivo que luego se envía a un tercero a través de Internet. Obviamente, los cibercriminales pueden dañar gravemente a la víctima al interceptar información vulnerable como contraseñas, códigos PIN o números de cuenta bancaria.

El objetivo de los keyloggers es pasar desapercibidos a los ojos de la víctima para evitar ser detectados antes de que se produzca el daño.

NOTE Los keyloggers pueden estar basados en hardware o en software. Asimismo, pueden utilizarse como una herramienta de monitoreo legítima.

Secuestro de cámara y micrófono (hijacking)

Este tipo de malware *hijacking* está diseñado para obtener acceso no autorizado a sus micrófonos y cámaras (tanto integrados como externos). De esta forma, su imagen y conversaciones pueden ser grabadas sin su consentimiento. Esto puede conducir a numerosos objetivos maliciosos y tener consecuencias muy desagradables: se interceptan datos confidenciales a través de grabaciones de audio, se graban videos y se venden a sitios web sospechosos, etc.

Caballos de Troya

Según la Odisea de Homero o la Eneida de Virgilio, los griegos ganaron la guerra de Troya gracias a la astucia y el engaño: en lugar de derribar las murallas de la ciudad de Troya, idearon un caballo de madera gigante que dejaron a las puertas de la ciudad. Los crédulos troyanos llevaron el caballo a la ciudad, y para su sorpresa, descubrieron que los soldados griegos habían estado escondidos en su interior todo el tiempo. Siguiendo la analogía de esta mitología griega, un caballo de Troya (o, simplemente, un troyano) es un programa malicioso que viaja sin ser detectado bajo la apariencia de software o contenido legítimo, como archivos de vídeo o audio (o cualquier otro tipo de contenido). De hecho, más que un programa malicioso, los troyanos pueden definirse como una estrategia de propagación multipropósito para cualquier tipo de malware que los cibercriminales quieran utilizar (virus, gusanos, ransomware, etc.).

Métodos comunes utilizados por los cibercriminales para causar estragos

Las siguientes subsecciones presentan un par de métodos utilizados por los ciberdelincuentes para ejecutar o implementar algunos (si no todos) los tipos de malware que acabamos de describir en las secciones anteriores.

Backdoors

Podemos definir una puerta trasera como una forma de acceder a un sistema informático que elude el protocolo legal preestablecido diseñado para ello (de forma muy similar a cómo las personas a veces utilizan puertas traseras reales para evitar ser vistas entrando en edificios en el mundo real). En otras palabras: un intruso accede al sistema eludiendo cualquier medida de seguridad. Pero, ¿las puertas traseras se crean intencionalmente o simplemente por casualidad? Bueno, ambas cosas; veámoslas.

En primer lugar, hay que tener en cuenta que el software en general, especialmente el que implica acceso remoto, tiene vulnerabilidades, por lo que los cibercriminales se esfuerzan mucho en detectar las denominadas vulnerabilidades de día cero (*zero-day vulnerabilites*). Como su nombre indica, estas vulnerabilidades se detectan el mismo día que se lanza el software y son realmente peligrosas porque aún no existen parches o soluciones para contrarrestar el daño potencial. Así, por ejemplo, un puerto podría quedar desprotegido sin darse cuenta y, de ser descubierto, proporcionar una puerta trasera a los intrusos.

En segundo lugar, los cibercriminales podrían intentar crear una puerta trasera ellos mismos. Para ello, podrían recurrir a la ingeniería social e intentar convencer a la víctima de que instale un programa aparentemente útil que contenga el malware que puede establecer la puerta trasera (creando un túnel entre su ordenador y el de la víctima).

Por último, pero no menos importante, los propios fabricantes y desarrolladores pueden crear y colocar puertas traseras en sus productos por una variedad de razones (una de ellas es garantizar el acceso al sistema en cualquier momento).

Entre las cosas desagradables más comunes para las que se pueden utilizar las puertas traseras, podemos nombrar las siguientes:

- Entrega de malware: troyanos, keyloggers, etc.
- Espionaje, es decir, robo de información sensible que puede llevar al robo de identidad o la realización de transacciones fraudulentas, etc.
- Secuestro de servidores
- Desfiguración de sitios web

NOTE

La *desfiguración de sitios web* (o *desfiguración web*) se puede definir como un ataque contra un sitio web en el que los cibercriminales reemplazan parte de su contenido con el de ellos (por ejemplo, la página de inicio se reemplaza por un mensaje que dice “Este sitio ha sido hackeado”).

Exfiltración de datos

La exfiltración de datos se refiere a cualquier transferencia no autorizada de datos desde un sistema de información. Una de las formas más comunes de exfiltración de datos implica el descifrado del sistema de resolución de DNS. En tal caso, los pasos son los siguientes:

1. Se lleva a cabo un ataque de phishing: se envía un mensaje de correo electrónico que contiene un fragmento de malware incrustado en un documento.
2. La víctima abre el mensaje de correo electrónico. Se ejecuta el código malicioso y se crea un canal de comando y control a través del resolutor DNS.
3. El malware comienza a propagarse hasta que encuentra datos confidenciales para exfiltrarlos. Luego, los datos se envían a un servidor externo.

NOTE

DNS significa *Sistema de nombres de dominio* y juega un papel muy importante en Internet, ya que se encarga de traducir los nombres de host en direcciones IP.

Cómo entra el malware en una computadora y qué hacer para protegerse

Como ya hemos visto, el malware puede llegar a tu equipo de múltiples formas: cuando un usuario hace clic en enlaces de mensajes de correo electrónico engañosos o ventanas emergentes de sitios web, al abrir archivos adjuntos, inserta una unidad USB, etc. Los criptomineros, también pueden llegar simplemente visitando un sitio web. Por ejemplo, un fragmento de JavaScript malicioso que se ha incrustado previamente en un sitio web para que todos los usuarios que lo visiten comiencen a realizar criptominería. Del mismo modo, los virus (y otros tipos de malware) pueden hacer copias de archivos críticos en el sistema para evitar ser detectados.

Los troyanos suelen distribuirse mediante algún tipo de método de ingeniería social. Normalmente, la víctima recibe un mensaje de correo electrónico de phishing con un archivo adjunto que contiene el fragmento de código malicioso. En cuanto hace clic en este, se ejecuta el código malicioso.

NOTE

La ingeniería social es un término general que hace referencia a prácticas sociales ilegítimas para obtener información confidencial. El phishing es un tipo de técnica de ingeniería social en la que un atacante envía un mensaje de correo electrónico falso a la víctima para engañarla y conseguir que revele información confidencial o sensible. Dentro del phishing, podemos encontrar ataques más específicos como el phishing de tipo spear (dirigido a un individuo en particular) o el phishing de tipo whaling (dirigido a personas de alto rango dentro de una empresa).

Existen varias formas de protegerse contra el malware:

- Utilice software antivirus y antimalware (escáneres, etc.).
- Mantenga todo el software (antimalware y otros) actualizado en todo momento.
- Limite el acceso a los datos.
- Ejecute programas en un entorno virtual (*sandboxing*).
- Analice correos electrónicos y archivos adjuntos en busca de malware.
- No descargue ni instale archivos ejecutables de fuentes no confiables.
- Esté atento a señales de correo electrónico de phishing (nombres de dominio extraños, errores gramaticales, errores tipográficos, etc.).
- Realice copias de seguridad de los dispositivos y datos importantes de forma regular.
- Fortalezca sus sistemas de autenticación.

NOTE

El kernel Linux viene con un potente cortafuegos (firewall), *iptables*, y algunas distribuciones tiene sus propias interfaces fáciles de usar (Por ejemplo, Ubuntu incluye *Gufw*). Asimismo, *nmap* (un escáner de red) se ofrece en los repositorios de todas las principales distribuciones de GNU/Linux y se puede utilizar para proteger las redes contra algunos tipos de malware. Hay muchas otras soluciones anti-malware disponibles para Linux, pero eso queda fuera del alcance de esta lección.

 Esta obra está bajo la licencia CC BY-NC-ND 4.0. |

Ejercicios guiados

1. Considere los siguientes síntomas e indique a qué tipo de malware pertenecen con mayor probabilidad:

Síntoma	**Tipo de malware**
Su computadora se calienta demasiado mientras navega por Internet.	
Observa una nueva barra de herramientas en su navegador que no ha instalado.	
Un mensaje de correo electrónico que no ha escrito se envía a todos los usuarios de su libreta de direcciones.	
No puede acceder a sus archivos porque han sido cifrados.	
Encuentra fotos suyas no autorizadas en Internet.	

2. Indique si las siguientes acciones son prácticas de riesgo o medidas de protección:

Acción	**Práctica de riesgo o medida de protección**
Limitar el acceso a los datos	
Instalar un archivo ejecutable de una fuente no confiable	
Hacer clic en una ventana emergente	
Instalar las últimas actualizaciones del sistema	
Insertar una memoria USB sospechosa en su computadora	
Realizar copias de seguridad periódicamente	
Enviar la información de su tarjeta de crédito por correo electrónico	

3. ¿En qué tipo de ataque recibes un mensaje de correo electrónico fraudulento que parece provenir de fuentes confiables (tu banco, redes sociales, familiares o conocidos, un superior de

tu empresa)?

4. ¿Qué término define al malware que se hace pasar por software (o contenido) legítimo?

5. ¿Qué tipo de malware registra de forma encubierta las teclas que presionas en tu teclado?

Ejercicios exploratorios

1. Supongamos que el micrófono de su dispositivo ha sido hackeado y los cibercriminales interceptan información personal sobre usted. ¿Cómo podrían utilizar esta información para acceder a sus servicios en línea?

2. El software antivirus utiliza la detección basada en firmas para identificar malware. ¿Qué queremos decir con los términos *firma de virus* o *definición de virus*?

3. Busque en la web los siguientes términos y explique su significado:
   a. Autenticación de dos factores (o multifactor):
   b. Botnet:

Resumen

En esta lección, aprendió qué es el malware, sus distintos tipos y cómo funcionan. También exploró las diferentes formas en que el malware puede infiltrarse en su computadora y cómo proteger eficazmente su sistema de ataques de malware.

 Esta obra está bajo la licencia CC BY-NC-ND 4.0. |

Respuestas a los ejercicios guiados

1. Considere los siguientes síntomas e indique a qué tipo de malware pertenecen con mayor probabilidad:

Síntoma	**Tipo de malware**
Su computadora se calienta demasiado mientras navega por Internet.	Criptominería
Observa una nueva barra de herramientas en su navegador que no ha instalado.	Adware
Un mensaje de correo electrónico que usted no ha escrito se envía a todos los contactos de su libreta de direcciones.	Virus
No puede acceder a sus archivos porque han sido cifrados.	Ransomware
Encuentra fotos suyas no autorizadas en Internet.	Secuestro de cámara

2. Indique si las siguientes acciones son prácticas de riesgo o medidas de protección:

Acción	**Práctica de riesgo o medida de protección**
Limitar el acceso a los datos	Medida de protección
Instalar un archivo ejecutable de una fuente no confiable	Práctica riesgosa
Hacer clic en una ventana emergente	Práctica riesgosa
Instalar las últimas actualizaciones del sistema	Medida de protección
Insertar una memoria USB sospechosa en el ordenador	Práctica riesgosa
Realizar copias de seguridad periódicamente	Medida de protección
Enviar la información de su tarjeta de crédito por correo electrónico	Práctica riesgosa

3. ¿En qué tipo de ataque recibes un mensaje de correo electrónico fraudulento que parece provenir de fuentes confiables (tu banco, redes sociales, familiares o conocidos, un superior de

tu empresa)?

Ataque de phishing

4. ¿Qué término define al malware que se hace pasar por software (o contenido) legítimo?

   Caballos de Troya

5. ¿Qué tipo de malware registra de forma encubierta las teclas que pulsas en tu teclado?

   Keyloggers

Respuestas a los ejercicios exploratorios

1. Supongamos que el micrófono de su dispositivo ha sido pirateado y los cibercriminales interceptan información personal sobre usted. ¿Cómo podrían utilizar esta información para acceder a sus servicios en línea?

   Recordemos que algunos servicios en línea hacen uso de *preguntas de seguridad* en caso de que haya olvidado su contraseña. Por lo tanto, los cibercriminales podrían iniciar sesión en su servicio respondiendo correctamente a preguntas como cuál es el nombre de su mascota o de qué color son sus ojos.

2. La detección basada en firmas es utilizada por el software antivirus para identificar malware. ¿Qué queremos decir con los términos *firma de virus* o *definición de virus*?

   La firma de virus o definición de virus se refiere a la huella digital del virus, es decir, el conjunto de datos únicos que permiten al software antivirus identificarlo.

3. Busque en la web los siguientes términos y explique su significado:

   a. Autenticación de dos factores (o multifactor):

      La autenticación de dos factores (2FA) o la autenticación multifactor (MFA) son formas de proporcionar capas adicionales de seguridad al proteger las cuentas de usuario.

   b. Botnet:

      Podemos definir una botnet como una red de computadoras infectadas (“bots”) utilizadas para realizar ataques masivos como denegación de servicio distribuida (DDOS), etc.

023.4 Disponibilidad de datos

Referencia al objetivo del LPI

Security Essentials version 1.0, Exam 020, Objective 023.4

Peso

2

Áreas de conocimiento clave

- Comprensión de la importancia de las copias de seguridad
- Comprensión de los tipos y estrategias de copia de seguridad más comunes
- Comprensión de las implicaciones de las copias de seguridad
- Creación y almacenamiento seguro de copias de seguridad
- Comprensión del almacenamiento, acceso y uso compartido de datos en servicios en la nube
- Comprensión de las implicaciones de seguridad del almacenamiento en la nube y el acceso compartido en la nube
- Conocimiento de la dependencia de la conexión a Internet y la sincronización de datos entre los servicios en la nube y el almacenamiento local

Lista parcial de archivos, términos y utilidades

- Copias de seguridad completas, diferenciales e incrementales
- Retención de copias de seguridad
- Servicios en la nube para compartir archivos

Lección 1

Certificado:	Fundamentos de seguridad
Versión:	1.0
Tema:	023 Seguridad de dispositivos y almacenamiento
Objetivo:	023.4 Disponibilidad de datos
Lección:	1 de 1

Introducción

En el mundo digital actual, los datos son el elemento vital de muchas actividades, ya sea para fines personales, académicos o comerciales. Garantizar la disponibilidad de los datos es fundamental, ya que la pérdida de datos puede ser catastrófica. Esta lección le guiará a través de los conceptos esenciales de la disponibilidad de datos, incluidas las copias de seguridad y el almacenamiento en la nube.

La importancia de las copias de seguridad

La pérdida de datos puede ocurrir por diversas razones, como fallas de hardware, de software, errores humanos o incluso ataques cibernéticos. Las copias de seguridad son copias de sus datos que se pueden utilizar para restaurarlos en caso de pérdida o daño. A continuación, se indican algunas razones clave por las que las copias de seguridad son esenciales.

Las copias de seguridad le permiten recuperar sus datos de forma rápida y eficaz en caso de eventos inesperados, como fallos de hardware, accidentes o ciberataques. Las copias de seguridad funcionan como una red de seguridad para sus datos.

Las copias de seguridad ayudan a mantener la integridad de sus datos, garantizando que permanezcan intactos y sin daños.

Para la continuidad del negocio, las copias de seguridad son fundamentales para mantener las operaciones y evitar tiempos de inactividad. Perder información de clientes o inventario podría ser fatal para una empresa, por lo que las copias de seguridad son esenciales.

Es necesario que una organización cuente con un buen plan de copias de seguridad. Se debe desarrollar un plan de copias de seguridad para determinar qué datos es importante conservar y con qué frecuencia se deben copiar dicha información.

Tipos y estrategias de copia de seguridad más comunes

Para implementar eficazmente un plan de respaldo, es fundamental considerar varios tipos y estrategias de respaldo además de establecer un cronograma consistente basado en la criticidad de sus datos y la frecuencia de cambio.

Una *copia de seguridad completa* copia todos los datos en un momento específico y permite recuperarlos por completo. Normalmente, la primera copia de seguridad de un sistema será completa. Si bien este método ofrece la opción de recuperar completamente todo, requiere mucho tiempo y un espacio de almacenamiento considerable. Las copias de seguridad completas suelen realizarse con menos frecuencia debido a las demandas de tiempo y recursos que requieren, pero suelen utilizarse como base para otros tipos de copias de seguridad.

Las *copias de seguridad incrementales* copian únicamente los datos que han cambiado desde la última copia de seguridad, ya sea una copia de seguridad completa o incremental. Este método es eficiente en términos de almacenamiento y tiempo, ya que requiere menos espacio y un procesamiento más rápido. Sin embargo, durante la restauración, se necesita la última copia de seguridad completa y todas las copias de seguridad incrementales posteriores, lo que puede hacer que la recuperación sea más compleja.

Una *copia de seguridad diferencial* guarda todos los cambios realizados desde la última copia de seguridad completa, independientemente de si se han realizado copias diferenciales anteriores. Este método requiere más espacio que las copias de seguridad incrementales, pero simplifica el proceso de restauración, ya que solo se necesitan la última copia de seguridad completa y la copia de seguridad diferencial más reciente.

Las *copias de seguridad instantáneas* capturan el estado de un sistema en un momento específico. A diferencia de las copias de seguridad tradicionales basadas en archivos, las instantáneas se pueden tomar rápidamente y ofrecen una recuperación casi instantánea al revertir el sistema a un estado anterior. Sin embargo, las instantáneas requieren sistemas de almacenamiento más

avanzados y es posible que no ofrezcan las mismas opciones de recuperación granular que otros métodos.

Escenarios de ejemplo

Comprender cuándo se debe utilizar una copia de seguridad diferencial o incremental después de una copia de seguridad completa es un aspecto importante de un plan de respaldos. Para ilustrar las diferencias entre las copias de seguridad diferenciales e incrementales, compare los siguientes escenarios.

Restauración de datos desde copias de seguridad completas e incrementales

Imaginemos a una administradora de TI llamada Emma que trabaja para una empresa de comercio electrónico de tamaño mediano. La base de datos de la empresa contiene información crítica sobre los pedidos de los clientes y realizan copias de seguridad periódicas para garantizar la disponibilidad de los datos.

El domingo por la noche, Emma inicia una copia de seguridad completa de toda la base de datos, capturando todos los pedidos de clientes y los datos del inventario de productos.

De lunes a sábado, se programan copias de seguridad incrementales a diario. Estas copias de seguridad capturan solo los datos que han cambiado desde la última copia de seguridad. Cada día, la base de datos experimenta actualizaciones menores debido a nuevos pedidos de clientes y adiciones de productos.

El miércoles se produce un fallo de hardware y algunos datos de la base de datos se corrompen. Los pedidos de los clientes realizados el miércoles por la mañana se pierden.

Para restaurar los datos perdidos, Emma comienza utilizando la copia de seguridad completa más reciente, que se realizó el domingo. Esta copia de seguridad contiene los datos de referencia. A continuación, Emma aplica las copias de seguridad incrementales del lunes, martes y miércoles. Este proceso garantiza que la base de datos esté actualizada y, al mismo tiempo, minimiza la cantidad de datos transferidos y el tiempo necesario para la restauración.

Al restaurar desde la copia de seguridad completa y aplicar las copias de seguridad incrementales, Emma recupera con éxito los datos perdidos, garantizando que todos los pedidos de los clientes y la información del producto estén intactos hasta el momento de la falla del hardware el miércoles.

Restauración de datos desde copias de seguridad completas y diferenciales

Ahora, consideremos un escenario diferente que involucra a la misma empresa de comercio electrónico y la administradora de TI Emma, pero esta vez utilizan una estrategia de respaldo

diferencial.

El domingo por la noche, Emma inicia una copia de seguridad completa de toda la base de datos, capturando todos los pedidos de clientes y los datos del inventario de productos.

A lo largo de la semana, Emma programa copias de seguridad diferenciales a diario. Estas copias de seguridad capturan todos los cambios de datos desde la última copia de seguridad completa.

El miércoles, se produce una corrupción en la base de datos debido a un fallo del software, lo que provoca la pérdida de datos.

Para restaurar los datos perdidos, Emma comienza utilizando la copia de seguridad completa más reciente realizada el domingo por la noche. Esta copia de seguridad completa contiene los datos de referencia. Luego, Emma aplica solo la última copia de seguridad diferencial del miércoles. Dado que las copias de seguridad diferenciales capturan todos los cambios desde la última copia de seguridad completa, solo se necesita la copia de seguridad diferencial más reciente.

Al restaurar desde la copia de seguridad completa y aplicar la copia de seguridad diferencial más reciente, Emma recupera con éxito los datos perdidos, lo que garantiza que todos los pedidos de clientes y la información de productos se restablezcan hasta el momento en que se produjo la falla del software el miércoles. Este método simplifica el proceso de restauración porque requiere restaurar solo la copia de seguridad completa y la copia de seguridad diferencial más reciente, a diferencia de las copias de seguridad incrementales que requerirían aplicar varias copias de seguridad en secuencia.

Retención de copias de seguridad

Una buena *política de retención* de copias de seguridad es esencial para una gestión eficaz de los datos y una planificación de la recuperación ante desastres. Define durante cuánto tiempo se conservan las copias de seguridad y en qué condiciones se eliminan. El objetivo de una política de retención bien diseñada es equilibrar la disponibilidad de los datos, los requisitos de cumplimiento, los costos de almacenamiento y la eficiencia operativa. A continuación, se presentan algunos componentes clave de una buena política de retención de copias de seguridad.

En primer lugar, los datos se clasifican en función de su importancia y se establecen períodos de uso y retención para diferentes categorías de datos (por ejemplo, las copias de seguridad diarias pueden conservarse durante 7 a 30 días para la recuperación operativa, las copias de seguridad semanales pueden conservarse durante 4 a 12 semanas para la recuperación a corto plazo, y las copias de seguridad mensuales o anuales pueden conservarse para fines de archivo a largo plazo).

Para garantizar el cumplimiento de las regulaciones específicas de la industria (por ejemplo, GDPR, HIPAA) que exigen períodos de retención de datos, se debe consultar a los equipos legales y

de cumplimiento para alinear las políticas de retención con los requisitos legales.

Otro aspecto a tener en cuenta es la granularidad de las copias de seguridad que se conservarán. Por ejemplo, puede conservar copias de seguridad cada hora de las últimas 24 horas, copias de seguridad diarias de la semana anterior y copias de seguridad semanales del año anterior.

Una organización también puede mantener múltiples versiones de copias de seguridad, especialmente de datos críticos, para permitir la recuperación en un momento determinado.

Dada la vida útil limitada de la mayoría de las copias de seguridad, los procesos automatizados pueden facilitar la eliminación de las copias de seguridad una vez que alcanzan los períodos de retención especificados. Esto ayuda a evitar errores manuales y garantiza el cumplimiento.

El almacenamiento externo para copias de seguridad a largo plazo protege contra desastres como incendios, inundaciones y fallas de hardware.

Es importante probar periódicamente el proceso de restauración de copias de seguridad con diferentes períodos de retención para garantizar que los datos se puedan recuperar con éxito.

La política de retención de copias de seguridad debe comunicarse claramente a todas las partes interesadas relevantes, incluido el personal de TI, los propietarios de datos y la administración.

Las partes interesadas también deben revisar y ajustar periódicamente la política de retención para alinearla con las necesidades comerciales cambiantes, los requisitos de cumplimiento y los avances tecnológicos.

Se debe crear y mantener una documentación completa de la política de retención de copias de seguridad, incluidos detalles sobre los períodos de retención, la clasificación de datos y las consideraciones de cumplimiento.

Las políticas de respaldo también necesitan procesos para gestionar excepciones, como extender los períodos de retención de datos específicos debido a investigaciones legales o litigios.

Los mecanismos de monitoreo y presentación de informes pueden garantizar el cumplimiento de la política y alertar a los administradores sobre posibles problemas o violaciones.

Una buena política de retención de copias de seguridad debe lograr un equilibrio entre la disponibilidad de los datos y los costos de almacenamiento, a la vez que se adhiere a los requisitos legales y de cumplimiento normativo. La revisión y actualización periódicas de la política garantizan que siga siendo eficaz para satisfacer las necesidades cambiantes de la organización.

Implicaciones de seguridad de las copias de seguridad

Las copias de seguridad deben tratarse con el mismo nivel de seguridad que los datos primarios.

Por lo tanto, deben cifrarse para protegerlos del acceso no autorizado.

El control de acceso garantiza que solo el personal autorizado tenga acceso a las copias de seguridad. Según la organización, puede resultar útil mantener un registro de quién accede a las copias de seguridad y cuándo. Este archivo de registro se puede auditar periódicamente para garantizar el cumplimiento de la política de copias de seguridad.

Se crea una resiliencia adicional al almacenar las copias de seguridad en una ubicación separada para protegerse contra desastres físicos como incendios o robos. Existen empresas de terceros que se encargan de tomar las copias de seguridad físicas (generalmente escritas en cinta) y almacenarlas en una ubicación externa con acceso restringido y climatizada. Este tipo de servicio puede ser costoso y normalmente lo emplean las grandes empresas. Todos los datos almacenados fuera de las instalaciones deben estar cifrados como medida de precaución contra el robo de datos.

Las copias de seguridad basadas en la nube o externas deben seguir protocolos de seguridad estrictos, incluido el cifrado, el control de acceso y el cumplimiento de las normas de protección de datos.

Las estrategias de respaldo resistentes a los ataques de ransomware incluyen el uso de almacenamiento inmutable o copias de seguridad con espacio de aire para garantizar que los datos permanezcan seguros en caso de una infección.

Creación y almacenamiento seguro de copias de seguridad

Las siguientes prácticas ayudan a crear y almacenar copias de seguridad de forma segura.

Los factores que se deben tener en cuenta al elegir un software o servicio de copia de seguridad incluyen la cantidad de sistemas que una solución puede respaldar y la facilidad para restaurar las copias de seguridad. Algunas soluciones de copia de seguridad ofrecen la posibilidad de realizar copias de seguridad de versiones anteriores, lo que permite acceder a versiones anteriores de archivos o datos y restaurarlas. La sincronización ayuda a mantener un historial de cambios, lo que permite volver a un punto específico en el tiempo cuando sea necesario. Esto es valioso para recuperarse de eliminaciones accidentales o corrupción de datos.

Las copias de seguridad programadas periódicamente garantizan que sus datos estén actualizados. Supervise la solución de copia de seguridad para asegurarse de que se cumpla el cronograma y de que haya recursos disponibles para la copia de seguridad.

Los dispositivos o servicios de almacenamiento confiables y seguros utilizan discos duros externos, almacenamiento conectado a red (NAS) o almacenamiento en la nube para lograr redundancia. La cinta magnética se utiliza a menudo para el almacenamiento de archivos fuera de las instalaciones.

Se debe verificar la integridad de las copias de seguridad para garantizar la capacidad de restauración. Establezca un cronograma en el que pueda probar sus copias de seguridad y usarlas para restaurar datos y sistemas en un entorno de prueba.

Comprensión del almacenamiento, acceso y uso compartido de datos en servicios en la nube

Los servicios en la nube ofrecen formas convenientes de almacenar, acceder y compartir datos. Los conceptos clave incluyen los siguientes.

En este modelo de copia de seguridad, los datos se almacenan en servidores remotos mantenidos por proveedores de servicios en la nube. El precio de estos servicios suele depender de diversos factores, como la cantidad de almacenamiento necesaria para las copias de seguridad, el tiempo de retención de las copias de seguridad y la velocidad a la que se transferirán los datos en caso de que se utilice una copia de seguridad para restaurar un sistema. Tenga en cuenta que algunos proveedores de servicios de Internet pueden cobrar una tarifa por grandes cantidades de datos que atraviesan su red.

Los servicios en la nube ofrecen un control granular sobre quién puede acceder a sus datos. Un administrador puede gestionar estos controles mediante herramientas disponibles en el proveedor de la nube, normalmente a través de una interfaz web o una utilidad de línea de comandos.

Los servicios de almacenamiento como Dropbox, Google Drive y OneDrive te permiten compartir archivos fácilmente con otras personas. Ten en cuenta que estos servicios no son necesariamente soluciones de copia de seguridad, sino que son un medio para proporcionar acceso a los archivos dentro de una organización. Cuando un usuario elimina un archivo, ya sea intencional o accidentalmente, según cómo estén configurados los sistemas cliente de los otros usuarios, es probable que se elimine el mismo archivo de su sistema. Para restaurar un archivo que se ha eliminado de esta manera, puede ser necesario ponerse en contacto con el proveedor de servicios en la nube y solicitarle que restaure el archivo. Esto también puede suponer un coste adicional.

Implicaciones de seguridad del almacenamiento en la nube y el acceso compartido

Es importante entender que las soluciones en la nube son básicamente “las computadoras de otros”. Teniendo esto en cuenta, el proveedor de almacenamiento en la nube debe demostrar un nivel de confianza hacia el cliente, considerando que sus sistemas almacenarán copias de los datos más importantes del cliente. En primer plano de esta confianza se encuentran las siguientes consideraciones.

Los administradores deben evaluar las medidas de seguridad proporcionadas por el proveedor de servicios en la nube y utilizar cifrado adicional si es necesario.

También es necesario tener cuidado al compartir datos para garantizar que solo las personas autorizadas tengan acceso a ellos. Mantenga un registro de quién accede a las copias de seguridad, así como de cuándo se accedió a ellas.

Dependencia de la conexión a Internet y sincronización de datos

Al trabajar con soluciones externas o en la nube para realizar copias de seguridad, tenga en cuenta lo siguiente:

El almacenamiento en la nube depende de una conexión a Internet. La falta de conectividad puede afectar el acceso a sus datos. Como se mencionó anteriormente, algunos proveedores de servicios de Internet pueden cobrar una tarifa más alta por el uso extensivo del ancho de banda. Además, tenga en cuenta las preocupaciones de seguridad que conlleva una conexión a Internet.

La sincronización garantiza que los datos almacenados en la copia de seguridad en la nube coincidan con los datos de los sistemas locales. Ayuda a mantener la coherencia de los datos al mantener la copia de seguridad actualizada con los cambios realizados en los datos de origen. Sin una sincronización adecuada, es posible que las copias de seguridad estén desactualizadas o incompletas, lo que puede ser problemático durante la recuperación de datos.

Ejercicios guiados

1. ¿Cuál es el propósito principal de una copia de seguridad?

2. ¿Qué tipo de copia de seguridad se describe como la más eficiente en términos de espacio de almacenamiento, pero puede ser más lenta al restaurar datos?

3. ¿Cuál es el propósito de una política de retención de copias de seguridad?

Ejercicios exploratorios

1. Cree un plan de respaldo para sus datos personales o laborales, teniendo en cuenta el tipo de datos, la frecuencia de los respaldos y las opciones de almacenamiento.

2. Investigue un servicio de almacenamiento en la nube popular y sus características de seguridad.

 Esta obra está bajo la licencia CC BY-NC-ND 4.0. |

Resumen

En esta lección, hemos explorado la importancia de las copias de seguridad de datos, los tipos y estrategias de copia de seguridad más comunes, las implicaciones de seguridad relacionadas con las copias de seguridad y los conceptos básicos del almacenamiento de datos en servicios en la nube. Si sigue las prácticas recomendadas en materia de gestión de datos y estrategias de copia de seguridad, puede garantizar la disponibilidad y seguridad de sus datos valiosos. Si utiliza almacenamiento externo para las copias de seguridad (incluida la nube), asegúrese de cifrarlas para garantizar la seguridad e integridad de los datos.

Respuestas a los ejercicios guiados

1. ¿Cuál es el propósito principal de una copia de seguridad?

   Recuperar datos en caso de pérdida o daño.

2. ¿Qué tipo de copia de seguridad se describe como el más eficiente en términos de espacio de almacenamiento, pero puede ser más lento al restaurar datos?

   Copias de seguridad incrementales.

3. ¿Cuál es el propósito de una política de retención de copias de seguridad?

   Definir durante cuánto tiempo se conservan las copias de seguridad y cuándo se eliminan.

 Esta obra está bajo la licencia CC BY-NC-ND 4.0. |

Respuestas a los ejercicios exploratorios

1. Cree un plan de respaldo para sus datos personales o laborales, teniendo en cuenta el tipo de datos, la frecuencia de los respaldos y las opciones de almacenamiento.

   Las soluciones para esta tarea varían según el sistema del que se va a realizar el respaldo. Los usuarios de Linux pueden usar Déjà Dup y duplicity para una gestión sencilla de los respaldos, los usuarios de Apple pueden usar Time Machine y los respaldos de iCloud, y los usuarios de Windows pueden usar la utilidad Windows Backup. Muchas de estas utilidades ofrecen formas de programar trabajos de respaldo para mantenerse al día con los cambios de datos.

2. Investigue un servicio de almacenamiento en la nube popular y sus características de seguridad.

   Los factores a tener en cuenta incluyen la cantidad de almacenamiento disponible para cada plan de servicio, las metodologías de cifrado utilizadas, las restricciones de acceso a los datos y las tarifas de transferencia de datos.

Linux Professional Institute

Tema 024: Seguridad de redes y servicios

 | Esta obra está bajo la licencia CC BY-NC-ND 4.0. |

024.1 Redes, servicios de red e Internet

Referencia al objetivo del LPI

Security Essentials version 1.0, Exam 020, Objective 024.1

Peso

4

Áreas de conocimiento clave

- Comprensión de los distintos tipos de medios y dispositivos de red
- Comprensión de los conceptos de redes IP e Internet
- Comprensión de los conceptos de enrutamiento y proveedores de servicios de Internet (ISP)
- Comprensión de los conceptos de direcciones MAC y de capa de enlace, direcciones IP, puertos TCP y UDP y DNS
- Comprensión de los conceptos de computación en la nube

Lista parcial de archivos, términos y utilidades

- Redes cableadas, redes WiFi, redes celulares
- Conmutadores, enrutadores, puntos de acceso
- Enrutador predeterminado
- Proveedor de servicios de Internet
- IPv4, IPv6
- TCP, UDP, ICMP, DHCP
- DNS, nombres de host DNS, DNS directo, DNS inverso
- Computación en la nube
- Infraestructura como servicio (IaaS)

- Plataforma como servicio (PaaS)
- Software como servicio (SaaS)

Linux Professional Institute

Lección 1

Certificado:	Fundamentos de seguridad
Versión:	1.0
Tema:	024 Seguridad de redes y servicios
Objetivo:	024.1 Redes, servicios de red e Internet
Lección:	1 de 2

Introducción

En el panorama digital actual, un conocimiento básico de las redes informáticas e Internet es esencial para cualquier profesional de TI. Esto incluye comprender los conceptos básicos de los medios de red, como las conexiones cableadas e inalámbricas, y cómo se transmiten los datos a través de las mismas. Es necesario tener conocimientos sobre esquemas de direccionamiento como direcciones IP, el proceso de enrutamiento y reenvío de paquetes y protocolos clave de Internet como TCP/IP, HTTP y DNS. Estos elementos forman la columna vertebral de la comunicación en red, lo que permite el intercambio continuo de datos a través de sistemas globales. El dominio de estos temas proporciona a los candidatos las habilidades necesarias para navegar y solucionar problemas en las infraestructuras de red modernas de manera eficaz.

Medios y dispositivos de red

En materia de ciberseguridad y redes, es fundamental comprender los tipos fundamentales de medios de red y los dispositivos que conectan las redes. Las redes *cableadas*, *inalámbricas* y *celulares* tienen características únicas y requieren dispositivos específicos para funcionar. En esta lección, se exploran los diferentes tipos de medios de red, los dispositivos que se utilizan para administrarlos y sus funciones para permitir la comunicación entre redes.

Antes de sumergirnos en Internet y los poderosos protocolos que impulsan su funcionalidad, es fundamental explorar primero sus bases: las redes locales. Para comprender verdaderamente cómo se conecta todo, debemos comenzar con los conceptos básicos: los tipos de medios de red y los dispositivos que hacen posibles estas conexiones.

Tipos de medios de red

Las *redes cableadas* utilizan cables físicos para conectar dispositivos, de forma similar a cómo un cargador conecta el teléfono a una toma de corriente. Los tipos de conexiones cableadas más comunes son Ethernet y fibra óptica.

Ethernet se utiliza ampliamente en hogares y oficinas porque permite enviar datos rápidamente, de forma similar a cómo cuando una manguera suministra agua a alta presión. Funciona bien tanto en distancias cortas, como entre su computadora y un enrutador cercano, así como en distancias más largas dentro de un edificio.

Por otro lado, los cables de fibra óptica son como las autopistas de Internet. En lugar de utilizar señales eléctricas como Ethernet, utilizan luz para transferir datos, lo que los hace mucho más rápidos y capaces de transportar datos a distancias mucho mayores (piense en la fibra óptica como un medio para transmitir información a la velocidad de la luz). Sin embargo, así como construir una autopista es más caro que tender una carretera normal, la fibra óptica es más costosa y compleja de instalar, por lo que se encuentra con mayor frecuencia en grandes empresas o para conexiones de Internet entre ciudades.

Por el contrario, las *redes Wi-Fi* utilizan ondas de radio para enviar datos, de forma similar a cómo la radio de tu coche capta música de una emisora sin necesidad de cables. El Wi-Fi es increíblemente popular porque permite que tus dispositivos, como teléfonos inteligentes y computadoras portátiles, se conecten a Internet sin la molestia de tener que enchufar ningún cable. Esta flexibilidad lo hace ideal para moverse por la casa y mantenerse conectado.

El Wi-Fi normalmente funciona en dos “canales” o bandas de frecuencia: 2,4 GHz y 5 GHz. Piense en ellos como carriles en una carretera. La banda de 2,4 GHz es como una carretera más ancha que llega más lejos, lo que le permite conectarse incluso en habitaciones alejadas del enrutador, pero la velocidad es más lenta, como conducir en una autopista con mucho tráfico. Por otro lado, la banda de 5 GHz es como un carril más rápido pero más estrecho. Le brinda velocidades más rápidas para streaming o juegos, pero necesita estar más cerca del enrutador, al igual que acelerar es más fácil en una carretera corta y despejada.

Sin embargo, si bien el Wi-Fi es muy conveniente, se puede interrumpir con mayor facilidad, de manera similar a cómo las señales de radio pueden verse afectadas por las paredes u otros dispositivos electrónicos. También está más expuesto a riesgos de seguridad, por lo que medidas

como contraseñas seguras y cifrado son importantes para mantener su red a salvo de visitantes no deseados.

Las *redes celulares*, incluidas 3G, 4G y ahora 5G, emplean torres de telefonía celular altas para enviar y recibir datos desde tu teléfono móvil. Estas torres envían señales que tu teléfono capta para que puedas acceder a Internet sin necesidad de Wi-Fi ni cables. Estas redes son las que te permiten usar aplicaciones, navegar por Internet o escuchar música en streaming mientras estás fuera de casa, incluso cuando estás lejos de ella.

Cada generación (3G, 4G y 5G) representa un salto en la velocidad y la potencia de estas redes. La 3G es como una carretera antigua y más lenta que solía ser ideal para actividades simples como enviar mensajes de texto o cargar sitios web básicos. La 4G llegó y aceleró todo, permitiendo actividades como la transmisión de videos y descargas más veloces. La 5G es la más nueva y rápida, como un tren bala de alta velocidad que puede manejar incluso más datos a la vez, lo que la hace ideal para actividades como la realidad virtual y los dispositivos inteligentes.

Sin embargo, así como algunas áreas tienen mejores condiciones viales que otras, la velocidad y la potencia de tu red celular dependen de dónde te encuentres. En algunos lugares, puedes tener una excelente cobertura 4G o 5G, lo que te brinda velocidades rápidas, mientras que en otras áreas, la señal puede ser más débil, lo que resulta en conexiones a Internet más lentas.

Dispositivos de red

Para comprender cómo se comunican los dispositivos de red, es fundamental comprender cómo se identifican y reconocen entre sí dentro de diferentes tipos de medios de red, como Wi-Fi, Ethernet, fibra óptica o redes celulares.

Esta identificación es esencial porque cuando un dispositivo realiza una solicitud a otro, debe ser posible determinar dónde se originó el paquete de datos y en qué computadora se encuentra el destinatario previsto.

A nivel de red local, este direccionamiento se gestiona mediante una convención conocida como dirección MAC (Media Access Control). La dirección MAC actúa como una “huella digital” única para cada dispositivo de la red, lo que garantiza que los datos se dirijan correctamente y se entreguen al dispositivo correcto. Sin este tipo de direccionamiento, sería imposible gestionar el tráfico de datos entre varios dispositivos conectados, lo que provocaría confusión y pérdida de datos.

Cada dispositivo conectado a una red tiene su propia dirección MAC, lo que hace que las direcciones sean esenciales para la comunicación dentro de esa red. Cada dirección MAC consta de seis pares de caracteres hexadecimales o bytes, donde los primeros tres pares suelen identificar al fabricante del dispositivo y los últimos tres pares son específicos de ese dispositivo

en particular.

El Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) mantiene el estándar para las direcciones MAC. El estándar define que los primeros tres bytes, conocidos como el Identificador Único Organizacional (OUI), identifican al fabricante: Cisco, Intel, etc. Los OUI son asignados a los fabricantes por el IEEE. Los tres bytes restantes son determinados por el fabricante, que es responsable de administrar la numeración de cada dispositivo que produce.

Un ejemplo de una dirección MAC es:

```
00:1A:2B:3C:4D:5E**
```

`00:1A:2B` identifica al fabricante. Este OUI en particular se refiere a un pequeño fabricante de productos de comunicaciones. `3C:4D:5E`` es el identificador único para ese dispositivo específico producido por el fabricante.

Aunque una dirección MAC es única y está incorporada en el hardware, se puede modificar mediante diversas técnicas, lo que permite cambiarla cuando sea necesario.

Para gestionar y dirigir el flujo de datos dentro de las redes, se utilizan varios dispositivos importantes, cada uno con una función específica. Estos se describen en las siguientes secciones.

Conmutador (Switch)

Un *switch* es como un policía de tránsito para los dispositivos dentro de la misma red, asegurándose de que puedan comunicarse entre sí de manera eficiente. Imagine que tiene varias computadoras, impresoras y otros dispositivos en una oficina, todos ellos que necesitan compartir información. El switch los conecta, asegurándose de que los datos correctos lleguen al dispositivo correcto. Esto se hace en lo que se llama la *capa de enlace de datos* (Capa 2) del modelo *Interconexión de sistemas abiertos* (OSI). Esta capa es donde se utilizan las direcciones físicas, las direcciones MAC.

Cuando un dispositivo envía datos, el conmutador analiza la dirección MAC para ver a qué dispositivo están destinados. En lugar de enviar los datos a todos los dispositivos de la red, el conmutador los dirige solo al dispositivo específico con la dirección MAC correspondiente. Esto hace que la comunicación sea más rápida y eficiente, lo que evita la congestión de la red y garantiza que los datos lleguen a donde deben ir.

Los conmutadores se presentan en dos variedades. Los conmutadores administrados son como herramientas personalizables que los administradores de red pueden controlar, ajustando el flujo de datos, monitoreando el tráfico y aplicando reglas para un mejor rendimiento y seguridad. Por

otro lado, los conmutadores no administrados son más básicos y funcionan automáticamente sin ninguna configuración o supervisión, como un simple dispositivo plug-and-play que simplemente hace el trabajo.

Enrutador (Router)

Un *enrutador* tiene una responsabilidad más amplia: conectar distintas redes entre sí. Opera en la capa de red (capa 3) del modelo OSI, donde se utilizan direcciones IP para guiar los datos entre redes. Piense en un enrutador como un servicio postal que sabe cómo entregar un paquete de una ciudad (red) a otra. En un entorno doméstico, su enrutador conecta todos sus dispositivos locales (como teléfonos, computadoras portátiles y televisores inteligentes) a Internet a través de su proveedor de servicios de Internet (ISP). Los enrutadores son fundamentales para garantizar que los datos sepan a dónde ir, ya sea entre dispositivos locales o hacia Internet.

Los enrutadores son esenciales no solo para administrar el tráfico de datos dentro de su red local (entre dispositivos como teléfonos y computadoras), sino también para enrutar el tráfico entre su red doméstica e Internet en general. Sin un enrutador, los dispositivos no podrían comunicarse fuera de su entorno local y no tendrían acceso a los recursos en línea.

Punto de acceso (Access Point)

Un punto de acceso (AP) es especialmente importante para las redes inalámbricas. Es un dispositivo que transmite una señal de Wi-Fi, lo que permite que dispositivos como teléfonos inteligentes, tabletas y computadoras portátiles se conecten a la red sin cables físicos. Imagine un punto de acceso como una baliza de Wi-Fi que permite que sus dispositivos inalámbricos se comuniquen con la red cableada. En áreas más grandes, como oficinas o escuelas, se pueden implementar múltiples puntos de acceso para garantizar una cobertura Wi-Fi perfecta, lo que permite que los dispositivos permanezcan conectados mientras se mueven por diferentes partes del edificio sin perder su conexión.

En muchos hogares, es habitual que el punto de acceso funcione también como enrutador. La mayoría de los enrutadores Wi-Fi modernos combinan ambas funciones en un solo dispositivo. Esto significa que el dispositivo no solo permite que sus teléfonos, computadoras portátiles y otros dispositivos inalámbricos se conecten a la red a través de Wi-Fi, sino que también administra el tráfico entre su red doméstica e Internet. Esta doble funcionalidad es conveniente porque simplifica la configuración: un dispositivo puede encargarse de todo, desde administrar el tráfico local entre dispositivos hasta garantizar el acceso a Internet.

Redes IP e Internet

En el corazón de las redes modernas se encuentran las redes IP e Internet, dos componentes

fundamentales que permiten que los dispositivos se comuniquen e intercambien datos a lo largo de grandes distancias. Comprender cómo funcionan estos conceptos es esencial para cualquier persona involucrada en la ciberseguridad, ya que forman la columna vertebral de la transmisión de datos y, por lo tanto, de la seguridad de la red.

Redes IP: La base de la comunicación

Una red IP es una red que utiliza el protocolo de Internet (IP) para enviar y recibir datos entre dispositivos. Cada dispositivo de una red IP (ya sea una computadora, un teléfono inteligente o un servidor) tiene un identificador único conocido como dirección IP. Esta dirección funciona como una dirección de domicilio para su dispositivo, lo que permite que los datos encuentren el camino hacia el destino correcto.

Hay dos versiones principales de direcciones IP, cada una con su propio formato y propósito.

El Protocolo de Internet versión 4 (IPv4) es la versión más utilizada de direccionamiento IP. Consiste en cuatro grupos de números, cada uno de ellos de 0 a 255, separados por puntos (por ejemplo, `192.168.1.1`). El número total de direcciones IPv4 disponibles es de alrededor de 4.300 millones, lo que puede parecer mucho, pero debido al crecimiento exponencial de los dispositivos conectados a Internet (teléfonos inteligentes, computadoras, dispositivos IoT, etc.), las direcciones IPv4 se han vuelto cada vez más escasas. Para abordar esta escasez, se implementaron técnicas como la Traducción de direcciones de red (NAT) para extender la utilidad de IPv4, pero esto fue solo una solución temporal.

El Protocolo de Internet versión 6 (IPv6) resuelve las limitaciones del IPv4. Esta versión utiliza un formato mucho más largo y complejo, que consta de ocho grupos de cuatro dígitos hexadecimales separados por dos puntos (por ejemplo, `2001:0db8:85a3:0000:0000:8a2e:0370:7334`). El IPv6 proporciona un conjunto de direcciones casi ilimitado (aproximadamente 340 undecillones), suficiente para satisfacer la creciente demanda de dispositivos conectados a Internet en el futuro. Además de ofrecer más direcciones, el IPv6 también mejora la eficiencia, simplifica el enrutamiento y mejora la seguridad con funciones como el cifrado integrado y la autenticación mejorada de dispositivos.

Las redes IP son increíblemente flexibles. Pueden ser pequeñas, como una red de área local (LAN) que conecta dispositivos en un hogar u oficina, o pueden ser grandes y complejas, como una red de área amplia (WAN) que abarca varias ciudades o países. Sin embargo, todas las redes IP se basan en los mismos principios fundamentales de direccionamiento y reenvío de paquetes para funcionar.

Cuando se envían datos a través de una red IP, se dividen en pequeñas unidades llamadas *paquetes*. Cada paquete se etiqueta con las direcciones IP de origen y destino y luego se enruta a

través de la red. Los enrutadores, que se analizaron anteriormente, son responsables de dirigir estos paquetes al destino correcto, utilizando las direcciones IP como guía.

Internet: una red IP global

Internet es en esencia, la red IP más grande del mundo, que conecta miles de millones de dispositivos a nivel mundial. Funciona interconectando varias redes más pequeñas, lo que les permite comunicarse entre sí. Cuando visita un sitio web, envía un mensaje de correo electrónico o transmite un video, su dispositivo se comunica con servidores ubicados en todo el mundo a través de Internet.

Internet se basa en una serie de protocolos, de los cuales el más importante es el Protocolo de Control de Transmisión/Protocolo de Internet (TCP/IP). Este conjunto de protocolos garantiza que los datos se transmitan de forma fiable a través de diferentes redes. La parte IP, ya analizada, se encarga del direccionamiento y el enrutamiento, mientras que la parte TCP garantiza que los datos lleguen intactos y en el orden correcto, incluso si se envían en varios paquetes.

Uno de los aspectos clave de Internet es la descentralización. Ninguna entidad controla la totalidad de Internet, sino que está formada por muchas redes interconectadas, cada una de ellas gestionada por diferentes organizaciones, empresas y gobiernos. Esta estructura descentralizada hace que Internet sea muy resistente, pero también plantea desafíos en materia de regulación, seguridad y privacidad.

Proveedores de servicios de Internet y enrutamiento (ISP)

En redes, el enrutamiento y el rol de los proveedores de servicios de Internet (ISP) son conceptos fundamentales que ayudan a comprender cómo viajan los datos a través de Internet y cómo se comunican los dispositivos en diferentes redes. Comprender estos conceptos es crucial, especialmente cuando se consideran las implicaciones de seguridad de la transmisión de datos a través de redes públicas y privadas.

Enrutamiento: cómo los datos encuentran su camino

En el centro de la comunicación por Internet se encuentra el enrutamiento, el proceso de determinar la mejor ruta para que los datos viajen de un dispositivo a otro a través de diferentes redes. Piense en ello como si fuera el GPS de Internet. Cuando envía una solicitud para cargar un sitio web, sus datos se dividen en pequeños paquetes, que deben encontrar su camino desde su dispositivo hasta el servidor que aloja ese sitio web. Como se mencionó anteriormente, los enrutadores son dispositivos especializados que dirigen el tráfico entre redes y determinan la ruta más eficiente para estos paquetes.

Los enrutadores toman decisiones en función de las direcciones IP. Reenvían datos en función de la dirección IP de destino, saltando de una red a otra hasta que los datos llegan a su destino final. Del mismo modo que un paquete en el correo puede pasar por varios centros de distribución antes de llegar a su hogar, los paquetes de datos viajan a través de varios enrutadores a través de diferentes redes.

El enrutamiento ocurre en la capa de red (capa 3) del modelo OSI, y los enrutadores utilizan protocolos como IP para guiar los paquetes.

Un concepto importante en el enrutamiento es el enrutador predeterminado, a menudo denominado puerta de enlace predeterminada, que desempeña un papel crucial en la forma en que los dispositivos se comunican tanto dentro de una red local como con Internet. En pocas palabras, un enrutador predeterminado actúa como un puente entre una red local (como la de su hogar) y redes externas, más comúnmente Internet.

Un enrutador predeterminado es el dispositivo que su computadora u otros dispositivos usan para acceder a redes externas. Cuando un dispositivo en una red local necesita enviar datos a otro dispositivo que no forma parte de la misma red (por ejemplo, para acceder a un sitio web o conectarse a un servicio en la nube), envía los datos al enrutador predeterminado. Luego, el enrutador reenvía estos datos al destino correspondiente en Internet u otra red externa.

En la mayoría de las configuraciones de hogares o pequeñas oficinas, el enrutador predeterminado es el mismo dispositivo que su enrutador inalámbrico, que conecta su hogar a Internet a través de un ISP.

Proveedores de servicios de Internet (ISP): Puertas de acceso a Internet

Tu conexión a Internet es posible gracias a los ISP, que son empresas que proporcionan acceso a Internet a hogares, empresas y organizaciones. Operan grandes redes de enrutadores, cables y servidores que conectan redes locales más pequeñas (como la red Wi-Fi de tu hogar) a Internet global.

Un ISP le asigna a su hogar o negocio una dirección IP pública única, que le permite a su enrutador comunicarse con otros dispositivos en Internet. Cuando escribe una dirección web, su dispositivo primero se comunica con su ISP, que dirige su solicitud al destino apropiado en Internet. El ISP actúa como un “intermediario”, enrutando sus datos a su destino y enviándole las respuestas a usted.

Ejercicios guiados

1. Describa las diferencias entre redes *cableadas* e *inalámbricas*. Proporcione ejemplos de cada una y explique cómo funcionan.

2. ¿Qué es una dirección MAC y cómo ayuda a los dispositivos a comunicarse en una red local? Proporcione un ejemplo de cómo podría verse una dirección MAC y explique su estructura.

3. Explique las diferencias entre las direcciones *IPv4* e *IPv6*. ¿Por qué se desarrolló IPv6 y en qué mejora a IPv4?

Ejercicios exploratorios

1. Investigue cómo se utiliza la suplantación de direcciones MAC en los ataques a la red. ¿Cuáles son los posibles riesgos de seguridad asociados con la suplantación de direcciones MAC y qué técnicas se pueden utilizar para prevenir dichos ataques?

2. Investigue el estado actual de la adopción de IPv6 en todo el mundo. ¿Qué desafíos han enfrentado las organizaciones en la transición de IPv4 a IPv6 y cuáles son los beneficios clave de usar IPv6 en lugar de IPv4?

 Esta obra está bajo la licencia CC BY-NC-ND 4.0. |

Resumen

En esta lección se presentan conceptos clave de las redes modernas, comenzando con los fundamentos de las redes locales y cómo se comunican los dispositivos mediante diferentes tipos de medios de red, como redes cableadas, inalámbricas y celulares. Se describe cada tipo de red, incluidas las funciones de Ethernet, fibra óptica, Wi-Fi y tecnologías celulares como 3G, 4G y 5G.

En esta lección se explica cómo los dispositivos de red, como conmutadores, enrutadores y puntos de acceso, administran el tráfico de datos. Se presentan las direcciones MAC como un medio para identificar dispositivos en una red local, lo que permite una comunicación eficaz entre ellos. Se explican las funciones de un conmutador en la administración del tráfico local y de un enrutador en la conexión de diferentes redes, especialmente para el acceso a Internet. Además, se analiza el concepto de punto de acceso, destacando cómo transmite una señal Wi-Fi a dispositivos inalámbricos.

La lección profundiza en las redes IP e Internet, y cubre cómo se utilizan las direcciones IP (tanto IPv4 como IPv6) para identificar dispositivos en redes globales. Presenta el Protocolo de Internet (IP) como el método para dirigir datos entre redes y explica la diferencia entre las dos versiones de direcciones IP. El enrutamiento se describe como el proceso de encontrar la mejor ruta para que viajen los datos, y se explica el enrutador predeterminado y el papel de los proveedores de servicios de Internet (ISP) como componentes clave para acceder a Internet en general.

Por último, se aborda la naturaleza descentralizada de Internet y la importancia de los protocolos TCP/IP para garantizar una comunicación segura y confiable. Se abordan conceptos como el enrutamiento de paquetes, las puertas de enlace predeterminadas y la función de los ISP en la provisión de acceso a Internet.

Respuestas a los ejercicios guiados

1. Describe las diferencias entre redes *cableadas* e *inalámbricas*. Proporciona ejemplos de cada una y explica cómo funcionan.

   Las redes cableadas dependen de cables físicos, como Ethernet o fibra óptica, para transmitir datos entre dispositivos. Los cables Ethernet son comunes en configuraciones domésticas y de oficina para conexiones estables en distancias más cortas, mientras que la fibra óptica usa luz para transmitir datos a velocidades mucho más altas en distancias más largas, a menudo entre ciudades o para grandes organizaciones. Las redes inalámbricas, como Wi-Fi, usan ondas de radio para enviar datos, lo que permite que dispositivos como teléfonos o computadoras portátiles se conecten sin necesidad de cables. Wi-Fi opera en diferentes bandas de frecuencia, con 2,4 GHz que ofrece un rango más amplio pero velocidades más lentas, y 5 GHz que proporciona velocidades más rápidas pero en una distancia más corta.

¿Qué es una dirección MAC y cómo ayuda a los dispositivos a comunicarse en una red local? Proporcione un ejemplo de cómo podría verse una dirección MAC y explique su estructura.

+ Una dirección MAC es un identificador de hardware único asignado a la tarjeta de red de cada dispositivo, lo que permite que los dispositivos se comuniquen dentro de la misma red. Asegura que los datos se envíen al dispositivo correcto en la red. La dirección consta de seis pares de caracteres hexadecimales, donde los primeros tres identifican al fabricante del dispositivo y los últimos tres son específicos del dispositivo individual. Un ejemplo de una dirección MAC es `00:1A:2B:3C:4D:5E`, donde `00:1A:2B` identifica al fabricante y `3C:4D:5E` es exclusivo del dispositivo en el catálogo de ese fabricante.

1. Explique las diferencias entre las direcciones *IPv4* e *IPv6*. ¿Por qué se desarrolló IPv6 y cómo mejora a IPv4?

   Las direcciones IPv4 constan de cuatro números separados por puntos, como `192.168.1.1`, y proporcionan una cantidad limitada de direcciones únicas, que se ha vuelto insuficiente a medida que más dispositivos se conectan a Internet. IPv6 se creó para abordar esta escasez, utilizando un formato mucho más largo con más combinaciones posibles, como `2001:0db8:85a3:0000:0000:8a2e:0370:7334`. IPv6 ofrece un suministro casi ilimitado de direcciones y mejora la eficiencia del enrutamiento y la seguridad al incluir características como cifrado integrado y autenticación mejorada.

Respuestas a los ejercicios exploratorios

1. Investigue cómo se utiliza la suplantación de direcciones MAC en los ataques de red. ¿Cuáles son los posibles riesgos de seguridad asociados con la suplantación de direcciones MAC y qué técnicas se pueden utilizar para prevenir tales ataques?

   La suplantación de direcciones MAC ocurre cuando un dispositivo se configura deliberadamente para imitar la dirección MAC de otro dispositivo. Los atacantes utilizan esta técnica para eludir los filtros de red, obtener acceso no autorizado o disfrazar su identidad en una red. Por ejemplo, en redes Wi-Fi públicas, un atacante puede suplantar la dirección MAC de un dispositivo autorizado para obtener acceso a áreas restringidas.

   Los riesgos incluyen el acceso no autorizado a datos confidenciales, la interrupción de los servicios de red y la dificultad de rastrear actividades maliciosas. Para prevenir la suplantación de direcciones MAC, los administradores pueden implementar técnicas como la seguridad de puertos en los conmutadores, que restringe la cantidad de direcciones MAC por puerto, y el filtrado de direcciones MAC en enrutadores y firewalls. Además, el cifrado de red (por ejemplo, WPA3 para Wi-Fi) y la supervisión de la actividad MAC inusual pueden ayudar a proteger las redes contra tales ataques.

2. Investigue el estado actual de la adopción de IPv6 en todo el mundo. ¿Qué desafíos han enfrentado las organizaciones en la transición de IPv4 a IPv6 y cuáles son los beneficios clave de usar IPv6 en lugar de IPv4?

   A nivel mundial, la adopción de IPv6 ha sido gradual, y algunas regiones e industrias han avanzado más rápido que otras. Uno de los principales desafíos ha sido el costo y la complejidad de la transición de la infraestructura de IPv4 a IPv6, ya que muchos sistemas heredados no son totalmente compatibles con IPv6. Además, algunas organizaciones carecen de la necesidad inmediata del vasto espacio de direcciones que proporciona IPv6, lo que ha ralentizado la adopción.

   A pesar de estos desafíos, IPv6 ofrece ventajas significativas sobre IPv4, incluido un espacio de direcciones exponencialmente más grande, una configuración de red simplificada con funciones como la configuración automática de direcciones sin estado (SLAAC) y una eficiencia mejorada en el enrutamiento. IPv6 también incorpora mejores funciones de seguridad, como IPsec para comunicación cifrada, que está integrado en el protocolo.

Linux Professional Institute

Lección 2

Certificado:	Fundamentos de seguridad
Versión:	1.0
Tema:	024 Seguridad de redes y servicios
Objetivo:	024.1 Redes, servicios de red e Internet
Lección:	2 de 2

Introducción

Comprender la comunicación en red y la computación en la nube es fundamental para los profesionales de TI. Esta lección cubre los componentes esenciales de la red y explica cómo el DNS traduce los nombres de dominio en direcciones IP. También explora DHCP y presenta los modelos de computación en la nube, destacando cómo brindan soluciones escalables y flexibles para administrar los recursos de TI.

TCP/IP y sus funciones en la comunicación en red

En esencia, el modelo TCP/IP permite que los datos se transmitan de forma fiable y eficiente entre dispositivos de una red. Los principales protocolos que funcionan dentro del modelo TCP/IP son TCP, UDP, ICMP y DHCP, cada uno con funciones y características distintas.

Protocolo de control de transmisión (TCP)

TCP es un *protocolo orientado a la conexión* que garantiza la entrega confiable, ordenada y libre de errores de datos a través de una red. Esto se logra estableciendo una conexión entre dos dispositivos mediante un proceso conocido como *three-way handshake*. Durante este protocolo, los

 Esta obra está bajo la licencia CC BY-NC-ND 4.0.

dispositivos intercambian mensajes de control (SYN, SYN-ACK y ACK) para sincronizar sus números de secuencia y acordar los parámetros de comunicación antes de que comience cualquier transferencia de datos real.

El handshake es como un cartero que entrega una carta importante con un acuse de recibo. Primero, el cartero (cliente) llama a la puerta (envía una solicitud SYN) para avisar al destinatario de que llegará una carta. El destinatario (servidor) abre la puerta y devuelve un acuse de recibo firmado (SYN-ACK) para confirmar la llegada de la carta. Finalmente, el cartero confirma el intercambio firmando el acuse de recibo (ACK) y se marcha, asegurándose de que ambas partes sepan que el mensaje se entregó correctamente. Este intercambio fiable garantiza que se establezca y confirme la comunicación, de forma muy similar a una entrega postal con acuse de recibo.

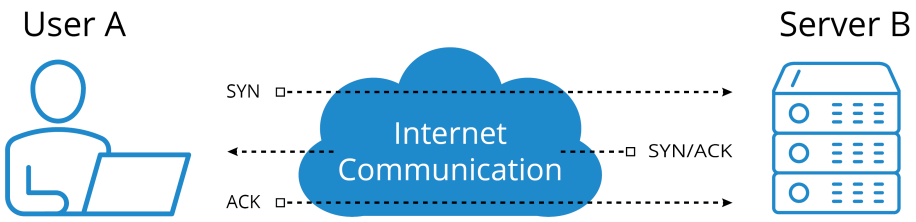

Figure 34. TCP/IP 3-way handshake

Una vez establecida la conexión, TCP utiliza *números de secuencia* para rastrear cada segmento de datos. Estos números de secuencia garantizan que, incluso si los paquetes llegan desordenados debido a rutas de red variables o demoras, el sistema receptor puede volver a ensamblar los datos correctamente. TCP también incorpora mecanismos de control de flujo mediante el uso de una ventana deslizante, que permite al receptor controlar el ritmo de transmisión de datos para evitar sobrecargar sus capacidades de procesamiento o capacidad de búfer.

Los números de secuencia y el control de flujo de TCP se pueden comparar con un cartero que entrega una serie de paquetes en un orden específico. Cada paquete (segmento de datos) está etiquetado con un número (número de secuencia) para que tanto el cartero (cliente) como el destinatario (servidor) puedan realizar un seguimiento del pedido. Si un paquete se pierde o se retrasa, el destinatario puede notificar al cartero que vuelva a enviar solo ese paquete específico.

Además de esa secuencia, TCP emplea paquetes de *acknowledgment* (ACK) para confirmar la recepción de datos. Por cada segmento recibido, el destino envía de vuelta una confirmación, asegurando la llegada correcta de los datos hasta un byte determinado en la secuencia. Si no se recibe una confirmación dentro de un período de tiempo determinado, TCP supone que se ha perdido el paquete y activa la *retransmisión* de los datos no confirmados. Esto hace que TCP sea

altamente confiable, asegurando que no se pierdan datos en tránsito, incluso en redes propensas a congestiones o pérdidas de paquetes.

Estos mecanismos de fiabilidad hacen que TCP sea el protocolo de elección para aplicaciones que requieren una entrega garantizada y la integridad de los datos. Los servicios web (mediante HTTP/HTTPS), la transmisión de correo electrónico (SMTP/IMAP) y las transferencias de archivos (FTP/SCP) dependen de TCP para garantizar que los datos se entreguen sin daños ni pérdidas. Por ejemplo, cuando un navegador web solicita una página web, TCP garantiza que todos los elementos de la página (incluidos el HTML, CSS, JavaScript y las imágenes) se transmitan de forma fiable desde el servidor al cliente. Si se interrumpe alguna parte del flujo de datos, TCP retransmite los segmentos faltantes, lo que garantiza que la página se cargue completa y correctamente.

Protocolo de datagramas de usuario (UDP)

UDP es un *protocolo sin conexión*, lo que significa que no requiere que se establezca una conexión entre dispositivos antes de transmitir datos. Ya que UDP simplemente envía datos en unidades discretas llamadas datagramas sin ningún proceso de configuración formal. A diferencia de TCP, UDP no garantiza la entrega, el orden o la integridad de estos datagramas. Esto significa que los paquetes pueden llegar desordenados, estar duplicados o perderse por completo, y UDP no intentará recuperarlos ni retransmitirlos.

La ausencia de mecanismos de configuración y retransmisión de la conexión reduce significativamente la sobrecarga, lo que hace que el protocolo UDP sea mucho más rápido y eficiente que el protocolo TCP en situaciones en las que se prioriza la velocidad sobre la confiabilidad. Esta característica es fundamental para aplicaciones en las que es necesario entregar datos rápidamente y en tiempo real, incluso si se pierden algunos paquetes. Por ejemplo, en la transmisión de video, un paquete faltante puede provocar una leve caída en la calidad del video o una falla visual breve, pero la transmisión general continúa sin interrupciones.

De manera similar, las aplicaciones de *voz sobre IP (VoIP)* utilizan UDP para transmitir datos de voz, donde una ligera pérdida de paquetes o fluctuaciones pueden pasar desapercibidas para el usuario, pero los retrasos causarían problemas notables en la calidad de la llamada.

Los juegos en línea se benefician de la baja latencia del protocolo UDP, ya que permite que los datos se transmitan con un retraso mínimo, lo que permite un juego rápido y con capacidad de respuesta. Incluso si se pierden o se retrasan paquetes ocasionales, el juego puede seguir funcionando sin congelarse ni detenerse.

Otro caso de uso común de UDP es en las consultas DNS, donde un cliente envía una solicitud para resolver un nombre de dominio en una dirección IP. UDP es ideal para esto porque las consultas

DNS suelen ser pequeñas y deben resolverse rápidamente. Si no se recibe una respuesta, el cliente puede simplemente volver a enviar la solicitud sin la necesidad de la sobrecarga asociada con el establecimiento y mantenimiento de una conexión TCP.

En general, la contrapartida es que UDP sacrifica la confiabilidad por la velocidad, pero en entornos de tiempo real, a menudo es preferible perder unos pocos paquetes a sufrir las demoras que introduce la retransmisión.

Protocolo de mensajes de control de Internet (ICMP)

El protocolo ICMP se utiliza principalmente para funciones de diagnóstico y notificación de errores en redes. A diferencia de TCP o UDP, el protocolo ICMP no es un protocolo de transporte y no está diseñado para la transmisión de datos de aplicaciones. En cambio, funciona como un protocolo de control que permite que los dispositivos de red intercambien información sobre las condiciones y los errores de la red, lo que garantiza el funcionamiento sin problemas de la comunicación basada en IP.

Uno de los principales propósitos de ICMP es informar sobre problemas de red, como hosts inaccesibles, congestión de la red o problemas de enrutamiento. Por ejemplo, si un enrutador no puede reenviar un paquete porque la red de destino es inaccesible, envía un mensaje ICMP al dispositivo de origen para informarle del problema. De manera similar, si un enrutador se sobrecarga o se congestiona, ICMP se puede utilizar para enviar mensajes que indiquen que se están descartando o retrasando paquetes.

Una herramienta muy conocida y ampliamente utilizada basada en ICMP es el comando `ping`. Ping es una utilidad de diagnóstico simple pero poderosa que prueba la accesibilidad de un host en una red. Cuando ejecuta `ping`, su sistema envía mensajes ICMP *echo request* al host de destino, y el host responde con respuestas ICMP *echo replies*. El tiempo de ida y vuelta entre el envío de la solicitud y la recepción de la respuesta ayuda a determinar la latencia y la conectividad entre su dispositivo y el host de destino. Si no se recibe respuesta, indica que el host puede estar inactivo o inaccesible debido a un problema de red.

Puertos TCP y UDP

Tanto TCP como UDP utilizan *puertos* para distinguir entre diferentes servicios en un único dispositivo. Un puerto es un punto final lógico para la comunicación, que garantiza que los datos se dirijan a la aplicación adecuada. Los puertos están numerados del 0 al 65535, y los puertos del 0 al 1023 se designan como *puertos conocidos* para protocolos ampliamente utilizados como HTTP (puerto 80), HTTPS (puerto 443), DNS (puerto 53), entre otros. Los puertos en el rango de 1024 a 49151 se conocen como *puertos registrados*, y los puertos del 49152 al 65535 son *puertos dinámicos* o *puertos privados*, que se utilizan normalmente para conexiones temporales o internas.

Cada servicio o aplicación de un servidor escucha en un *número de puerto* específico, por lo que cuando llega un paquete TCP o UDP, se dirige al servicio correcto según el puerto de destino. Por ejemplo, una visita a un sitio web a través de un navegador envía la solicitud al puerto 80 (para HTTP) o al puerto 443 (para HTTPS). Del mismo modo, una consulta DNS se envía al puerto UDP 53.

Comprender las diferencias entre estos protocolos y su uso de los puertos es fundamental para la seguridad de la red, ya que los atacantes suelen aprovechar las vulnerabilidades en estas áreas. Los profesionales de seguridad deben supervisar el tráfico de la red, garantizar la configuración adecuada de los servicios y proteger los puertos críticos para defenderse de las amenazas comunes.

DHCP: cómo un dispositivo obtiene una dirección IP

Cuando un dispositivo, como una computadora o un teléfono inteligente, se conecta a una red, necesita una dirección IP para comunicarse con otros dispositivos. Este proceso generalmente lo gestiona un servicio llamado *Protocolo de configuración dinámica de host* (DHCP). DHCP asigna automáticamente direcciones IP a los dispositivos, lo que facilita su conexión sin necesidad de configuración manual.

Así es como funciona: cuando un dispositivo se une a una red por primera vez, aún no tiene una dirección IP. Para solicitarla, el dispositivo envía un mensaje especial, llamado mensaje de descubrimiento DHCP, en el que solicita una dirección IP. Este mensaje se transmite a todos los dispositivos de la red porque el dispositivo no conoce la ubicación específica del servidor DHCP. El servidor DHCP es un sistema que administra la distribución de direcciones IP.

Una vez que el servidor DHCP recibe esta solicitud, responde con una *oferta DHCP*, que incluye una dirección IP disponible que el dispositivo puede usar, así como otras configuraciones necesarias, como la máscara de subred y la puerta de enlace predeterminada. Estas configuraciones son importantes porque ayudan al dispositivo a saber cómo comunicarse con otros dispositivos en la red y acceder a Internet.

Después de recibir la oferta, el dispositivo envía un mensaje, llamado *solicitud DHCP*, indicando que acepta la dirección IP propuesta. Esto garantiza que el servidor DHCP sepa que el dispositivo desea utilizar la dirección IP específica que ofreció. Finalmente, el servidor DHCP confirma esta asignación enviando un acuse de recibo, llamado *confirmación DHCP* (ACK). En este punto, el dispositivo puede comenzar a utilizar su nueva dirección IP para enviar y recibir datos a través de la red.

La dirección IP asignada por el servidor DHCP no es permanente, sino que se le otorga al dispositivo por un período específico. Cuando el período de concesión está por vencer, el

dispositivo puede renovarlo para mantener la misma dirección IP.

DHCP simplifica el proceso de conexión a una red al automatizar la asignación de direcciones IP. Sin DHCP, los administradores de red tendrían que configurar manualmente cada dispositivo con una dirección IP única, lo que llevaría mucho tiempo y sería propenso a errores, especialmente en redes grandes.

El rol del DNS

Cuando utilizas Internet, a menudo recurres a nombres de dominio, como `lpi.org`, para acceder a sitios web. Sin embargo, las computadoras no entienden estos nombres directamente. Se comunican mediante direcciones IP. El sistema que traduce los nombres de dominio fáciles de usar en direcciones IP se denomina *Sistema de nombres de dominio* (DNS).

El DNS actúa como una guía telefónica para Internet. Cuando escribes la dirección de un sitio web (como `learning.lpi.org`) en tu navegador, el DNS se encarga de encontrar la dirección IP asociada a ese nombre de dominio para que tu navegador pueda localizar y conectarse al servidor web correcto.

En la terminal de la computadora, es posible obtener información sobre qué dirección IP está asociada a un nombre de dominio o viceversa usando el comando `nslookup` o `dig`:

```
$ nslookup learning.lpi.org
Server: 127.0.0.1
Address: 127.0.0.1#53

Non-authoritative answer:
Name: learning.lpi.org
Server: 208.94.166.201
```

Nombres de host DNS

A cada dispositivo conectado a una red se le puede asignar un *nombre de host DNS*, que es una etiqueta legible por humanos asociada con su dirección IP. Por ejemplo, un servidor podría tener el nombre de host `webserver1.example.com`. Este nombre de host es más fácil de recordar para las personas que la dirección IP numérica que usan las computadoras. Los nombres de host son parte del sistema DNS más amplio, lo que ayuda a los usuarios y administradores a manejar e identificar dispositivos en una red de manera más conveniente.

Búsqueda DNS directa

La consulta DNS directa es el uso más común de este servicio. Implica convertir un nombre de dominio en su dirección IP correspondiente. Cuando ingresa una URL en su navegador, se realiza una consulta DNS directa para resolver ese nombre de dominio en una dirección IP. Por ejemplo, si escribe "www.example.com" en su navegador, el sistema DNS realiza una búsqueda directa para encontrar la dirección IP asociada, como "192.0.2.1", y dirige su navegador al servidor correcto.

El sistema DNS utiliza una serie de servidores DNS para realizar esta búsqueda. Tu dispositivo primero contacta con un *resolver* DNS local, que puede almacenar en caché consultas anteriores para acelerar el proceso. Si no se encuentra la dirección IP en la caché, el *resolver* contacta con otros servidores DNS, incluido el servidor DNS autorizado del dominio, para encontrar la dirección IP correcta. Una vez que se encuentra la dirección IP, se devuelve a tu navegador y se realiza la conexión con el servidor web.

Búsqueda DNS inversa

Una *búsqueda DNS inversa* funciona de forma opuesta. En lugar de convertir un nombre de dominio en una dirección IP, convierte una dirección IP nuevamente en un nombre de dominio. Esto es útil para verificar la identidad de un host y se utiliza a menudo en servidores de correo electrónico y resolución de problemas de red. Por ejemplo, si un servidor recibe una solicitud de una dirección IP y desea confirmar la identidad del host, puede realizar una búsqueda DNS inversa para ver el nombre de dominio asociado con esa dirección IP. Esto ayuda a prevenir actividades maliciosas.

Si bien las búsquedas de DNS directas son esenciales para el uso diario de Internet, las búsquedas de DNS inversas son comúnmente más utilizadas por administradores de red, sistemas de seguridad y servidores de correo electrónico para garantizar la integridad de las conexiones.

El DNS es un componente fundamental del funcionamiento de Internet, ya que permite traducir nombres de dominio fáciles de entender para los humanos en direcciones IP legibles por máquinas. Ya sea mediante búsquedas DNS directas que permiten a los usuarios acceder a sitios web por nombre de dominio o mediante búsquedas DNS inversas que se utilizan para verificar identidades y mantener la seguridad, el DNS garantiza que los dispositivos y las personas puedan comunicarse de manera eficiente en la web. Sin el DNS, navegar por Internet sería mucho más complicado y requeriría que los usuarios recuerden direcciones IP complejas para cada sitio web y servicio al que quieran acceder.

Conceptos de computación en la nube

La computación en la nube es un modelo que permite a los usuarios acceder y administrar recursos informáticos como servidores, almacenamiento, bases de datos y software a través de Internet, en lugar de depender de hardware e infraestructura locales. Este modelo proporciona flexibilidad, escalabilidad y ahorro de costos al eliminar la necesidad de invertir en infraestructura física costosa. La computación en la nube generalmente se clasifica en tres modelos de servicio principales: *Infraestructura como servicio* (IaaS), *Plataforma como servicio* (PaaS) y *Software como servicio* (SaaS). Cada modelo ofrece diferentes niveles de control y administración, que se adaptan a diferentes necesidades y casos de uso.

Infraestructura como servicio (IaaS)

IaaS es el nivel más básico de servicios de computación en la nube. Proporciona recursos informáticos virtualizados a través de Internet, como máquinas virtuales, almacenamiento y redes. Con IaaS, los usuarios pueden alquilar estos recursos a pedido y ampliarlos o reducirlos según sus necesidades. Este modelo de servicio ofrece a los usuarios el mayor nivel de control, ya que los usuarios son responsables de administrar sus propios sistemas operativos, aplicaciones y datos, mientras que el proveedor de la nube se encarga de la infraestructura física subyacente.

La IaaS es ideal para empresas que necesitan recursos flexibles y escalables sin los gastos adicionales que supone comprar y mantener su propio hardware. Por ejemplo, una empresa podría utilizar la IaaS para poner en marcha rápidamente servidores virtuales para probar nuevas aplicaciones o para ampliar su infraestructura a fin de gestionar un aumento temporal del tráfico durante una campaña de marketing. Entre los proveedores de IaaS más populares se incluyen Amazon Web Services (AWS), Microsoft Azure y Google Cloud.

Plataforma como servicio (PaaS)

PaaS es un modelo de servicio en la nube que ofrece una plataforma para que los desarrolladores crean, implementen y administren aplicaciones sin preocuparse por la infraestructura subyacente. PaaS incluye todo lo que un desarrollador necesita para crear y ejecutar aplicaciones, como herramientas de desarrollo, middleware, bases de datos y sistemas operativos. Con PaaS, los usuarios pueden concentrarse en escribir código y crear funciones, mientras que el proveedor de la nube se encarga de administrar servidores, almacenamiento, redes y otros servicios de back-end.

PaaS es ideal para desarrolladores y empresas que desean optimizar el proceso de desarrollo y reducir la complejidad de la gestión de la infraestructura. Por ejemplo, un equipo de desarrollo podría utilizar PaaS para implementar rápidamente una nueva aplicación web sin necesidad de configurar servidores ni mantener bases de datos. Entre las ofertas de PaaS más populares se

incluyen Google App Engine, Microsoft Azure App Service y Heroku.

Software como servicio (SaaS)

SaaS es el modelo de servicio en la nube más fácil de usar y ampliamente adoptado. Con SaaS, los usuarios acceden a aplicaciones de software alojadas en la nube a través de un navegador web o una aplicación cliente, sin necesidad de instalar o administrar el software localmente. El proveedor de la nube se encarga de todos los aspectos de la administración del software, incluidas las actualizaciones, la seguridad y la infraestructura, lo que permite a los usuarios centrarse en el uso de la aplicación en sí.

El SaaS es ideal para empresas y particulares que desean utilizar software sin preocuparse por el mantenimiento, las actualizaciones o los detalles técnicos. Algunos ejemplos comunes de SaaS son los servicios de correo electrónico como Gmail, las herramientas de colaboración como Slack y los sistemas de gestión de relaciones con los clientes (CRM) como Salesforce. Las aplicaciones SaaS suelen ofrecerse mediante suscripción, lo que las hace accesibles y asequibles para empresas de todos los tamaños.

La computación en la nube ha revolucionado la forma en que las empresas y los individuos acceden y utilizan la tecnología, ofreciendo flexibilidad, escalabilidad y rentabilidad. Los tres modelos principales de servicios en la nube (IaaS, PaaS y SaaS) ofrecen distintos niveles de control y gestión, lo que permite a los usuarios elegir el modelo que mejor se adapta a sus necesidades. Ya sea alquilando infraestructura virtual con IaaS, desarrollando aplicaciones con PaaS o utilizando software totalmente administrado con SaaS, la computación en la nube proporciona un marco poderoso para las operaciones de TI modernas y la innovación.

Ejercicios guiados

1. ¿Cómo convierte el sistema de nombres de dominio (DNS) un nombre de dominio como `www.example.com` en una dirección IP? ¿Cuáles son las funciones del DNS directo y del DNS inverso, y en qué se diferencian?

2. ¿Cuáles son las diferencias entre Infraestructura como servicio (IaaS), Plataforma como servicio (PaaS) y Software como servicio (SaaS)? Proporcione un ejemplo de cada uno y explique el nivel de control que tiene el usuario en cada modelo.

Ejercicios exploratorios

1. Investigar y explicar algunos de los riesgos de seguridad más comunes asociados con el DNS, como la suplantación de DNS o el envenenamiento de caché. ¿Cómo funcionan estos ataques y qué medidas se pueden tomar para protegerse contra ellos?

2. Compare tres importantes proveedores de servicios en la nube (Amazon Web Services (AWS), Microsoft Azure y Google Cloud) en términos de sus ofertas de IaaS, PaaS y SaaS. ¿Cuáles son las principales diferencias en sus modelos de precios, servicios y audiencias objetivo?

 Esta obra está bajo la licencia CC BY-NC-ND 4.0. |

Resumen

Esta lección ofrece una exploración en profundidad de los protocolos de red fundamentales y los conceptos de computación en la nube. Comienza explicando los protocolos clave como TCP, UDP, ICMP y DHCP, centrándose en sus funciones en la comunicación de red. Luego, el texto detalla cómo funciona el DNS, traduciendo los nombres de dominio en direcciones IP mediante búsquedas directas e inversas. Además, enfatiza la importancia de los puertos TCP/UDP para dirigir el tráfico de red a los servicios y aplicaciones adecuados.

La lección finalmente pasa a cubrir los modelos de computación en la nube, explicando las diferencias entre Infraestructura como Servicio (IaaS), Plataforma como Servicio (PaaS) y Software como Servicio (SaaS). Estos modelos ofrecen distintos niveles de control y flexibilidad para empresas y desarrolladores, desde la gestión de infraestructura virtual con IaaS hasta la creación e implementación de aplicaciones con PaaS, pasando por el uso de aplicaciones totalmente administradas a través de SaaS.

Respuestas a los ejercicios guiados

1. ¿Cómo convierte el Sistema de nombres de dominio (DNS) un nombre de dominio como `www.example.com` en una dirección IP? ¿Cuáles son las funciones del DNS directo y del DNS inverso, y en qué se diferencian?

   El Sistema de nombres de dominio (DNS) traduce nombres de dominio legibles por humanos como `www.example.com` en direcciones IP como `192.0.2.1`, lo que permite que los dispositivos se comuniquen a través de Internet. En una búsqueda de DNS directo, el nombre de dominio se convierte en su dirección IP correspondiente, lo que permite que el dispositivo localice el servidor web correcto. Por el contrario, la búsqueda de DNS inversa toma una dirección IP y la resuelve en su nombre de dominio asociado, que a menudo se utiliza para verificar la identidad de un host, como en sistemas de correo electrónico o diagnósticos de red. Ambos procesos son esenciales para garantizar una comunicación fluida y la seguridad en Internet.

2. ¿Cuáles son las diferencias entre Infraestructura como servicio (IaaS), Plataforma como servicio (PaaS) y Software como servicio (SaaS)? Proporcione un ejemplo de cada uno y explique el nivel de control que tiene el usuario en cada modelo.

   IaaS proporciona recursos virtualizados, como servidores y almacenamiento, lo que brinda a los usuarios un control total sobre el sistema operativo y las aplicaciones. AWS EC2 es un ejemplo destacado de IaaS.

   PaaS ofrece una plataforma para que los desarrolladores creen e implementen aplicaciones sin administrar la infraestructura, donde el control se limita a la capa de aplicación. Google App Engine es un ejemplo destacado de PaaS.

   SaaS ofrece software completamente administrado a través de Internet, y los usuarios simplemente acceden a la aplicación sin control sobre la infraestructura o la administración del software. Gmail es un ejemplo destacado de SaaS.

Respuestas a los ejercicios exploratorios

1. Investigue y explique algunos de los riesgos de seguridad más comunes asociados con DNS, como la suplantación de DNS o el envenenamiento de caché. ¿Cómo funcionan estos ataques y qué medidas se pueden tomar para protegerse contra ellos?

   Los riesgos de seguridad de DNS, como la suplantación de DNS y el envenenamiento de caché, ocurren cuando los atacantes manipulan las respuestas de DNS para redirigir a los usuarios a sitios maliciosos. En la suplantación de DNS, el atacante falsifica las respuestas de DNS para hacer creer al dispositivo de la víctima que se está conectando a un dominio legítimo, mientras que en realidad se está redirigiendo a un servidor dañino. El envenenamiento de caché funciona corrompiendo el caché de DNS en un servidor, lo que hace que almacene y devuelva direcciones IP incorrectas para los nombres de dominio. Para protegerse contra estos ataques, se pueden implementar técnicas como DNSSEC (extensiones de seguridad de DNS) para verificar la autenticidad de las respuestas de DNS, y el vaciado regular de caché puede ayudar a minimizar los riesgos de envenenamiento de caché. Además, el uso de consultas DNS cifradas a través de protocolos como DNS sobre HTTPS (DoH) puede ayudar a prevenir la interceptación y manipulación del tráfico de DNS.

2. Compare tres importantes proveedores de servicios en la nube: Amazon Web Services (AWS), Microsoft Azure y Google Cloud, en términos de sus ofertas para IaaS, PaaS y SaaS. ¿Cuáles son las principales diferencias en sus modelos de precios, servicios y audiencias objetivo?

   Amazon Web Services (AWS), Microsoft Azure y Google Cloud son los tres principales proveedores de servicios en la nube, cada uno de los cuales ofrece soluciones IaaS, PaaS y SaaS. AWS es conocido por su extensa infraestructura global y una amplia gama de servicios, lo que lo hace popular entre las grandes empresas. Su modelo de precios es muy flexible y ofrece opciones de pago por uso. Microsoft Azure está estrechamente integrado con otros productos y servicios de Microsoft, lo que lo convierte en una opción sólida para las empresas que ya utilizan una infraestructura basada en Windows. Su precio también sigue un modelo de pago por uso, pero es particularmente competitivo para las empresas que utilizan software de Microsoft. Google Cloud, por otro lado, enfatiza el análisis de datos y el aprendizaje automático.

024.2 Seguridad de redes e Internet

Referencia al objetivo del LPI

Security Essentials version 1.0, Exam 020, Objective 024.2

Peso

3

Áreas de conocimiento clave

- Comprensión de las implicaciones del acceso a la capa de enlace
- Comprensión de los riesgos y uso seguro de redes WiFi
- Comprensión de los conceptos de interceptación de tráfico
- Comprensión de las amenazas de seguridad comunes en Internet junto con los enfoques de mitigación

Lista parcial de archivos, términos y utilidades

- Capa de enlace
- WiFi público y sin cifrar
- Seguridad y encriptación WiFi
- WEP, WPA, WPA2
- Interceptación de tráfico
- Ataques de hombre en el medio
- Ataques DoS y DDoS
- Botnets
- Filtros de paquetes

Linux Professional Institute

Lección 1

Certificado:	Fundamentos de seguridad
Versión:	1.0
Tema:	024 Seguridad de redes y servicios
Objetivo:	024.2 Seguridad de redes e Internet
Lección:	1 de 1

Introducción

En el mundo interconectado de hoy, comprender los aspectos fundamentales de la seguridad de la red es esencial para salvaguardar los datos y mantener la integridad de las comunicaciones. Un área crucial a considerar son las implicaciones del acceso a la capa de enlace, que puede exponer vulnerabilidades en la capa más baja de la red, lo que potencialmente permite a los atacantes interceptar o manipular el tráfico. De manera similar, los riesgos y el uso seguro de las redes Wi-Fi son cada vez más importantes a medida que la conectividad inalámbrica se vuelve omnipresente, y las redes mal configuradas o desprotegidas presentan oportunidades para el acceso no autorizado.

Otra área crítica de atención es la interceptación de tráfico, donde los atacantes espían o alteran el tráfico de la red, lo que plantea riesgos significativos para la confidencialidad e integridad de los datos. Por último, comprender las amenazas de seguridad comunes en Internet, como los ataques de denegación de servicio, los ataques de intermediario y las redes de bots, junto con las estrategias de mitigación adecuadas, es vital para que los profesionales de TI protejan los sistemas de las amenazas cibernéticas en evolución. En conjunto, estos temas forman la columna vertebral de la seguridad de la red, lo que ayuda a prevenir el acceso no autorizado y garantizar una comunicación segura en los entornos digitales.

Acceso a la capa de enlace

La *capa de enlace* es la segunda capa del modelo OSI de redes. Se encarga de los aspectos físicos y de enlace de datos de la comunicación en red. Esta capa es responsable de la forma en que se transmiten los datos a través de un segmento de red local, y gestiona aspectos como la transmisión de tramas, la detección de errores y el control de flujo. Los dispositivos de una red se comunican a través de la capa de enlace mediante protocolos como Ethernet o Wi-Fi. El acceso a esta capa es fundamental para controlar la forma en que se transmiten los datos entre dispositivos de la misma red local.

Sin embargo, el acceso no autorizado a la capa de enlace puede suponer importantes riesgos de seguridad. Un atacante que obtenga acceso a esta capa podría interceptar, manipular o inyectar tráfico en la red. Esto podría permitirle realizar una variedad de ataques, como el *sniffing de paquetes*, en el que el atacante captura y analiza paquetes de datos, o un *ataque de intermediario*, en el que intercepta y posiblemente altera las comunicaciones entre dos dispositivos sin que las partes se den cuenta. Estos ataques pueden provocar filtraciones de datos, acceso no autorizado a información confidencial o incluso la interrupción de los servicios de red.

Para mitigar los riesgos asociados con el acceso a la capa de enlace es necesario proteger la infraestructura de red física, implementar mecanismos de autenticación sólidos y utilizar cifrado. Por ejemplo, se puede habilitar la *seguridad de puertos* en los conmutadores para limitar el acceso a los dispositivos autorizados y se puede emplear la *segmentación de red* para limitar el alcance de posibles ataques.

Todavía existe un riesgo inherente en la capa de datos, que es el envenenamiento del protocolo de resolución de direcciones (ARP). El ARP se utiliza para asignar direcciones IP a direcciones MAC en una red local, y un atacante puede aprovechar esto enviando mensajes ARP falsificados para asociar su dirección MAC con la dirección IP de otro dispositivo. Esto le permite al atacante interceptar o alterar el tráfico destinado a ese dispositivo.

En las redes Wi-Fi, los desafíos de proteger la capa de datos y de enlace son aún mayores debido a la física de la comunicación inalámbrica, donde los datos se transmiten a través de ondas de radio abiertas.

Redes Wi-Fi

Las redes Wi-Fi ofrecen comodidad y flexibilidad, ya que permiten que los dispositivos se conecten a Internet de forma inalámbrica. Sin embargo, también presentan riesgos de seguridad importantes, especialmente cuando no están protegidas adecuadamente. Una de las principales preocupaciones surge con las redes Wi-Fi públicas y sin cifrar, que suelen encontrarse en espacios públicos como cafeterías, aeropuertos y hoteles. Estas redes suelen proporcionar acceso abierto a

cualquier persona que se encuentre dentro del alcance y, como carecen de cifrado, los datos que se transmiten a través de ellas son vulnerables a la interceptación. Los atacantes pueden supervisar fácilmente el tráfico de la red y capturar información confidencial, como credenciales de inicio de sesión, datos personales o detalles financieros, utilizando técnicas como el rastreo de paquetes. Las redes Wi-Fi públicas son un objetivo principal para los ciberdelincuentes que buscan explotar estas vulnerabilidades.

Para mitigar estos riesgos, se debe implementar la seguridad y el cifrado de Wi-Fi para garantizar que los datos transmitidos entre los dispositivos y la red estén protegidos. El cifrado codifica los datos de modo que, incluso si son interceptados, no se pueden leer ni entender sin la clave de descifrado correcta. Con el tiempo, se han desarrollado varios estándares de cifrado para mejorar la seguridad de las redes Wi-Fi. Uno de los primeros fue Wired Equivalent Privacy (WEP), pero rápidamente se descubrió que no era seguro debido a fallas que permitían a los atacantes vulnerar su cifrado fácilmente. Como resultado, WEP ahora se considera obsoleto y no se debe utilizar.

La introducción del Acceso Protegido Wi-Fi (WPA) mejoró la seguridad al abordar muchas de las debilidades de WEP. WPA utilizaba el *Protocolo de Integridad de Clave Temporal* (TKIP) para cambiar dinámicamente la clave de cifrado con cada paquete, lo que dificultaba su descifrado por los atacantes. Sin embargo, WPA aún tenía vulnerabilidades, lo que llevó al desarrollo de WPA2, el estándar de cifrado más utilizado en la actualidad. WPA2 utiliza el Estándar de cifrado avanzado (AES), que ofrece un nivel de cifrado mucho más fuerte que sus predecesores y sigue siendo el estándar de la industria para la seguridad Wi-Fi.

A pesar de la solidez de WPA2, no es totalmente inmune a los ataques y, con el aumento de amenazas cibernéticas más sofisticadas, se han introducido estándares más nuevos como WPA3. WPA3 proporciona un cifrado aún más fuerte y una mejor protección contra ataques de fuerza bruta. En entornos seguros, el uso del último estándar de cifrado y contraseñas seguras es crucial para garantizar la confidencialidad e integridad de los datos transmitidos a través de redes Wi-Fi. Actualizar periódicamente los enrutadores y el equipo de red para que admitan los protocolos de seguridad más recientes también ayuda a protegerse contra amenazas emergentes, lo que garantiza que las redes inalámbricas permanezcan seguras frente al acceso no autorizado.

Intercepción de tráfico

La interceptación de tráfico se produce cuando un usuario no autorizado, conocido como atacante, se introduce entre los puntos de comunicación de los nodos de una red. Esto también se puede denominar ataque de intermediario. Las formas de interceptación de tráfico pueden ser un ataque pasivo o activo contra los hosts de la red.

Intercepción pasiva del tráfico

Un *ataque pasivo* o *intercepción pasiva de tráfico* ocurre cuando un atacante escucha a escondidas las transacciones de red entre los hosts de una red. Es probable que el atacante pase desapercibido porque la información entre los hosts parece intacta, pero está siendo monitoreada y analizada por un intermediario.

Los motivos de un interceptor pasivo de tráfico pueden variar, incluido el robo de información para ventas o el intento de empresas rivales de obtener una ventaja competitiva en Internet. La interceptación pasiva de tráfico es relativamente difícil de detectar porque no altera los datos transmitidos a través de la red y la información se envía y recibe normalmente. Una posible solución es no detectar, sino prevenir este tipo de ataque cifrando la información que viaja a través de los puntos de la red. Sin embargo, conocer los patrones de comunicación y el tipo de comunicación que se está transmitiendo puede proporcionar información valiosa a un atacante en algunas situaciones.

TIP Los comandos `tcpdump` o `wireshark` se pueden usar para monitorear y analizar el tráfico en la red.

Intercepción de tráfico activo

Se puede decir que una interceptación de tráfico es un ataque *activo* si implica la modificación de datos en tránsito a través de una red. En esencia, la interceptación no es solo una escucha clandestina, como en el caso de los ataques pasivos, sino que también puede implicar ataques como una *suplantación de ARP* en una conexión LAN o la reproducción de datos de autenticación válidos capturados mediante secuencias de comandos entre sitios (principalmente para actuar como otro usuario en la red y, por lo tanto, usurpar los privilegios autorizados de dicho usuario).

La interceptación activa de tráfico es un ataque activo que también podría implicar la modificación, redirección o retraso de mensajes en tránsito entre los hosts emisores y receptores de una red. Un ejemplo es cuando se envía un mensaje que dice “Permitir a Jane Smith editar la cuenta del perfil”, pero lo que se recibe es “Permitir a John Doe editar la cuenta del perfil”, alterando así la integridad de la información. La idea principal es que el atacante modifique el mensaje para adaptarlo a sus propias intenciones, que podrían ser intentos sutiles de obtener mayores privilegios.

Los ataques de interceptación de tráfico pasivos y activos requieren, en cierta medida, protecciones opuestas. Si bien los administradores y los usuarios deben prevenir el ataque pasivo en lugar de detectarlo, deben detectar un ataque activo y tomar medidas lo antes posible para remediar la situación y evitar más daños en la red.

TIP Los comandos `arp` o `nmap` se pueden usar para obtener información sobre los hosts

vecinos en la red.

Ataques DoS y DDoS

La denegación de servicio (DoS) es una forma de ataque activo que se produce cuando se niega a los usuarios autorizados el acceso a un sistema informático, una red o información específica. Esto se debe a un ataque a la red o a un sistema en particular. Para llevar a cabo este ataque, un atacante puede explotar una vulnerabilidad conocida en una aplicación específica del sistema o en el sistema operativo que se ejecuta en el host. La explotación suele adoptar la forma de que el atacante inunde el sistema con tantas solicitudes que la máquina se sobrecarga y bloquea el sistema, lo que lo deja fuera de línea o lo deja inutilizable para los usuarios autorizados.

Cuando se lanza un ataque de denegación de servicio en un host específico, el objetivo podría ser impedir el acceso al host o, cuando se combina con otras acciones, comprometer el sistema informático. También podría usarse para obtener acceso no autorizado al sistema informático o a la red. Algunos ejemplos de ataques DoS incluyen la *inundación SYN (SYN flooding)* y el *Ping de la muerte (Ping of Death)*.

En el caso de la inundación SYN, un ataque aprovecha el protocolo TCP/IP utilizado para la comunicación entre dos hosts. Básicamente, el ataque consiste en inundar el host con solicitudes para que no tenga tiempo de descartar las solicitudes no respondidas en la secuencia de comunicación SYN, SYN/ACK y ACK. La solicitud ACK completa el protocolo de enlace de tres vías, pero como la conexión inicial proviene de una dirección IP falsa, el host no emite una respuesta ACK y continúa esperando. Pronto, se acumulan más solicitudes hasta que el host ya no puede manejar más solicitudes, lo que impide que se procesen en ese host las solicitudes genuinas de los usuarios autorizados.

Ping of Death es otro ataque DoS que envía paquetes ICMP (Internet Control Message Protocol) de gran tamaño a un host objetivo. Los paquetes de datos normalmente deberían tener menos de 65.536 bytes (o 64 kilobytes), pero cuando el tamaño del paquete es mayor que esto y se envía a un host que no puede manejar un tamaño de paquete tan grande, el sistema se congelará o bloqueará y no estará disponible para los usuarios autorizados.

Los ataques DoS suelen ejecutarse por un único sistema atacante. Sin embargo, cuando se han empleado varios sistemas para atacar al objetivo, se habla de denegación de servicio distribuida (DDoS). En los ataques DDoS, el atacante infecta varios sistemas y hace que realicen funciones nefastas en su nombre. Esto puede ocurrir cuando los usuarios han sido engañados para que instalen software en su ordenador que permanece inactivo durante un tiempo sin que se den cuenta. El ataque también puede aprovecharse de sistemas que no han sido parcheados o actualizados contra las últimas vulnerabilidades conocidas. En cuanto se han infectado suficientes hosts, se lanza el ataque. Este ataque podría ser una inundación SYN, en la que varios hosts

infectados envían solicitudes de comunicación falsas a un servidor objetivo hasta que este se desgasta.

Una de las formas de prevenir un ataque DoS de inundación SYN es modificar el tiempo que un host espera antes de descartar solicitudes no utilizadas. También es una buena práctica asegurarse de que los sistemas estén parcheados con las últimas actualizaciones de seguridad. Existen herramientas que pueden detectar y deshacerse del software "zombi" inactivo, como algunos paquetes anti-spyware o antivirus. Si bien bloquear el protocolo ICMP podría ayudar a prevenir el Ping of Death, también podría ser un obstáculo para herramientas legítimas y útiles de resolución de problemas.

Bots y botnets

Un *bot* es un software que ejecuta tareas bajo el control de otro programa. Un grupo de bots que se operan y controlan a través de la red se denomina *botnet*. Una botnet se puede utilizar para realizar acciones legítimas y requeridas a través de la red, por ejemplo, al distribuir cargas de trabajo informáticas. Sin embargo, una botnet también se puede utilizar para acciones maliciosas y dañinas en la red, como los ataques DDoS analizados en la sección anterior. Las botnets también se pueden utilizar como software espía para robar información mediante registradores de pulsaciones de teclas a través de la red. Las botnets se pueden utilizar para enviar correos electrónicos no deseados, es decir, enviar mensajes no solicitados a un objetivo.

Por lo general, cuando un equipo está infectado por un malware de tipo bot, el usuario no es consciente de ello y puede propagar la infección a otros hosts de la red. Esto puede crear una gran red de bots que luego se utiliza para lanzar un ataque masivo contra un objetivo específico. Los desarrolladores de bots también son capaces de modificar sus bots para evadir las medidas de seguridad, como las listas negras de IP y las medidas de control de acceso, tomando direcciones IP de zonas residenciales y utilizándolas en diferentes ocasiones para evitar ser detectados. Todos los usuarios de Internet deberían instalar un software de seguridad dedicado, como paquetes antispyware y antivirus, y actualizarlos periódicamente. Estas herramientas deberían realizar comprobaciones de rutina para ayudar a prevenir una infección o un ataque. También es una buena práctica de seguridad no hacer clic en enlaces ni abrir mensajes de correo electrónico de fuentes poco claras, desconocidas o que no sean de confianza.

Filtros de paquetes y otras estrategias de mitigación de ataques a la red

Los *filtros de paquetes* pueden desempeñar un papel crucial en la mitigación de diversos ataques de red, como inundaciones SYN, denegación de servicio (DoS), denegación de servicio distribuida (DDoS), botnets y ataques de intermediarios. Un filtro de paquetes es un mecanismo de firewall

que inspecciona los paquetes entrantes y salientes en la capa de red, analizando sus encabezados para determinar si se deben permitir o bloquear según reglas de seguridad predefinidas.

Los filtros de paquetes pueden mitigar los ataques de inundación SYN, en los que un atacante sobrecarga un servidor enviando una cantidad masiva de solicitudes de conexión incompletas, limitando la cantidad de solicitudes SYN entrantes o implementando *cookies SYN*, que permiten que el servidor gestione más conexiones sin sobrecargar los recursos. Los filtros de paquetes también pueden detectar y bloquear las direcciones IP de atacantes conocidos, lo que impide que su tráfico llegue al servidor.

Para evitar ataques DoS y DDoS, los filtros de paquetes pueden identificar patrones de tráfico anormales (como una cantidad inusualmente alta de solicitudes desde una sola dirección IP o múltiples fuentes en un escenario DDoS) y bloquear o limitar la velocidad de ese tráfico. Esto evita que el servidor se vea sobrecargado por tráfico malicioso, mientras que las solicitudes legítimas continúan siendo procesadas.

En el caso de las botnets, que son redes de dispositivos infectados que se utilizan para lanzar ataques coordinados, los filtros de paquetes pueden detectar el tráfico procedente de direcciones IP de botnets conocidas o bloquear las comunicaciones de dispositivos que se comportan de forma sospechosa. Al bloquear el tráfico de comando y control (C2) que utilizan los operadores de botnets para gestionar los dispositivos infectados, los filtros de paquetes pueden reducir significativamente la eficacia de los ataques de botnets.

Por último, los filtros de paquetes pueden evitar los ataques de intermediario, en los que un atacante intercepta las comunicaciones entre dos dispositivos, al imponer conexiones seguras mediante protocolos como HTTPS o SSL/TLS, que cifran el tráfico. Los filtros también se pueden configurar para descartar paquetes sospechosos que parezcan ser parte de un ataque de intermediario, como aquellos con encabezados alterados o que se originan en fuentes no confiables.

Al configurar correctamente los filtros de paquetes, las organizaciones pueden reducir significativamente el riesgo de diversos tipos de ataques, mejorando la seguridad y la integridad de sus redes.

Ejercicios guiados

1. ¿Cuál es la diferencia entre un ataque DoS y un ataque DDoS?

2. ¿Cuáles son los riesgos potenciales del acceso no autorizado a la capa de enlace de una red y qué métodos de ataque específicos se pueden utilizar en esta capa?

3. ¿Cuál es la diferencia entre los estándares de cifrado WEP, WPA y WPA2 y por qué es importante utilizar los protocolos de cifrado más recientes en las redes Wi-Fi?

4. ¿Cómo pueden los filtros de paquetes ayudar a mitigar los ataques DoS y DDoS, y qué técnicas específicas utilizan para prevenir este tipo de ataques?

 Esta obra está bajo la licencia CC BY-NC-ND 4.0.

Ejercicios exploratorios

1. Mientras Henry está trabajando en su computadora, ve una ventana emergente rápida del símbolo del sistema y desaparece, después de lo cual todo lo demás parece estar normal en la computadora. Pero mientras revisa los procesos que se están ejecutando en la computadora, ve que también se está ejecutando un proceso extraño. ¿Qué es probable que sea y qué puede hacer de inmediato?

2. Henry intenta espiar el tráfico de red entre Dave y Carol, aunque su comunicación está cifrada. ¿Es posible?

3. ¿Qué tipo de interceptación de tráfico es el ataque descrito en el ejercicio anterior?

Resumen

En esta lección se analiza la seguridad de la red, comenzando por los riesgos del acceso a la capa de enlace y destacando ataques como el rastreo de paquetes, los ataques de intermediario y el envenenamiento de ARP. Se hace hincapié en la protección de la infraestructura física y el uso de una autenticación sólida.

La lección también aborda los riesgos de seguridad de las redes Wi-Fi públicas sin cifrar y la evolución de los estándares de cifrado de Wi-Fi, desde WEP hasta WPA2 y WPA3. Además, explica la interceptación de tráfico, distinguiendo entre ataques pasivos y activos. Por último, cubre los ataques DoS, DDoS y botnet, y cómo los filtros de paquetes pueden ayudar a mitigar estas amenazas al bloquear el tráfico sospechoso.

 Esta obra está bajo la licencia CC BY-NC-ND 4.0. |

Respuestas a los ejercicios guiados

1. ¿Cuál es la diferencia entre un ataque DoS y un ataque DDoS?

   Mientras que una denegación de servicio utiliza un solo sistema para atacar un objetivo, la denegación de servicio distribuida utiliza varias computadoras para realizar el ataque.

¿Cuáles son los riesgos potenciales del acceso no autorizado a la capa de enlace de una red y qué métodos de ataque específicos se pueden utilizar en esta capa?

+ El acceso no autorizado a la capa de enlace plantea riesgos de seguridad significativos, porque los atacantes pueden interceptar, manipular o inyectar tráfico en la red. Los métodos de ataque específicos incluyen el rastreo de paquetes, donde el atacante captura y analiza los datos transmitidos a través de la red, y los ataques de intermediario, donde el atacante intercepta y posiblemente altera las comunicaciones entre dispositivos. El envenenamiento de ARP es otro ataque común, donde el atacante falsifica los mensajes ARP para asociar su dirección MAC con la dirección IP de otro dispositivo, lo que le permite interceptar o modificar el tráfico destinado a ese dispositivo.

1. ¿Cuál es la diferencia entre los estándares de cifrado WEP, WPA y WPA2 y por qué es importante utilizar los protocolos de cifrado más recientes en las redes Wi-Fi?

   WEP es el estándar de cifrado Wi-Fi más antiguo y ahora se considera inseguro debido a fallas que permiten descifrar fácilmente su cifrado. WPA mejoró la seguridad al usar TKIP para cambiar dinámicamente las claves de cifrado, pero aún tenía vulnerabilidades. WPA2 es el estándar más utilizado en la actualidad y proporciona una seguridad más sólida al usar cifrado AES. Es importante utilizar los protocolos de cifrado más recientes, como WPA3, porque ofrecen una protección mejorada contra ataques de fuerza bruta y otras amenazas avanzadas, lo que garantiza la confidencialidad e integridad de los datos en las redes Wi-Fi.

2. ¿Cómo pueden los filtros de paquetes ayudar a mitigar los ataques DoS y DDoS, y qué técnicas específicas utilizan para prevenir este tipo de ataques?

   Los filtros de paquetes mitigan los ataques DoS y DDoS analizando los paquetes entrantes y salientes en la capa de red y bloqueando o limitando el tráfico que coincide con patrones sospechosos, como un gran volumen de solicitudes de una sola dirección IP o de múltiples fuentes. Para mitigar los ataques de inundación SYN, los filtros de paquetes pueden limitar la cantidad de solicitudes SYN o usar cookies SYN para manejar más conexiones sin sobrecargar el servidor. Para lidiar con los ataques DDoS, los filtros de paquetes ayudan identificando patrones de tráfico anormales y limitando la velocidad o bloqueando el tráfico malicioso mientras permiten que pase el tráfico legítimo.

Respuestas a los ejercicios exploratorios

1. Mientras Henry estaba trabajando en su computadora, vio una ventana emergente rápida del símbolo del sistema y desapareció, después de lo cual todo lo demás parecía estar normal en la computadora. Pero mientras revisaba los procesos que se estaban ejecutando en la computadora, vio que también se estaba ejecutando un proceso extraño. ¿Qué es probable que sea y qué puede hacer de inmediato?

   Es probable que se trate de un bot. La computadora debe analizarse con un software antivirus.

2. Henry intenta espiar el tráfico de red entre Dave y Carol a pesar de que su comunicación está cifrada. ¿Es posible?

   Sí, es posible obtener información del patrón del mensaje, el tipo de protocolo y el tiempo del tráfico a pesar de que el contenido del mensaje está cifrado.

3. ¿Qué tipo de interceptación de tráfico es el ataque descrito en el ejercicio anterior?

   La escucha clandestina del tráfico de la red es un ataque de interceptación de tráfico pasivo.

024.3 Cifrado y anonimato de red

Referencia al objetivo del LPI

Security Essentials version 1.0, Exam 020, Objective 024.3

Peso

3

Áreas de conocimiento clave

- Comprensión de las redes privadas virtuales (VPN)
- Comprensión de los conceptos de cifrado de extremo a extremo
- Comprender el anonimato y el reconocimiento en Internet
- Identificación debida a direcciones de capa de enlace e IPs
- Comprensión de los conceptos de servidores proxy
- Comprensión de los conceptos de TOR
- Conocimiento sobre la Darknet
- Conocimiento de las criptomonedas y sus aspectos de anonimato

Lista parcial de archivos, términos y utilidades

- Red privada virtual (VPN)
- Proveedores de VPN públicos
- VPN específica de la organización (por ejemplo, VPN de empresa o universidad)
- Cifrado de extremo a extremo
- Cifrado de transferencia
- Anonimato

- Servidores proxy
- TOR
- Servicio oculto
- .onion
- Cadena de bloques

Linux Professional Institute

Lección 1

Certificado:	Fundamentos de seguridad
Versión:	1.0
Tema:	024 Seguridad de redes y servicios
Objetivo:	024.3 Cifrado y anonimato en redes
Lección:	1 de 2

Introducción

En el mundo interconectado de hoy, la necesidad de una comunicación segura y privada se ha vuelto más crítica que nunca. Con las crecientes amenazas a la privacidad de los datos y la ciberseguridad, las personas y las organizaciones buscan soluciones sólidas para proteger su información confidencial y mantener la confidencialidad. Una de las tecnologías clave que permiten una comunicación segura a través de redes públicas es la red privada virtual (VPN). Al crear un túnel cifrado entre el dispositivo de un usuario y la red de destino, una VPN garantiza que los datos permanezcan a salvo de escuchas y accesos no autorizados. Esto hace que las VPN sean una herramienta esencial para cualquiera que busque proteger sus actividades en línea o acceder a recursos restringidos de forma remota.

La versatilidad y adaptabilidad de la tecnología VPN la han hecho popular entre usuarios individuales y empresas, atendiendo a diversos casos de uso que van desde la privacidad personal hasta la seguridad corporativa.

A pesar de sus beneficios, las VPN no son una solución universal. Comprender los diferentes tipos de VPN, sus casos de uso y sus limitaciones es fundamental para elegir el servicio adecuado que satisfaga sus necesidades específicas. En esta lección, se exploran los distintos aspectos de las VPN,

incluida su funcionalidad, sus usos y las tecnologías que las sustentan, y se ofrece una descripción general completa de cómo contribuyen a la seguridad digital moderna.

Introducción a las redes privadas virtuales (VPN)

Una red privada virtual (VPN) crea una conexión segura y cifrada a través de una red menos segura, como Internet. Las VPN protegen los datos confidenciales, mantienen la privacidad y permiten acceder a recursos restringidos según la ubicación geográfica o la segmentación de la red. Básicamente, una VPN establece un túnel seguro entre el dispositivo del usuario y la red de destino, lo que garantiza que los datos transmitidos a través de este túnel estén protegidos contra escuchas y accesos no autorizados.

La funcionalidad principal de una VPN se basa en el uso de protocolos de cifrado que salvaguardan la integridad y confidencialidad de los datos. Protocolos como *IPsec* (Internet Protocol Security), *OpenVPN* y *WireGuard* se utilizan habitualmente para establecer estas conexiones seguras. Estos protocolos cifran los datos en un extremo del túnel y los descifran en el otro, lo que impide que los datos interceptados sean legibles.

Las VPN se pueden clasificar en dos categorías principales: VPN públicas y VPN específicas para organizaciones. Cada una tiene un propósito único y está diseñada para distintos casos de uso, según los requisitos del usuario o la organización.

Proveedores de VPN públicos

Los proveedores de VPN públicos ofrecen servicios a usuarios individuales que desean proteger su tráfico de Internet, ocultar su dirección IP o eludir las restricciones impuestas por su ubicación geográfica. Estos proveedores mantienen redes de servidores en todo el mundo y permiten a los usuarios conectarse a través de diferentes ubicaciones geográficas, ocultando de manera eficaz su ubicación real. Esto resulta especialmente útil para acceder a contenido restringido a ciertos países o para evitar la censura en regiones restrictivas.

Las VPN públicas también son útiles para proteger las conexiones a Internet en redes Wi-Fi públicas. Cuando se conectan a un punto de acceso Wi-Fi no seguro, los usuarios son vulnerables a diversos ataques, como ataques de intermediario, en los que un atacante puede interceptar y potencialmente alterar los datos que se transmiten. Cuando se utiliza una VPN pública, todo el tráfico entre el usuario y el servidor VPN está cifrado, lo que reduce significativamente el riesgo de que los datos se vean comprometidos.

Sin embargo, si bien las VPN públicas ofrecen comodidad y seguridad para uso personal, no están exentas de riesgos. Los usuarios deben ser cautelosos al seleccionar un proveedor de VPN, ya que algunos pueden registrar la actividad del usuario, vender datos a terceros o incluso verse

comprometidos. Es fundamental elegir un proveedor de confianza que tenga una política clara y estricta de no guardar registros, utilice estándares de cifrado sólidos y sea transparente en cuanto a sus operaciones y políticas.

VPN específicas de la organización

Las VPN específicas para cada organización están diseñadas para satisfacer las necesidades de seguridad y conectividad de empresas, instituciones educativas y otras entidades que requieren acceso remoto a sus redes internas. Estas VPN permiten que los empleados, estudiantes y personal autorizado se conecten de forma segura a la red de la organización desde ubicaciones remotas. Esto es particularmente importante para acceder a recursos confidenciales, como bases de datos internas, intranets o aplicaciones propietarias, sin exponerlos a Internet en general.

Las VPN de empresas y universidades suelen requerir autenticación mediante credenciales de usuario, certificados o autenticación multifactor (MFA) para verificar la identidad del usuario que se conecta. Una vez que el usuario está autenticado, la VPN crea un túnel seguro entre el dispositivo del usuario y la red de la organización, lo que garantiza que todos los datos transmitidos estén protegidos contra interceptaciones y manipulaciones.

Además de proporcionar acceso seguro, las VPN específicas de la organización pueden aplicar políticas de seguridad, como restringir el acceso en función del rol del usuario, la ubicación o la conformidad del dispositivo. Por ejemplo, una VPN de la empresa podría permitir conexiones solo desde dispositivos administrados que tengan un software antivirus actualizado y cumplan con los estándares de seguridad de la organización.

Una VPN corporativa es a menudo una *VPN de acceso remoto*, que permite a los usuarios remotos conectarse de forma segura a la red de la organización como si estuvieran físicamente en la oficina (<<remote-access-vpn> >). Este tipo de VPN basada en extranet es comúnmente utilizada por empleados que trabajan desde casa o viajan, lo que les permite acceder a recursos internos. Por ejemplo, un empleado puede usar una VPN de acceso remoto para conectarse a la intranet de la empresa mientras trabaja desde una cafetería, lo que garantiza que la información confidencial permanezca cifrada y protegida incluso en redes Wi-Fi públicas no seguras.

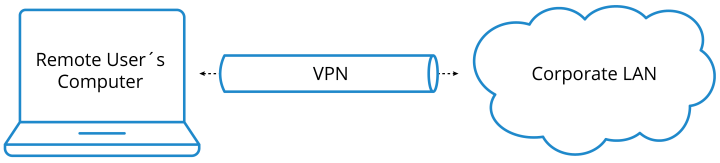

Figure 35. VPN de acceso remoto

Por otro lado, las *VPN de sitio a sitio*, conectan redes enteras en diferentes ubicaciones físicas, proporcionando un canal de comunicación seguro entre ellas (<<site-to-site-vpn> >). Este tipo de

VPN basada en intranet generalmente vincula sucursales o redes de socios a la red corporativa principal. Por ejemplo, una empresa multinacional podría utilizar una VPN de sitio a sitio para conectar sus oficinas en diferentes países, lo que permite una comunicación fluida y el intercambio de datos entre ellas sin exponer el tráfico interno a Internet público. Al utilizar VPN de sitio a sitio, las organizaciones pueden crear una infraestructura de red unificada y segura, lo que facilita la colaboración y el intercambio de recursos en ubicaciones geográficamente dispersas.

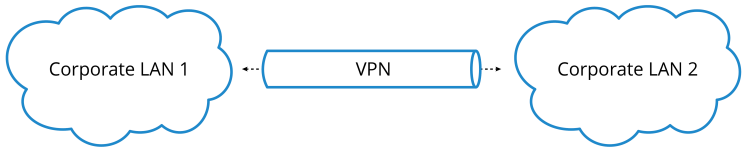

Figure 36. VPN sitio a sitio

Conceptos de cifrado de extremo a extremo y cifrado de transferencia

El *cifrado de extremo a extremo* (E2EE) y el *de transferencia* son partes integrales de los mecanismos de seguridad empleados en las VPN, ya que ambos dependen del cifrado para proteger los datos durante la transmisión. Las VPN crean un túnel seguro entre el dispositivo de un usuario y un servidor remoto, lo que garantiza que todos los datos que pasan por este túnel permanezcan cifrados. En general, el cifrado de transferencia protege los datos mientras viajan entre el dispositivo del usuario y el servidor VPN.

Cifrado de transferencia

El cifrado de transferencia, también conocido como cifrado en tránsito, se centra en proteger los datos a medida que se transfieren entre sistemas, como entre el navegador de un usuario y un servidor web o entre dos servidores dentro de una red. El cifrado de transferencia garantiza que los datos no puedan ser interceptados ni leídos por terceros no autorizados mientras se transmiten.

Por ejemplo, cuando un usuario se conecta a una VPN corporativa, se suelen utilizar protocolos como IPsec u OpenVPN para cifrar los datos en el origen y descifrarlos solo al llegar al servidor VPN. Este cifrado evita que terceros intercepten y accedan al contenido de la comunicación entre el usuario y el servidor VPN. Sin embargo, una vez que los datos llegan al servidor VPN, se descifran y se reenvían a su destino previsto. Esto significa que una VPN ofrece cifrado para los datos durante su recorrido hasta el servidor VPN, pero no proporciona inherentemente cifrado de extremo a extremo en toda la ruta de comunicación. Por ejemplo, cuando un usuario envía una solicitud a un sitio web o una aplicación remota a través de una VPN, solo se cifra el tráfico entre

el usuario y el servidor VPN, lo que deja los datos vulnerables a una posible interceptación más allá del servidor VPN.

Como otro ejemplo, cuando un visitante accede a un sitio web seguro (indicado por “https” en la URL), el cifrado de transferencia garantiza que todos los datos intercambiados entre el navegador del visitante y el servidor del sitio web estén cifrados y protegidos contra escuchas o manipulaciones no autorizadas. Esto es crucial para proteger la información confidencial, como las credenciales de inicio de sesión o los detalles de pago, de ser interceptada por atacantes durante la transmisión. En HTTPS, los datos se cifran entre el navegador del visitante y el servidor, pero el servidor aún tiene acceso a los datos no cifrados una vez que llegan. Esto se debe a que el servidor tiene las claves de descifrado. Por lo tanto, si bien HTTPS protege sus datos de las escuchas no autorizadas durante el tránsito, no los protege del servidor en sí.

El cifrado de transferencia a menudo se combina con otras medidas de seguridad para proporcionar una defensa en capas para los datos en entornos de red complejos.

Cifrado de extremo a extremo

El cifrado de extremo a extremo (E2EE) proporciona un mayor nivel de seguridad al garantizar que los datos se cifran en el dispositivo del remitente y se descifran solo en el dispositivo del destinatario, sin que ningún intermediario tenga acceso a la información no cifrada. Este enfoque es particularmente eficaz para evitar que terceros, incluidos los proveedores de servicios o los piratas informáticos, vean o alteren los datos transmitidos. El E2EE se utiliza ampliamente en aplicaciones de mensajería segura, servicios de correo electrónico y plataformas de intercambio de archivos. Por ejemplo, en una aplicación de mensajería segura, el mensaje se cifra en el dispositivo del remitente y permanece cifrado durante todo su tránsito hasta que llega al destinatario, donde finalmente se descifra. Incluso si el mensaje se intercepta durante su transmisión, sería ilegible sin las claves de descifrado específicas, que se almacenan solo en los dispositivos de comunicación.

Una de las principales ventajas de E2EE es que protege los datos tanto en tránsito como en reposo (almacenados en el dispositivo de destino). Esto significa que, incluso si el servidor del proveedor de servicios se ve comprometido, los datos siguen siendo inaccesibles para terceros no autorizados.

Si bien las VPN brindan un cifrado sólido para los datos en tránsito, no ofrecen la misma protección integral que E2EE porque no cubren toda la cadena de comunicación. Para lograr la máxima seguridad, se recomienda utilizar VPN junto con servicios de cifrado de extremo a extremo. Este enfoque en capas garantiza que los datos permanezcan protegidos no solo mientras atraviesan el túnel VPN, sino también cuando llegan a su destino final.

Anonimato y reconocimiento en Internet

El anonimato y el reconocimiento en Internet son conceptos complejos que giran en torno a cómo se puede identificar a los usuarios o cómo se puede permanecer ocultos mientras navegan por la web. Internet no se diseñó originalmente con el anonimato en mente; en cambio, sus protocolos fundamentales se centran en la conectividad y la transferencia de datos. Esto significa que a cada dispositivo conectado a Internet se le asigna un identificador, como una dirección IP o una dirección de capa de enlace, que se puede utilizar para rastrear su actividad e interacciones. Comprender estos conceptos es fundamental para comprender cómo se puede comprometer el anonimato y qué medidas se pueden tomar para preservarlo.

Direcciones de capa de enlace y direcciones IP

Los dispositivos conectados a una red se identifican mediante direcciones únicas en diferentes capas de comunicación. En la capa de enlace, cada tarjeta de interfaz de red (NIC) tiene una dirección de control de acceso a medios (MAC) única. Esta dirección se utiliza para la comunicación dentro de la red local y se puede utilizar para identificar un dispositivo específico en esa red. Aunque la dirección MAC normalmente no se transmite más allá de la red local, los administradores de red o actores maliciosos dentro del mismo segmento de red pueden utilizarla para rastrear y monitorear la actividad del dispositivo.

En la *capa de red*, a los dispositivos se les asignan direcciones de *protocolo de Internet* (IP), que pueden ser estáticas o dinámicas. Las direcciones IP son fundamentales para enrutar datos a través de Internet, pero también sirven como identificador digital para los dispositivos. Cuando visita un sitio web, el servidor registra su dirección IP y luego la puede usar para aproximar su ubicación geográfica, determinar su proveedor de servicios de Internet y rastrear su comportamiento en línea.

Aunque las direcciones IP por sí solas no revelan su identidad personal, pueden vincularse con usted a través de puntos de datos adicionales, como inicios de sesión en cuentas, hábitos de navegación o interacciones con otros sitios web. Vincular las direcciones IP a personas individuales compromete el anonimato y permite el reconocimiento y la elaboración de perfiles de los usuarios.

Anonimato en Internet

El anonimato en Internet significa utilizar la web sin revelar su verdadera identidad o sin que le rastreen fácilmente. Para lograrlo es necesario ocultar u ofuscar los identificadores que se utilizan normalmente para rastrear a los usuarios, como las direcciones IP y las direcciones de la capa de enlace. Un método habitual para lograr el anonimato es a través de redes de anonimato como Tor (The Onion Router), que enruta el tráfico de Internet a través de una serie de servidores operados

por voluntarios, ocultando su dirección IP y dificultando el rastreo de sus actividades hasta llegar a usted.

Otro método es utilizar una red privada virtual (VPN), que enmascara tu dirección IP al enrutar tu tráfico a través de un servidor seguro. Si bien una VPN proporciona cierto nivel de anonimato al ocultar tu dirección IP a los sitios web que visitas, no es completamente infalible. El propio proveedor de VPN puede ver tu dirección IP real y rastrear tu actividad, por lo que es importante elegir un proveedor confiable con una estricta política de no guardar registros.

Los servidores proxy también se pueden utilizar para lograr un cierto grado de anonimato. Al utilizar un proxy, su dirección IP se reemplaza con la dirección IP del servidor proxy, enmascarando su verdadera ubicación e identidad. Esto puede ser particularmente útil para eludir restricciones geográficas o acceder a contenido que puede estar bloqueado en ciertas regiones. Sin embargo, al igual que las VPN, los proxies no ofrecen un anonimato completo, ya que el servidor proxy puede registrar y potencialmente revelar la actividad del usuario. Para mantener un mayor nivel de privacidad, es fundamental utilizar proxies que no guarden registros y combinarlos con otras herramientas de privacidad como Tor o VPN.

Mantener el anonimato también implica utilizar herramientas y prácticas centradas en la privacidad, como desactivar las cookies que rastrean tus actividades en la web, utilizar navegadores anónimos como Tor y evitar credenciales de inicio de sesión que puedan vincularse a tu identidad real. A pesar de estas medidas, el verdadero anonimato en Internet es difícil de lograr, ya que aún se pueden utilizar diversas tecnologías y técnicas, como la identificación de navegadores y el análisis de metadatos, para identificar a los usuarios.

Servidores proxy

Un *servidor proxy* actúa como intermediario entre el dispositivo de un usuario e Internet. Cuando un usuario se conecta a Internet a través de un servidor proxy, todas las solicitudes y respuestas se enrutan a través del proxy antes de llegar al destino previsto. Esto puede tener varios propósitos, como mejorar la seguridad, mejorar el rendimiento y mantener el anonimato. Cuando el tráfico pasa por un proxy, la dirección IP del usuario se oculta a los sitios web que visita y, en su lugar, se muestra la dirección IP del proxy, lo que enmascara de manera eficaz la identidad y la ubicación del usuario.

Los servidores proxy se pueden configurar para distintos niveles de anonimato y funcionalidad. Algunos servidores proxy simplemente reenvían solicitudes sin ninguna modificación, mientras que otros filtran el contenido, almacenan en caché datos a los que se accede con frecuencia o incluso modifican los datos entrantes y salientes. Esta flexibilidad hace que los servidores proxy sean una herramienta popular para diversos casos de uso, como eludir restricciones geográficas, filtrar el tráfico de Internet y controlar el acceso de los usuarios a los recursos de la red.

Tipos de servidores proxy

Los servidores proxy vienen en varias formas, cada una adaptada a necesidades y casos de uso específicos. Un *proxy de reenvío* es el tipo más común, en el que el servidor proxy maneja las solicitudes de un cliente (como un navegador web) a Internet. Este tipo de proxy se utiliza a menudo en entornos corporativos para controlar y supervisar el uso de Internet por parte de los empleados o para eludir las restricciones de contenido. Por ejemplo, una organización podría utilizar un proxy de reenvío para restringir el acceso a los sitios de redes sociales durante el horario laboral.

Por otro lado, un *proxy reverso* se ubica frente a los servidores web y maneja las solicitudes de los clientes en nombre de esos servidores. Esto se usa generalmente para equilibrar la carga: distribuir el tráfico entrante entre varios servidores para garantizar que ningún servidor se vea sobrecargado. Los proxy inversos también pueden brindar seguridad adicional al ocultar la estructura interna de la red de servidores a los usuarios externos. Por ejemplo, un sitio web que usa un proxy inverso puede proteger sus servidores de origen de ataques directos, ya que el proxy actúa como un escudo.

Los *proxies anónimos* y los *proxies de alto anonimato* ofrecen distintos niveles de privacidad para el usuario. Los proxies anónimos ocultan la dirección IP del usuario pero se identifican como proxies, mientras que los proxies de alto anonimato, también conocidos como *proxies de élite*, no revelan que son servidores proxy, lo que dificulta que los sitios web los detecten y bloqueen.

Casos de uso

Los servidores proxy se utilizan ampliamente en diversos escenarios para mejorar la seguridad, la privacidad y el control del tráfico de Internet. En entornos corporativos, los servidores proxy pueden aplicar políticas de uso aceptable al bloquear el acceso a sitios web inapropiados o improductivos. También se pueden utilizar para supervisar y registrar la actividad de los usuarios con fines de cumplimiento y seguridad. Por el contrario, las personas pueden utilizar servidores proxy para eludir la censura de Internet, acceder a contenido bloqueado por región o mantener el anonimato mientras navegan por la web.

Además, los servidores proxy se utilizan para la extracción de datos web y la agregación de datos. Al rotar entre varias direcciones IP de servidores proxy, los usuarios pueden evitar la detección y eludir los límites de velocidad impuestos por los sitios web. Esto resulta especialmente útil para recopilar grandes cantidades de datos sin que los sitios de destino los bloqueen o restrinjan.

Limitaciones y riesgos

Si bien los servidores proxy ofrecen numerosos beneficios, no están exentos de limitaciones y

riesgos. Un proxy mal configurado o poco confiable puede comprometer la privacidad y seguridad del usuario, lo que podría exponer información confidencial. Los usuarios deben tener cuidado al usar servidores proxy gratuitos o que no sean de confianza, ya que pueden registrar o usar indebidamente datos, inyectar anuncios o incluso realizar actividades maliciosas.

Además, los proxies no cifran el tráfico entre el usuario y el servidor proxy, lo que significa que los datos podrían ser interceptados o monitoreados por terceros. Para un mayor nivel de seguridad, los proxies deben usarse junto con otras tecnologías, como VPN o cifrado de extremo a extremo, para garantizar la confidencialidad e integridad de los datos.

En conclusión, los servidores proxy son herramientas versátiles que brindan diversos beneficios, desde mejorar la privacidad y la seguridad hasta mejorar el rendimiento y el control de la red. Sin embargo, es esencial comprender sus capacidades y limitaciones y utilizarlos de manera responsable para mitigar los posibles riesgos.

Ejercicios guiados

1. ¿Cuáles son los datos clave sobre los dos tipos de VPN de sitio a sitio?

2. ¿Qué hace que una conexión VPN sea privada?

 | Esta obra está bajo la licencia CC BY-NC-ND 4.0. |

Ejercicios exploratorios

1. Explique las diferencias entre los siguientes protocolos VPN: IPsec, OpenVPN y WireGuard. Incluya detalles sobre sus casos de uso típicos, fortalezas y debilidades.

2. Imagina que te encargan de configurar una VPN de acceso remoto para los empleados de una empresa. ¿Qué pasos seguirías para garantizar una configuración segura y eficaz? Incluye al menos tres medidas de seguridad que implementarías.

Resumen

Esta lección proporciona una descripción general de las redes privadas virtuales (VPN) y explica su función en la creación de conexiones seguras y cifradas en redes públicas. Comienza analizando los aspectos básicos de la tecnología VPN, incluidos los protocolos de tunelización y cifrado como IPsec, OpenVPN y WireGuard, y diferencia entre las VPN públicas que se utilizan para la privacidad personal y las VPN específicas de la organización diseñadas para el acceso remoto seguro y la conectividad de sitio a sitio. El texto también aborda las limitaciones y los riesgos asociados con las VPN, ofrece orientación sobre la selección de proveedores confiables y destaca la importancia de combinar las VPN con otros métodos de cifrado para garantizar una protección integral de los datos.

Además, la lección explora los conceptos de anonimato y reconocimiento en línea, y detalla cómo los identificadores como las direcciones IP pueden comprometer la privacidad del usuario. Se analizan diversas herramientas y técnicas, incluido el uso de servidores proxy, redes de anonimato y prácticas centradas en la privacidad, para ayudar a los usuarios a lograr un mayor anonimato.

 Esta obra está bajo la licencia CC BY-NC-ND 4.0.

Respuestas a los ejercicios guiados

1. ¿Cuáles son los datos clave sobre los dos tipos de VPN de sitio a sitio?

   Cuando existe una conexión privada entre dos redes LAN corporativas remotas, se dice que existe una VPN de sitio a sitio. Cuando las dos redes LAN remotas son sucursales de la misma organización, se trata de una VPN de sitio a sitio basada en intranet. Cuando las dos redes LAN remotas pertenecen a dos partes colaboradoras diferentes, se trata de una VPN de sitio a sitio basada en extranet.

2. ¿Qué hace que una conexión VPN sea privada?

   Primero se establece un canal privado entre dos partes remotas que desean comunicarse. Todos los datos enviados a través del canal privado se encapsulan y cifran. Esto da como resultado una conexión VPN privada. Cualquiera que intente husmear a través del canal privado no podrá obtener información útil.

Respuestas a los ejercicios exploratorios

1. Explique las diferencias entre los siguientes protocolos VPN: IPsec, OpenVPN y WireGuard. Incluya detalles sobre sus casos de uso típicos, fortalezas y debilidades.

   IPsec es un conjunto de protocolos diseñados para proteger las comunicaciones IP mediante la autenticación y el cifrado de cada paquete IP. Opera en la capa de red, lo que lo hace adecuado tanto para VPN de sitio a sitio como de acceso remoto. Sus puntos fuertes incluyen funciones de seguridad sólidas y compatibilidad con la mayoría de los dispositivos de red. Sin embargo, puede ser complejo de configurar y puede tener problemas de rendimiento debido a su gran sobrecarga de cifrado.

   OpenVPN es un protocolo VPN de código abierto que utiliza SSL/TLS para el cifrado, lo que lo hace altamente configurable y seguro. Admite protocolos de transporte TCP y UDP, lo que permite flexibilidad en diferentes entornos de red. OpenVPN se usa ampliamente para VPN de acceso remoto debido a sus sólidas funciones de seguridad y su capacidad para eludir los firewalls. Su principal debilidad es que requiere software de cliente y puede ser más lento que otros protocolos debido a su amplio cifrado.

   WireGuard es un protocolo VPN relativamente nuevo y liviano que apunta a ser más rápido y simple que IPsec y OpenVPN. Utiliza criptografía de última generación y está diseñado para tener una base de código mínima, lo que reduce el potencial de vulnerabilidades de seguridad. Los puntos fuertes de WireGuard incluyen un alto rendimiento y facilidad de configuración. Sin embargo, todavía está en proceso de integración en algunos sistemas y su compatibilidad con cambios dinámicos de direcciones IP puede ser limitada en comparación con protocolos más maduros.

2. Imagina que tienes la tarea de configurar una VPN de acceso remoto para los empleados de una empresa. ¿Qué pasos tomarías para garantizar una configuración segura y eficaz? Incluye al menos tres medidas de seguridad que implementarías.

   Selecciona un protocolo VPN seguro y confiable, como OpenVPN o IPsec, para la configuración de la VPN. Esto garantiza que todos los datos transmitidos entre los empleados y la red de la empresa estén cifrados y protegidos contra escuchas no autorizadas.

   Exige a los empleados que utilicen la autenticación multifactor (MFA) cuando se conecten a la VPN. Esto agrega una capa adicional de seguridad más allá de los nombres de usuario y las contraseñas, lo que dificulta el acceso de usuarios no autorizados.

   Configura la VPN para aplicar políticas de control de acceso basadas en los roles de usuario y la conformidad del dispositivo. Por ejemplo, permite el acceso a recursos confidenciales solo a los

 Esta obra está bajo la licencia CC BY-NC-ND 4.0.

usuarios que hayan pasado las verificaciones del dispositivo, como tener un software antivirus actualizado y los últimos parches de seguridad instalados. Esto ayuda a prevenir el acceso no autorizado y limita el impacto potencial de cuentas o dispositivos comprometidos.

Linux Professional Institute

Lección 2

Certificado:	Fundamentos de seguridad
Versión:	1.0
Tema:	024 Seguridad de redes y servicios
Objetivo:	024.3 Cifrado y anonimato en redes
Lección:	2 de 2

Introducción

En una era en la que la privacidad y el anonimato digitales están cada vez más amenazados, tecnologías como Tor, las criptomonedas y la darknet han surgido como herramientas cruciales para quienes buscan proteger sus actividades en línea. Tor, o The Onion Router, es una red diseñada para brindar anonimato al enrutar el tráfico de Internet a través de múltiples servidores, ocultando las identidades de los usuarios y dificultando el rastreo de sus actividades. Esta tecnología se ha vuelto crucial para los defensores de la privacidad, los periodistas y las personas que viven bajo regímenes represivos que necesitan acceder a la información libremente y comunicarse de forma segura.

El concepto de anonimato se extiende más allá de los simples hábitos de navegación a sistemas más complejos como la darknet, una parte oculta de Internet a la que solo se puede acceder mediante software especializado como Tor. La darknet alberga una variedad de contenidos, desde foros legítimos centrados en la privacidad y plataformas de denuncia de irregularidades hasta mercados ilícitos. Si bien los medios de comunicación suelen retratarla de forma negativa, también es un espacio fundamental para quienes requieren un alto nivel de confidencialidad y anonimato para sus actividades.

Las criptomonedas, en particular el bitcoin y otros activos basados en cadenas de bloques, han introducido una nueva dimensión en el debate sobre el anonimato. Aunque las transacciones en la mayoría de las cadenas de bloques son transparentes y rastreables, el uso de direcciones seudónimas proporciona una capa de anonimato que los sistemas financieros tradicionales no ofrecen. Sin embargo, este anonimato percibido puede ser engañoso, ya que las técnicas analíticas avanzadas son cada vez más capaces de desanonimizar las transacciones en cadenas de bloques. Comprender los matices de estas tecnologías y sus limitaciones es esencial para cualquier persona interesada en navegar por las complejidades del anonimato y la privacidad digitales.

Tor

Tor, abreviatura de *The Onion Router*, es una red descentralizada diseñada para mejorar la privacidad y el anonimato en línea. Permite a los usuarios navegar por Internet sin revelar su dirección IP ni información personal a terceros. Tor logra esto enrutando el tráfico de Internet a través de una serie de servidores operados por voluntarios, o nodos, cada uno de los cuales aplica su propia capa de cifrado.

Este proceso es similar a las capas de una cebolla, de ahí el nombre de “onion router”. A medida que el tráfico pasa por varios nodos, la fuente y el destino original de los datos se vuelven oscuros, lo que dificulta que cualquier persona, incluidas las agencias gubernamentales o los piratas informáticos, puedan rastrear la actividad hasta el usuario.

Tor fue desarrollado inicialmente a mediados de los años 90 por el Laboratorio de Investigación Naval de los Estados Unidos para proteger las comunicaciones de inteligencia de los Estados Unidos en línea. El objetivo era crear un sistema que permitiera a los usuarios navegar por Internet de forma anónima sin revelar su ubicación o identidad. En 2002, el código fuente de Tor se publicó bajo una licencia libre y se convirtió en una herramienta disponible públicamente para cualquiera que buscara mayor privacidad y seguridad en Internet.

El proyecto cobró mayor impulso en 2004, cuando la Electronic Frontier Foundation (EFF) comenzó a apoyar su desarrollo. Desde entonces, Tor se ha convertido en un recurso vital para periodistas, activistas y personas preocupadas por la privacidad en todo el mundo. Permite a los usuarios eludir la censura, proteger su identidad en línea y acceder a la información libremente, lo que lo convierte en una herramienta esencial en la lucha por la privacidad digital y la libertad de expresión.

Tor se utiliza para diversos fines, desde proteger la privacidad del usuario contra la vigilancia y el seguimiento hasta eludir la censura y acceder a información en regiones con acceso restringido a Internet. Sin embargo, debido a sus fuertes características de anonimato, Tor a veces se asocia con actividades ilegales. A pesar de esto, es ampliamente utilizado por periodistas, activistas y personas que buscan proteger su privacidad en entornos opresivos. Tor es accesible a través del

Tor Browser, una versión modificada de Mozilla Firefox, que facilita a los usuarios conectarse a la red Tor y navegar por Internet de forma segura (<<tor-screen> >).

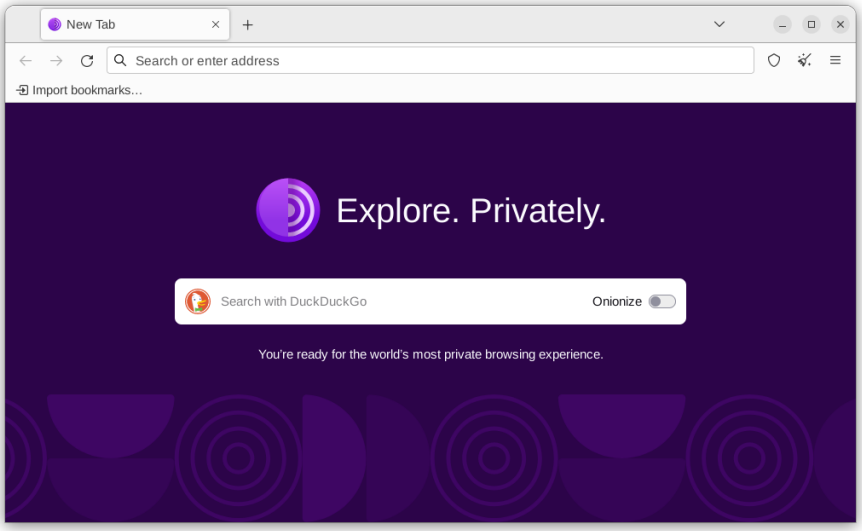

Figure 37. Tor Browser

Servicios ocultos y dominios .onion

Además de proporcionar anonimato para navegar por Internet, Tor admite *servicios ocultos*. Estos permiten que los sitios web y servidores operen de forma anónima dentro de la red Tor, lo que dificulta el rastreo tanto del usuario como del servidor. Estos servicios utilizan dominios ".onion", a los que no se puede acceder a través de navegadores web o motores de búsqueda habituales. En cambio, solo se puede acceder a ellos a través del Navegador Tor o de un software similar configurado para conectarse a la red Tor.

Un dominio .onion es un tipo especial de dirección web que termina en «.onion» y representa un servicio oculto dentro de la red Tor. Estos dominios se generan mediante algoritmos criptográficos, lo que garantiza que tanto el servidor como los usuarios permanezcan anónimos. Los servicios ocultos se utilizan para diversos fines legítimos, como plataformas de comunicación seguras, sitios de denuncia de irregularidades y foros anónimos, donde la privacidad y la confidencialidad son primordiales. Por ejemplo, las organizaciones de medios como The New York Times y las plataformas de denuncia de irregularidades como SecureDrop utilizan direcciones .onion para permitir la comunicación anónima con las fuentes.

Estos dominios .onion se generan mediante un proceso criptográfico que crea un par único de claves públicas y privadas. La clave pública se utiliza para formar la dirección .onion, mientras que la clave privada permanece protegida en el servidor, lo que garantiza que solo el servidor designado con la clave privada correcta pueda alojar ese servicio .onion específico.

Cuando un usuario intenta acceder a un sitio .onion, su solicitud se enruta a través de varios nodos Tor que actúan como servidores proxy, lo que oculta la identidad y la ubicación del usuario al servicio. Este enrutamiento de múltiples capas garantiza que la dirección IP del usuario permanezca oculta al sitio, lo que mantiene su privacidad. Además, la comunicación entre el usuario y el servicio .onion está cifrada de extremo a extremo, lo que significa que los datos se transmiten de forma segura desde el dispositivo del usuario al servidor de alojamiento sin riesgo de interceptación o manipulación por parte de terceros.

Para visitar un sitio .onion, los usuarios deben utilizar un navegador configurado para la red Tor, como el Tor Browser. Los navegadores web comunes no pueden resolver direcciones .onion, ya que estos dominios no forman parte del sistema DNS convencional. Este acceso especializado proporciona un método seguro y anónimo para alojar y visitar contenido, lo que convierte a los sitios .onion en una herramienta esencial para servicios centrados en la privacidad, la comunicación segura y el intercambio de información en entornos restrictivos.

Cómo navegar de forma segura por sitios .onion

La búsqueda en la red Onion es diferente a la navegación tradicional en Internet porque los sitios .onion no están indexados por los motores de búsqueda estándar como Google. En su lugar, se han diseñado motores de búsqueda específicos para ayudar a encontrar contenido alojado en sitios .onion dentro de la red Tor. Uno de los motores de búsqueda más populares para la red Onion es DuckDuckGo, que tiene una versión Onion que respeta la privacidad del usuario y no realiza un seguimiento de los usuarios. También admite la indexación de sitios .onion.

Otra opción es Ahmia, un motor de búsqueda que indexa sitios .onion y se centra en proporcionar acceso a contenido legítimo y seguro, al tiempo que filtra material potencialmente dañino. Es un recurso fiable para encontrar contenido en la red Tor. Además, Torch es uno de los motores de búsqueda más antiguos de la red Onion y cuenta con un gran índice de sitios .onion. A pesar de su sencilla interfaz, es eficaz para localizar una amplia gama de contenido en la red Tor.

Para utilizar estos buscadores, debes acceder a ellos a través del Navegador Tor, que permite navegar de forma anónima en la red Tor. Es importante tener precaución al utilizar cualquier buscador de la red Onion, ya que puedes encontrarte con contenido ilegal o malicioso. Mantente siempre alerta y asegúrate de acceder a recursos legítimos y de confianza.

Consideraciones prácticas y riesgos

Aunque Tor ofrece un alto nivel de anonimato, no es completamente infalible. Los usuarios deben ser conscientes de los posibles riesgos asociados con el uso de Tor, como los nodos de salida maliciosos, que pueden monitorear el tráfico no cifrado que sale de la red Tor. Además, las actividades que revelan información personal, como iniciar sesión en cuentas personales o

descargar archivos, pueden comprometer el anonimato incluso cuando se utiliza Tor. Para maximizar la privacidad, los usuarios deben combinar Tor con otras herramientas centradas en la privacidad, como la mensajería cifrada de extremo a extremo y las prácticas de navegación segura.

En general, Tor es una herramienta poderosa para quienes necesitan proteger su privacidad y acceder a la información libremente, pero debe usarse con una comprensión clara de sus capacidades y limitaciones.

La Darknet

La *darknet* se refiere a una parte de Internet que está oculta intencionalmente y requiere software, configuración o autorización específicos para acceder a ella. A diferencia de la web superficial, que está indexada por motores de búsqueda tradicionales como Google y es accesible a través de navegadores estándar, la darknet opera dentro de redes cifradas como Tor, I2P y Freenet. Estas redes brindan anonimato tanto a los usuarios como a los operadores de sitios web, lo que hace de la darknet un espacio donde se preserva la privacidad y la libertad de expresión, pero también donde pueden ocurrir actividades ilícitas.

La darknet suele asociarse con mercados ilegales y actividades delictivas debido a sus características de anonimato. Alberga plataformas en las que los usuarios pueden comprar y vender bienes y servicios ilegales, como drogas, documentos falsificados y datos robados, utilizando criptomonedas como Bitcoin y Monero. Sin embargo, la darknet no es únicamente un centro de actividades ilegales. También es un recurso vital para periodistas, activistas y denunciantes que operan en regímenes opresivos o en condiciones en las que la comunicación abierta podría tener graves consecuencias. Las plataformas de comunicación segura, los foros anónimos y los sitios de denuncia de irregularidades como SecureDrop son parte de la darknet y brindan espacios seguros para quienes necesitan confidencialidad.

Para acceder a la darknet, normalmente es necesario utilizar un software especializado, como el navegador Tor. Una vez conectados, los usuarios pueden navegar a sitios .onion u otros servicios ocultos a los que no se puede acceder a través de los navegadores web estándar. A pesar de la percepción de la darknet como un lugar peligroso, también es una herramienta para proteger la privacidad digital y permitir la libre expresión en entornos donde estos derechos están restringidos. Como ocurre con cualquier herramienta, el valor de la darknet y su potencial de daño dependen de cómo se utilice, y una navegación responsable es esencial para cualquiera que se aventure en esta parte oculta de Internet.

Criptomonedas: Entendiendo la cadena de bloques

Las *criptomonedas*, como Bitcoin y Monero, han ganado popularidad por ofrecer un grado de privacidad financiera y anonimato que normalmente no está disponible en los sistemas bancarios tradicionales.

Estas monedas digitales operan en redes descentralizadas que utilizan la tecnología blockchain, que sirve como estructura fundamental para registrar y verificar transacciones sin la necesidad de una autoridad central como un banco o un gobierno. La blockchain es esencialmente un libro de contabilidad distribuido que es compartido y mantenido por una red de nodos (computadoras) que participan en la red. Cada nodo contiene una copia de toda la blockchain, y las nuevas transacciones se validan a través de un mecanismo de consenso, como la prueba de trabajo (PoW) o la prueba de participación (PoS). Este proceso garantiza que todos los nodos estén de acuerdo sobre el estado de la blockchain, lo que la hace resistente al fraude y la manipulación.

Cuando un usuario inicia una transacción, esta se agrupa con otras transacciones en un *bloque*. Luego, este bloque se transmite a la red, donde los nodos trabajan para validarlo de acuerdo con las reglas del protocolo blockchain. Por ejemplo, en Bitcoin, este proceso implica resolver un rompecabezas matemático complejo, un proceso conocido como *minería*. Una vez que se valida el bloque, se agrega a la cadena de bloques previamente validados, lo que crea un registro permanente e inalterable de esa transacción. Esta cadena de bloques, o blockchain, forma un historial completo y cronológico de todas las transacciones que alguna vez ocurrieron en la red.

Si bien la transparencia de la cadena de bloques permite que cualquiera pueda ver el historial completo de transacciones, no necesariamente vincula estas transacciones a identidades del mundo real. En cambio, los usuarios están representados por direcciones alfanuméricas únicas, conocidas como *claves públicas*. Estas claves públicas se generan mediante algoritmos criptográficos y sirven como identificadores seudónimos. Por ejemplo, en lugar de mostrar “Carol Doe envió 1 Bitcoin a Dave Smith”, la cadena de bloques registrará que una dirección específica (por ejemplo, `1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa`) envió 1 Bitcoin a otra dirección. Esto crea una capa de *seudonimia*, ya que las direcciones no revelan directamente las identidades de las personas detrás de ellas.

Sin embargo, el grado de anonimato varía significativamente según el diseño de la cadena de bloques. En criptomonedas como Bitcoin, todas las transacciones son visibles públicamente, lo que significa que cualquiera puede rastrear el flujo de fondos de una dirección a otra. Si la identidad de un individuo está vinculada a una dirección particular a través de filtraciones de información, uso en un intercambio conocido o divulgación accidental, se hace posible rastrear todo su historial de transacciones. Es por eso que Bitcoin se considera seudónimo en lugar de anónimo.

Por el contrario, las criptomonedas centradas en la privacidad, como Monero y Zcash,

implementan funciones adicionales para ocultar los detalles de las transacciones. Monero, por ejemplo, utiliza firmas de anillo y transacciones confidenciales de anillo (RingCT) para mezclar la transacción del remitente con muchas otras, lo que hace que sea prácticamente imposible determinar el origen o el destino de los fondos. También utiliza direcciones ocultas, que generan una dirección única y de un solo uso para cada transacción. Esto significa que incluso si alguien conoce una dirección de Monero, no puede ver todas las transacciones entrantes a esa dirección en la cadena de bloques.

Por otro lado, Zcash ofrece a los usuarios la opción de elegir entre transacciones transparentes y protegidas. Las transacciones protegidas utilizan una sofisticada técnica criptográfica llamada zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge). Esto permite a la red verificar que una transacción es válida sin revelar ningún detalle sobre el remitente, el destinatario o el monto de la transacción. Esto ofrece un alto nivel de privacidad, pero requiere más recursos computacionales, lo que puede degradar la escalabilidad y la eficiencia.

Además, el anonimato percibido de las criptomonedas puede verse socavado por el uso de servicios centralizados como las casas de cambio, que a menudo exigen la verificación de identidad mediante procesos de *Conozca a su cliente* (KYC). Una vez que la identidad de un usuario está vinculada a una dirección a través de una casa de cambio, se puede rastrear y analizar su historial de transacciones. Esto ha llevado al desarrollo de herramientas avanzadas de análisis de cadenas de bloques que pueden identificar patrones, rastrear movimientos de fondos e incluso desanonimizar a los usuarios en determinadas condiciones.

Para combatir esto, los usuarios que priorizan la privacidad suelen emplear medidas adicionales, como el uso de monedas de privacidad, servicios de mezcla (tumblers) o billeteras que mejoran la privacidad y ocultan las rutas de las transacciones. Por ejemplo, los servicios de mezcla combinan múltiples transacciones de diferentes usuarios, lo que dificulta rastrear el origen de cada transacción individual. Sin embargo, estos servicios han sido objeto de escrutinio por parte de los reguladores, ya que pueden usarse para blanquear fondos ilícitos.

Si bien la tecnología blockchain ofrece una forma transparente y segura de registrar transacciones, el nivel de privacidad y anonimato que ofrece varía en gran medida según el diseño de la cadena de bloques y las medidas que tomen los usuarios para proteger sus identidades. Comprender estos matices es fundamental para cualquiera que desee interactuar con criptomonedas, ya sea por motivos de privacidad, seguridad o financieros.

Ejercicios guiados

1. Describa cómo Tor mejora el anonimato de los usuarios en Internet. Explique el proceso mediante el cual Tor oculta la identidad de un usuario y el contexto histórico de su desarrollo.

2. ¿Cuáles son las principales diferencias entre Bitcoin y Monero en términos de anonimato? Analice las técnicas que utiliza cada criptomoneda para proteger la privacidad del usuario.

3. ¿Qué papel desempeña la red oscura en el contexto del anonimato y cómo se puede acceder a ella? Explique sus aspectos positivos y negativos.

Ejercicios exploratorios

1. Investigar los distintos métodos utilizados por las fuerzas de seguridad para desanonimizar a los usuarios de Tor. Identificar al menos dos técnicas o tecnologías específicas empleadas en dichas investigaciones y proporcionar estudios de casos en los que estos métodos se hayan utilizado con éxito para descubrir la identidad de las personas que utilizan Tor. Analizar la eficacia de estos métodos y su impacto en el anonimato percibido que proporciona la red Tor.

 Esta obra está bajo la licencia CC BY-NC-ND 4.0. |

Resumen

Esta lección explora la interacción entre la privacidad digital, el anonimato y las tecnologías que respaldan estos conceptos, como Tor, la red oscura y las criptomonedas. Tor, o The Onion Router, es una red que brinda anonimato al enrutar el tráfico de Internet a través de múltiples servidores, lo que dificulta el rastreo de las actividades de los usuarios. La red oscura, una parte oculta de Internet a la que solo se puede acceder mediante software especializado como Tor, sirve como refugio tanto para actividades legítimas centradas en la privacidad como para mercados ilícitos, lo que refleja la naturaleza dual de estas tecnologías de anonimato.

Las criptomonedas, aunque suelen percibirse como anónimas, funcionan con tecnología blockchain, en la que las transacciones se registran en un libro de contabilidad público. Esta transparencia puede socavar el anonimato, especialmente en el caso de criptomonedas como Bitcoin, que son seudónimas en lugar de completamente anónimas. Los análisis avanzados a veces pueden vincular las transacciones con identidades del mundo real. Por el contrario, las criptomonedas centradas en la privacidad, como Monero y Zcash, ofrecen funciones de anonimato mejoradas para ocultar las identidades de los usuarios y los detalles de las transacciones. A pesar de estas capacidades, mantener el anonimato total con las criptomonedas sigue siendo un desafío debido al escrutinio regulatorio y al panorama cambiante del análisis de blockchain.

Respuestas a los ejercicios guiados

1. Describe cómo Tor mejora el anonimato del usuario en Internet. Explica el proceso por el cual Tor oculta la identidad de un usuario y el contexto histórico de su desarrollo.

   Tor mejora el anonimato del usuario al enrutar el tráfico de Internet a través de una red de servidores operados por voluntarios, cada uno aplicando una capa de cifrado, que es similar a las capas de una cebolla. A medida que el tráfico pasa a través de múltiples nodos, la fuente y el destino originales de los datos se oscurecen, lo que hace que sea extremadamente difícil para cualquiera rastrear las actividades del usuario hasta ellos. Tor fue desarrollado inicialmente a mediados de la década de 1990 por el Laboratorio de Investigación Naval de los Estados Unidos para proteger las comunicaciones de inteligencia de EE. UU. En 2002, su código fuente fue publicado bajo una licencia libre y se convirtió en una herramienta disponible públicamente para cualquiera que buscara mayor privacidad y seguridad en Internet. Desde entonces, se ha convertido en un recurso fundamental para periodistas, activistas y personas conscientes de la privacidad.

2. ¿Cuáles son las principales diferencias entre Bitcoin y Monero en términos de anonimato? Analice las técnicas que utiliza cada criptomoneda para proteger la privacidad del usuario.

   La principal diferencia entre Bitcoin y Monero en términos de anonimato es que Bitcoin es seudónimo, mientras que Monero está diseñado para proporcionar un verdadero anonimato. Bitcoin registra todas las transacciones en un libro de contabilidad público y, aunque los usuarios están representados por direcciones alfanuméricas, es posible con suficientes datos y análisis rastrear estas direcciones hasta los individuos. Monero, por otro lado, utiliza técnicas de privacidad avanzadas como firmas de anillo, direcciones ocultas y transacciones confidenciales para ocultar tanto la información del remitente como la del destinatario, así como el monto de la transacción. Esto hace que sea mucho más difícil rastrear las transacciones de Monero y vincularlas a individuos específicos, lo que proporciona un mayor nivel de privacidad que Bitcoin.

3. ¿Qué papel desempeña la red oscura en el contexto del anonimato y cómo se puede acceder a ella? Explique sus aspectos positivos y negativos.

   La red oscura es una parte de Internet que proporciona un mayor anonimato al requerir un software específico, como el navegador Tor, para acceder a su contenido. Permite a los usuarios navegar por servicios ocultos y sitios .onion que no están indexados por los motores de búsqueda convencionales y a los que no se puede acceder a través de navegadores estándar. La red oscura puede ser un recurso vital para periodistas, activistas y denunciantes que buscan comunicarse de forma segura y acceder a la información sin temor a la vigilancia o la censura. Sin embargo, también se asocia con actividades ilegales, ya que sus características de

anonimato se explotan para operar mercados ilícitos y distribuir contenido ilegal. Por lo tanto, si bien la red oscura es una herramienta esencial para proteger la privacidad digital y permitir la libre expresión en entornos restrictivos, también presenta importantes desafíos éticos y legales.

Respuestas a los ejercicios exploratorios

1. Investigar los distintos métodos utilizados por las fuerzas del orden para desanonimizar a los usuarios de Tor. Identificar al menos dos técnicas o tecnologías específicas empleadas en dichas investigaciones y proporcionar estudios de casos en los que estos métodos se hayan utilizado con éxito para descubrir la identidad de personas que utilizan Tor. Analizar la eficacia de estos métodos y su impacto en el anonimato percibido que proporciona la red Tor.

   Una técnica común utilizada por las fuerzas del orden para desanonimizar a los usuarios de Tor es el análisis de tráfico. Esto implica supervisar el tráfico que entra y sale de la red Tor e identificar patrones que puedan asociarse a usuarios específicos. En el caso del desmantelamiento de "Silk Road", las fuerzas del orden supervisaron los patrones de tráfico y los combinaron con otras técnicas de investigación para identificar a Ross Ulbricht, el operador del sitio, como "Dread Pirate Roberts". Este caso demostró que, si bien Tor proporciona un nivel significativo de anonimato, puede verse comprometido cuando se combina con otras fuentes de datos y técnicas de vigilancia.

   Otra técnica implica el uso de nodos de salida de Tor maliciosos. Estos son nodos operados por las fuerzas del orden u otras entidades que interceptan y registran el tráfico que pasa por ellos. Por ejemplo, en 2014, la operación “Onymous”, una operación conjunta del FBI y Europol, dio como resultado la incautación de varios mercados de la darknet. Se sospecha que la operación implicó el uso de nodos de salida maliciosos para capturar tráfico no cifrado e identificar a los administradores y usuarios de estos sitios. Este método puso de relieve una vulnerabilidad clave en la red Tor, donde los datos no cifrados que salen de la red Tor pueden ser interceptados y utilizados para identificar a los usuarios.

Linux Professional Institute

Tema 025: Identidad y privacidad

025.1 Identidad y autenticación

Referencia al objetivo del LPI

Security Essentials version 1.0, Exam 020, Objective 025.1

Peso

3

Áreas de conocimiento clave

- Comprensión de los conceptos de identidades digitales
- Comprensión de los conceptos de autenticación, autorización y contabilidad
- Comprensión de las características de una contraseña segura (por ejemplo, longitud, caracteres especiales, frecuencias de cambio, complejidad)
- Uso de un administrador de contraseñas
- Comprensión de los conceptos de preguntas de seguridad y herramientas de recuperación de cuentas
- Comprensión de los conceptos de autenticación multifactor (MFA), incluidos los factores comunes
- Comprensión de los conceptos de inicio de sesión único (SSO) e inicios de sesión en redes sociales
- Comprensión del rol de las cuentas de correo electrónico para la seguridad informática
- Comprensión de cómo se almacenan las contraseñas en los servicios en línea
- Comprensión de los ataques comunes contra las contraseñas
- Monitoreo de cuentas personales para detectar fugas de contraseñas (por ejemplo, alertas de motores de búsqueda para nombres de usuario y verificadores de fugas de contraseñas)
- Comprensión de los aspectos de seguridad de la banca en línea y las tarjetas de crédito

Lista parcial de archivos, términos y utilidades

- Gestores de contraseñas online y offline
- keepass2
- Inicio de sesión único (SSO)
- Autenticación de dos factores (2FA) y autenticación multifactor (MFA)
- Contraseñas de un solo uso (OTP), contraseñas de un solo uso basadas en el tiempo (TOTP)
- Aplicaciones de autenticación
- Hashing y salting de contraseñas
- Ataques de fuerza bruta, ataques de directorio, ataques de rainbow table

Linux Professional Institute

Lección 1

Certificado:	Fundamentos de seguridad
Versión:	1.0
Tema:	025 Identidad y privacidad
Objetivo:	025.1 Identidad y autenticación
Lección:	1 de 1

Introducción

La cuestión de la *identidad* se reduce a "¿quién eres?". Si vas a la fiesta de un amigo, éste podrá reconocerte por tu cara. Pero si vas a una conferencia, el personal podría querer comprobar tu documento de identidad (que probablemente tenga una foto de tu cara) antes de dejarte entrar. Así que, incluso en la vida cotidiana, la identidad no siempre es una cuestión sencilla.

La *autenticación* es una forma de determinar la identidad. En la conferencia, el personal te autentifica mediante un documento de identidad con tu fotografía. Cuando recoges la ropa de la tintorería, no necesitas demostrar tu identidad, pero es mejor que lleves el recibo que indica la lavandería. Esa es otra forma de autenticación.

Esta lección trata sobre la *identidad digital*, que es la forma en que los programas informáticos y los servicios en línea lo identifican a usted para otorgarle acceso. Analizaremos temas relacionados, como la administración de contraseñas, la autenticación multifactor y el inicio de sesión único. Le diremos cómo maximizar el uso seguro de estas tecnologías, de modo que a los atacantes les resulte difícil robar su identidad.

 Esta obra está bajo la licencia CC BY-NC-ND 4.0.

Conceptos de identidad y autenticación

A lo largo de los siglos se han desarrollado muchas formas de autenticación. En los bares clandestinos (los puntos de venta ilegal de alcohol que existían en Estados Unidos durante la época de la Prohibición), la gente se autenticaba diciendo una contraseña que conocía el personal (la famosa frase "Joe me envió") y así conseguía entrar. Las contraseñas (o, en términos más generales, las claves secretas) son ahora fundamentales para la autenticación informática.

Los expertos en seguridad dividen los tipos de autenticación en algunas categorías: "algo que sabes" (una contraseña), "algo que tienes" (un documento de identidad, una tarjeta de cajero automático) y "algo que eres" (una huella digital, un escaneo de retina).

La identidad y la autenticación son fundamentales para las interacciones informáticas. Necesitamos identificarnos y que nos autentifiquen las escuelas, las empresas, los bancos, los minoristas, las oficinas gubernamentales, las cuentas de redes sociales y más.

Un error en la autenticación puede tener consecuencias graves. Hay personas que han perdido los ahorros de toda su vida a causa de fraudes de identidad o estafas provocadas por atacantes que se identificaron falsamente como instituciones de confianza.

Pasos en la identificación: autenticación, autorización y contabilidad

Cuando utiliza un servicio, su identidad se utiliza de las siguientes maneras básicas.

La *autenticación*, como hemos visto, simplemente valida que Julie es Julie, y no George o Ahmed.

La *autorización* utiliza la identidad autenticada para determinar si usted tiene derecho a acceder a algún recurso. Por ejemplo, es posible que esté autorizado a leer y escribir archivos en su computadora, pero no a cambiar su configuración de seguridad.

La contabilidad (también conocida como registro) mantiene un registro de lo que ha hecho, de modo que un administrador pueda verificar si ha ocurrido algo sospechoso en el pasado. Por ejemplo, si parece que se han robado datos, al administrador le puede interesar saber que se registró que uno de los miembros del personal inició sesión en el sistema a las 3:00 a. m. Es posible que ese inicio de sesión haya sido realizado por un intruso malintencionado que robó las credenciales del miembro del personal.

Seguridad de la contraseña

Las contraseñas son fundamentales para la identidad y la seguridad en la informática. Aunque se

habla mucho de alternativas a las contraseñas, estas alternativas siguen basándose en el mismo concepto de “algo que sabes” y requieren la elección de una cadena de texto que sea difícil de adivinar.

Cuando se utilizan identificaciones físicas y datos biométricos, generalmente se utilizan junto con una contraseña u otro tipo de clave segura.

Cómo elegir una buena contraseña

Son pocos los usuarios de Internet que mantienen una buena seguridad de contraseñas. En esta sección, analizaremos las pautas de seguridad, y más adelante, analizaremos las herramientas que pueden resultar de ayuda.

Cuando usted se registra para una cuenta en línea, generalmente recibe algunas pautas para elegir una buena contraseña, como una longitud mínima (y a veces máxima) y una regla para variar el texto incluyendo letras mayúsculas, dígitos y puntuación (a veces una lista limitada de caracteres para elegir).

La complejidad es importante, pero la longitud lo es aún más. Esto se debe a que los atacantes suelen adivinar las contraseñas simplemente probando combinaciones aleatorias de caracteres, un método llamado *ataque de fuerza bruta*. Por lo tanto, si tiene una contraseña compleja pero corta como `H*z-6d`, un ataque de fuerza bruta podría intentar esa combinación de seis caracteres como parte de sus intentos aleatorios de iniciar sesión.

Si desea elegir una contraseña larga que pueda escribir fácilmente, comience por formar una cadena de palabras aleatorias que pueda recordar. Por ejemplo, podría comenzar con “scarf lunch wingnut rhino pretty” y luego mezclar caracteres especiales para formar la contraseña `scarf\lunch5wingnut(rhino,pretty`.

Si logras elegir una contraseña difícil, ¿puede ser adivinada por un intruso? Siempre existe una pequeña posibilidad. Alguien podría verte ingresando la contraseña y adivinar algunos de los caracteres. Un malware podría ingresar a tu computadora y monitorear tus pulsaciones de teclas. Un sitio en el que inicies sesión podría almacenar la contraseña de manera insegura y ser pirateado.

Por lo tanto, elija una contraseña diferente para cada sitio en el que inicie sesión. Los atacantes tienden a probar una combinación de nombre de usuario y contraseña en muchos servicios de Internet populares en un proceso llamado *relleno de credenciales*. Esto suele funcionar porque muchas personas usan la misma contraseña para varios sitios. Si usa contraseñas únicas, un atacante que obtenga la contraseña de su sitio de redes sociales podría interrumpir sus redes sociales, pero al menos no accederá a su cuenta bancaria.

Es una buena idea cambiar las contraseñas cada año aproximadamente. Algunos sitios requieren que cambies la contraseña con frecuencia. No intentes hacer trucos como alternar entre dos contraseñas: utiliza una nueva cada vez. Cambia la contraseña si te enteraste de que tu servicio fue víctima de una vulneración de seguridad.

Nunca compartas tu contraseña. No hay razón para que un empleador, un administrador de sistemas o cualquier otra persona que te llame y diga representar a tu banco conozca tu contraseña.

Las contraseñas nunca deben enviarse a través de canales no cifrados, como el correo electrónico o los mensajes de texto. Como hemos visto, las contraseñas nunca deben compartirse.

Preguntas de seguridad y herramientas de recuperación de cuenta

Además de la contraseña, los servicios suelen hacerte preguntas personales como "¿Dónde naciste?" y guardan las respuestas. A veces utilizan estas preguntas de seguridad para añadir comprobaciones adicionales cuando introduces tu nombre de usuario y contraseña. Si te bloquean el acceso y olvidas tu contraseña, busca un enlace como "¿Olvidaste tu contraseña?" en la pantalla de inicio de sesión de los servicios. Ese enlace te lleva a una página con las preguntas de seguridad que respondiste anteriormente.

Después de responder las preguntas con precisión, el servicio suele requerir otro paso para mayor seguridad: envía un enlace especial para un solo uso a su dirección de correo electrónico. Debe iniciar sesión utilizando ese enlace dentro de un período de tiempo especificado. Allí puede restablecer su contraseña. Este paso adicional garantiza que, incluso si un intruso malintencionado logra responder correctamente sus preguntas de seguridad, no podrá ingresar al servicio a menos que también tenga acceso a su correo electrónico.

El problema con las preguntas de seguridad es que alguien podría adivinar las respuestas. Probablemente no sea difícil para un atacante averiguar dónde naciste. Incluso un dato más oscuro, como "¿Cuál era el modelo de tu primer coche?", podría ser conocido por alguien.

Por lo tanto, es mejor inventar respuestas a las preguntas de seguridad y realizar un seguimiento de las respuestas falsas.

Gestores de contraseñas

Hemos descrito algunas reglas detalladas para la gestión de contraseñas. Afortunadamente, existen herramientas disponibles para ayudar con este proceso.

Mucha gente guarda una lista de contraseñas en papel y, en algunas circunstancias, es una forma razonable de mantenerlas. Si trabaja desde casa y nadie entra en su oficina, una lista en papel

puede ser segura (sin embargo, un ladrón podría encontrarla).

Y si tienes una lista en papel, tienes que escribir cada contraseña, lo que es complicado y propenso a errores. Muchos sitios te bloquean después de unos pocos intentos de inicio de sesión para frustrar ataques de fuerza bruta. Por eso, una lista en papel nunca es ideal.

Una lista de texto simple en su computadora es aún menos segura, porque el malware podría instalar una herramienta que encuentre la lista.

Por lo tanto, para una mayor seguridad, utilice un *administrador de contraseñas*. Este programa puede ejecutarse en su computadora personal (de escritorio, portátil o dispositivo móvil) o en la nube. Comience ingresando en el administrador de contraseñas toda la información de inicio de sesión relevante para cada servicio o programa que utilice: su dirección de correo electrónico o nombre de usuario, su contraseña y las respuestas a las preguntas de seguridad.

Un administrador de contraseñas encripta la información de inicio de sesión para que un intruso no pueda usarla si el archivo de datos es robado. Si un administrador de contraseñas se ejecuta en la nube, también utiliza encriptación al transmitir sus datos entre su computadora y el servidor en la nube.

Solo necesita recordar una contraseña, llamada *contraseña maestra,* para poder ingresar al administrador de contraseñas. Luego puede indicarle al administrador de contraseñas que inicie sesión en todos los programas y servicios que haya almacenado allí. Cambiar las contraseñas también es sencillo.

Existen ventajas y desventajas entre usar un *administrador de contraseñas sin conexión* en su computadora y usar uno _ basado en la nube_. No puede usar el administrador de contraseñas local cuando desea iniciar sesión en la computadora de un familiar o amigo en caso de que su sistema se caiga o esté visitando a alguien. El administrador de contraseñas en la nube está disponible en todas partes y es claramente útil cuando está de viaje.

Los administradores de contraseñas sin conexión almacenan los datos de las contraseñas localmente en el dispositivo del usuario, lo que proporciona un mayor nivel de seguridad porque los datos no se almacenan en la nube y no son vulnerables a los ataques en línea. Este tipo de administrador es ideal para los usuarios que priorizan la seguridad sobre la comodidad y no necesitan acceder a sus contraseñas en varios dispositivos. Los administradores sin conexión, como *KeePass2*, ofrecen funciones de seguridad sólidas, incluido el cifrado local y la capacidad de administrar contraseñas sin una conexión a Internet. El principal inconveniente es que los usuarios son responsables de realizar copias de seguridad de sus datos y puede resultarles menos conveniente sincronizar las contraseñas en los dispositivos manualmente.

Los administradores de contraseñas en línea almacenan datos de contraseñas encriptados en la

nube, lo que permite a los usuarios acceder a sus contraseñas desde cualquier dispositivo conectado a Internet. Esta función de sincronización es particularmente útil para los usuarios que necesitan acceder a sus contraseñas en varios dispositivos, como teléfonos inteligentes, tabletas y computadoras. Algunos ejemplos populares son LastPass, 1Password y Dashlane. Sin embargo, almacenar contraseñas en la nube presenta algunos riesgos de seguridad, ya que se podría acceder a los datos si el servicio se ve comprometido o el administrador de contraseñas en la nube puede dejar de funcionar o usted puede perder el acceso a Internet. La empresa también puede aumentar sus precios, cerrar o abandonarlo de otras maneras.

Algunos navegadores web también cuentan con administradores de contraseñas. Estos son prácticos siempre que realices todo tu trabajo en el mismo navegador, pero el administrador de contraseñas de un navegador no es accesible desde otro navegador.

KeePass 2 es un popular gestor de contraseñas gratuito que funciona en todos los sistemas operativos más conocidos. El sitio web ofrece descargas para una amplia gama de sistemas (Windows, macOS, GNU/Linux y dispositivos móviles populares) y distribuye su código fuente abierto bajo la Licencia Pública General de GNU.

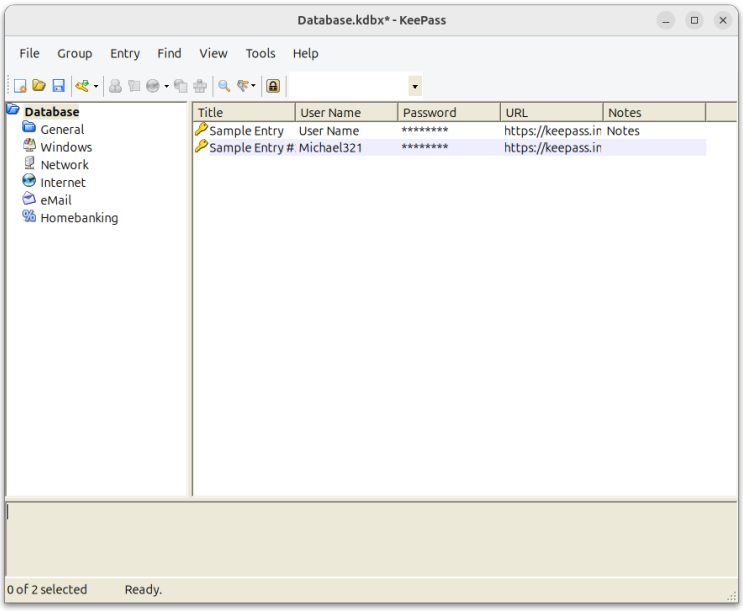

Figure 38. Pantalla principal de Keepass2

Inicio de sesión único

El *inicio de sesión único* (SSO) le permite iniciar sesión en un servicio y luego usar otros servicios sin tener que iniciar en ellos individualmente. Por ejemplo, supongamos que mantiene Facebook abierto en su computadora todo el tiempo. Cuando visita algún otro servicio, es posible que aparezca un cuadro de diálogo que le permita iniciar sesión con su cuenta de Facebook. Google es

otro servicio popular que se usa a menudo para el inicio de sesión único.

Se están produciendo intercambios de datos complicados entre bastidores para permitir el inicio de sesión único. La idea básica es que, después de hacer clic en el icono que presenta el segundo servicio, este envía un mensaje a Facebook y recibe un token (un mensaje aleatorio y cifrado) que lo autentica.

Cuando quieras usar el inicio de sesión único, es posible que el servicio que quieras usar no esté ejecutándose en el mismo navegador. Por ejemplo, es posible que hayas cerrado la sesión de Facebook o que lo hayas dejado ejecutándose en un navegador diferente. En ese caso, el segundo servicio hace que Facebook abra un cuadro de diálogo y te pida que inicies sesión en Facebook. En este caso, usar el inicio de sesión único la primera vez es tan complicado como iniciar sesión con una cuenta diferente, pero los usos posteriores del inicio de sesión único serán fáciles porque Facebook sigue ejecutándose.

Al igual que con un administrador de contraseñas en línea, depender de un servicio para el inicio de sesión único tiene un riesgo: si pierde el acceso a su cuenta o el servicio cierra, perderá el acceso a todos los demás servicios que consultaron su información de inicio de sesión.

Además, cuando un nuevo servicio solicita acceso a otro, es posible que el nuevo servicio le pida muchos datos sobre usted que no son necesarios para iniciar sesión: ubicación y fecha de nacimiento, por ejemplo. Si le piden que apruebe la transferencia de datos de un servicio a otro, piense detenidamente si desea que el nuevo servicio tenga esos datos.

Autenticación multifactor

Cada vez más, a los usuarios de Internet se les solicita que ingresen una cadena de dígitos que se les envía a sus teléfonos o que realicen alguna otra tarea antes de iniciar sesión en un servicio. Los servicios requieren dos o más formas de identificarlo, conocidas como *autenticación multifactor* (MFA), para abordar los riesgos de las contraseñas. El escenario descrito anteriormente, en el que restablece su contraseña mediante un enlace enviado a su dirección de correo electrónico, es otra forma de MFA. Estos procedimientos evitan que alguien del otro lado del mundo, o incluso de la oficina de al lado, se haga pasar por usted.

Todas las formas de autenticación multifactor requieren un esfuerzo adicional por parte del usuario (ya que se trata de dos o más formas de identificarse), pero valen la pena porque eliminan muchos ataques comunes. Casi todos los usuarios de computadoras tienen un teléfono celular en la actualidad, por lo que es razonable usarlo para la autenticación multifactor. Muchos servicios pueden enviar el código a su correo electrónico, por lo que también puede usarlo desde su computadora de escritorio o portátil.

La mayoría de los MFA requieren una contraseña y otro factor, y por lo tanto pueden

denominarse *autenticación de dos factores* (2FA).

Desde hace algún tiempo se utilizan muchas otras formas de autenticación multifactor. Una tarjeta de cajero automático, combinada con un PIN de cuatro dígitos, es una forma sencilla y eficaz de que su banco le identifique dondequiera que vaya en el mundo. Muchos cajeros automáticos también contienen cámaras para que, en caso de un retiro fraudulento, un administrador pueda ver quién lo hizo.

Hay dispositivos especiales que se conectan a las computadoras del trabajo y permiten autenticarse sosteniendo una credencial con una tira como la que se encuentra en los cajeros automáticos.

Las *contraseñas de un solo uso* se desarrollaron mucho antes de la informática digital. Las personas que querían verificar su identidad por teléfono o por radio llevaban consigo un "bloc de un solo uso", en el que cada hoja contenía un código aleatorio. Una persona decía el código, la otra lo validaba y, a continuación, cada una de ellas arrancaba la hoja.

En informática, puedes ejecutar un programa o dispositivo que genere una contraseña de un solo uso y usarlo para autenticarte.

Un tipo de autenticación relacionado es la contraseña de un solo uso basada en el tiempo (TOTP, por sus siglas en inglés). Este servicio genera un código aleatorio cada 30 segundos aproximadamente. Cuando desee iniciar sesión en su lugar de trabajo u otro servicio, puede presionar un botón en el servicio para generar un código e ingresarlo cuando el servicio en el que está iniciando sesión lo solicite. El servidor genera simultáneamente el mismo código a partir del servicio. Cuando los códigos coinciden, puede iniciar sesión.

Muchos dispositivos móviles permiten iniciar sesión con la huella dactilar. Los lectores de huellas dactilares de estos dispositivos son solo parcialmente precisos y las huellas dactilares tampoco son completamente únicas. Por lo tanto, es mejor utilizar la huella dactilar con una contraseña u otra forma de autenticación.

Aunque la autenticación multifactor puede resultar tediosa, se recomienda que la utilices para todos los programas y servicios a los que accedas. Después de todo, probablemente inicies sesión en los servicios solo unas pocas veces al día. Si instalas una *aplicación de autenticación*, puedes configurar el uso de la autenticación multifactor para tus servicios y detener muchos tipos de ataques.

Protección de contraseñas en servicios en línea

Hemos hablado de cómo deberías gestionar tus contraseñas de forma segura, pero ¿qué ocurre con el servidor? Tiene que reconocer tu contraseña, pero si contiene una base de datos de

usuarios y contraseñas, es muy vulnerable a intrusiones maliciosas.

Las dos formas principales de proteger su contraseña son el *hashing* y el *salting*. Estas técnicas se conocen desde hace muchas décadas y todos los servidores deberían utilizarlas.

El hash consiste en ejecutar los caracteres de la contraseña mediante una función matemática sencilla, que suele consistir en sumas, multiplicaciones y divisiones. Un buen hash produce una cadena de caracteres aleatorios de longitud fija. Como durante el hash se pierde información, nadie puede reconstruir la contraseña original a partir del hash.

Cuando inicia sesión y envía la contraseña, el servidor la codifica y se asegura de que el resultado coincida con lo que hay en su base de datos.

Los atacantes decididos y bien financiados han encontrado una forma de atacar los hashes: crean una enorme base de datos de cadenas y sus hashes asociados (lo que supone que pueden determinar qué función hash se está utilizando). Esta base de datos se llama *rainbow table*. Si el atacante entra en un servidor y obtiene los hashes, busca cada hash en el "rainbow table" y prueba las distintas cadenas que coinciden.

Por lo tanto, el hash debe complementarse con el salting. Esto significa agregar una cadena corta y única (denominada *salt* o *nonce*) a la contraseña del usuario. Luego, se realiza el hash de la combinación de contraseña y salt.

Cuentas de correo electrónico y seguridad informática

Las cuentas de correo electrónico suelen ser la puerta de entrada a nuestras identidades digitales y funcionan como un centro central para gestionar el acceso a diversos servicios en línea, como las redes sociales, el comercio electrónico, la banca e incluso las plataformas relacionadas con el trabajo. Por este motivo, proteger las cuentas de correo electrónico es uno de los aspectos más críticos de la seguridad informática. Una cuenta de correo electrónico comprometida puede dar lugar a una serie de infracciones de seguridad, ya que los atacantes pueden utilizarla para restablecer contraseñas y obtener acceso no autorizado a otros servicios conectados.

Para proteger las cuentas de correo electrónico, es fundamental implementar medidas de seguridad sólidas. Una de las estrategias más efectivas es utilizar la autenticación multifactor.

También es importante supervisar periódicamente la actividad de su cuenta de correo electrónico. Esté atento a cualquier intento de inicio de sesión inusual o cambios en la configuración, como reglas de reenvío que usted no haya configurado. Estos podrían ser indicadores de que alguien está intentando obtener acceso no autorizado a su cuenta.

Monitoreo de cuentas personales

Monitorear las cuentas personales para detectar filtraciones de contraseñas es una práctica esencial para mantener la seguridad digital y proteger su identidad en línea. Las filtraciones de contraseñas ocurren cuando los piratas informáticos obtienen acceso no autorizado a bases de datos que contienen credenciales de usuario, que luego pueden exponerse o venderse en la red oscura.

Para mitigar los riesgos asociados con las filtraciones de contraseñas, es fundamental ser proactivo y supervisar sus cuentas para detectar indicios de vulnerabilidad. Un método eficaz es configurar alertas de motores de búsqueda para sus nombres de usuario o direcciones de correo electrónico.

Además, los comprobadores de fugas de contraseñas son una herramienta invaluable para identificar credenciales comprometidas. Los sitios web y servicios como *Have I Been Pwned* y *Google's Password Checkup* pueden escanear su dirección de correo electrónico o contraseña comparándola con bases de datos de infracciones conocidas para determinar si su información ha sido filtrada.

Si recibe una alerta de que su contraseña ha sido comprometida, es importante actuar rápidamente. Cambie su contraseña inmediatamente en el sitio afectado y en cualquier otro sitio en el que haya usado la misma contraseña.

Los navegadores web modernos, como Google Chrome, Firefox y Safari, tienen funciones de seguridad integradas que alertan a los usuarios si sus contraseñas se han visto comprometidas en una filtración de datos. Estos navegadores pueden detectar cuándo las contraseñas guardadas ya no son seguras y notificar a los usuarios sobre qué cuentas se vieron afectadas, lo que les solicita que tomen medidas para proteger su información.

Cuando utiliza el administrador de contraseñas integrado de un navegador, este almacena de forma segura sus credenciales de inicio de sesión para varios sitios web. Si alguna de estas contraseñas almacenadas coincide con una filtración de datos conocida, el navegador emitirá una alerta de seguridad.

Aspectos de seguridad de la banca en línea y las tarjetas de crédito

La banca en línea y el uso de tarjetas de crédito ofrecen comodidad y accesibilidad a los usuarios para gestionar sus finanzas desde cualquier lugar. Sin embargo, esta comodidad conlleva importantes riesgos de seguridad, ya que estos servicios son objetivos principales para los cibercriminales que buscan robar información personal y activos financieros.

Una de las bases de la seguridad de la banca online es el uso de conexiones seguras, que suelen indicarse mediante una URL que comienza con `https://` y un icono de candado en la barra de direcciones del navegador. Asegúrese siempre de estar en el sitio web legítimo del banco antes de introducir cualquier información personal. Los ataques de phishing, en los que sitios web fraudulentos imitan a los legítimos, son una amenaza habitual. Otro aspecto de seguridad fundamental es la autenticación multifactor (MFA), que la mayoría de los bancos exigen actualmente u ofrecen como opción.

Evite utilizar computadoras públicas o compartidas, ya que pueden estar infectadas con malware que puede capturar sus pulsaciones de teclas o robar sus credenciales de inicio de sesión. De manera similar, las redes Wi-Fi públicas suelen ser inseguras y pueden ser utilizadas por atacantes para interceptar sus datos. Si debe utilizar una red Wi-Fi pública, considere utilizar una red privada virtual (VPN) para cifrar su conexión y proteger su información.

 Esta obra está bajo la licencia CC BY-NC-ND 4.0. |

Ejercicios guiados

1. ¿Por qué es importante que una contraseña sea larga?

2. ¿Qué debe hacer si alguien lo llama de Microsoft y le pide su contraseña para poder solucionar un problema de seguridad en su sistema Windows?

3. ¿Cuáles son algunas ventajas de utilizar un administrador de contraseñas?

Ejercicios exploratorios

1. En los hospitales, los médicos suelen desplazarse de un piso a otro y deben iniciar sesión con frecuencia para controlar a los pacientes y registrar sus notas. ¿Qué forma de autenticación podría ser útil para un hospital?

2. Algunos profesionales delegan las publicaciones en las redes sociales a un servicio que las publica en horarios planificados. ¿Tiene que darle su contraseña a ese servicio y permitirle tener acceso completo a su cuenta?

Resumen

En esta lección se tratan las formas de demostrar su identidad para poder acceder de forma segura a los recursos de Internet. Se analiza cómo proteger las contraseñas que debe utilizar tanto usted, el usuario, como el servidor en el que inicia sesión. Se presentan distintos tipos de autenticación multifactor, junto con los administradores de contraseñas y el inicio de sesión único.

Respuestas a los ejercicios guiados

1. ¿Por qué es importante que una contraseña sea larga?

   Las contraseñas largas (20 caracteres, o idealmente incluso más largas) son las más resistentes a los ataques de fuerza bruta.

2. ¿Qué debe hacer si alguien lo llama de Microsoft y le pide su contraseña para poder solucionar un problema de seguridad en su sistema Windows?

   Cuelgue. Los estafadores que dicen ser de Microsoft son comunes, pero cualquiera que le pida su contraseña es un estafador y puede ser útil llamar a la empresa a la que dicen representar y advertirle que alguien está estafando a sus clientes.

3. ¿Cuáles son algunas de las ventajas de utilizar un gestor de contraseñas?

   Tus contraseñas se almacenan de forma segura y cifrada, de modo que no tienes que escribirlas en texto normal. Solo tienes que recordar tu contraseña maestra. Puedes crear contraseñas largas y complejas sin tener que intentar escribirlas.

 | Esta obra está bajo la licencia CC BY-NC-ND 4.0. |

Respuestas a los ejercicios exploratorios

1. En los hospitales, los médicos suelen desplazarse de un piso a otro y deben iniciar sesión con frecuencia para controlar a los pacientes e ingresar sus notas. ¿Qué forma de autenticación podría ser buena para un hospital?

   Los lectores de credenciales son una buena solución en un entorno de este tipo. Cada médico lleva una credencial con una banda que contiene su información de identificación. Cada puesto de enfermería tiene una computadora con un lector de credenciales. Para acceder a los registros electrónicos, cada médico o enfermero sostiene su credencial frente al lector de credenciales y posiblemente también ingrese una contraseña para la autenticación de dos factores. Si se van sin cerrar sesión, la cuenta se cierra automáticamente después de un tiempo de inactividad.

2. Algunos profesionales delegan las publicaciones en las redes sociales a un servicio que las publica en horarios planificados. ¿Tiene que darle su contraseña a ese servicio y permitirle tener acceso completo a su cuenta?

   No. Estos servicios tienen un acceso muy limitado a su cuenta. El servicio utiliza la interfaz de programación de aplicaciones (API) de la red social para realizar sus publicaciones. El servicio tiene su propia contraseña de API, por lo que puede revocar el acceso cuando lo desee. Las operaciones permitidas al servicio también pueden ser limitadas.

025.2 Confidencialidad de la información y comunicación segura

Referencia al objetivo del LPI

Security Essentials version 1.0, Exam 020, Objective 025.2

Peso

2

Áreas de conocimiento clave

- Comprender las implicaciones y los riesgos de las fugas de datos y las comunicaciones interceptadas
- Comprensión del phishing, la ingeniería social y las estafas
- Comprender los conceptos de los filtros de spam de correo electrónico
- Manejo seguro de archivos adjuntos de correo electrónico recibidos
- Compartir información de forma segura y responsable mediante recursos compartidos en la nube de correo electrónico y servicios de mensajería
- Uso de mensajería instantánea cifrada

Lista parcial de archivos, términos y utilidades

- Phishing e ingeniería social
- Robo de identidad
- Estafas y scareware
- Correo no deseado, filtrado de correo no deseado
- Acuerdos de confidencialidad (NDA)
- Clasificación de la información

Linux Professional Institute

Lección 1

Certificado:	Fundamentos de seguridad
Versión:	1.0
Tema:	025 Identidad y privacidad
Objetivo:	025.2 Confidencialidad de la información y comunicación segura
Lección:	1 de 1

Introducción

En el mundo interconectado de hoy, donde los datos confidenciales se comparten frecuentemente en línea, es importante saber cómo mantener la confidencialidad de la comunicación digital. Esto incluye proteger la información personal y profesional y reconocer amenazas como el phishing y la ingeniería social, que explotan la psicología humana para obtener acceso a datos confidenciales. Identificar estos intentos es clave para prevenir el acceso no autorizado. Las filtraciones de datos y las comunicaciones interceptadas pueden provocar pérdidas financieras, daños a la reputación y problemas legales. Esta lección cubre el impacto de las filtraciones de datos, la importancia de los acuerdos de confidencialidad (NDA) y el papel de la clasificación de la información en la protección de los datos confidenciales.

Fugas de datos y comunicaciones interceptadas

Una fuga de datos ocurre cuando se expone información confidencial, ya sea accidentalmente o con malas intenciones. Esto puede suceder debido a medidas de seguridad inadecuadas, errores humanos o ataques deliberados por parte de cibercriminales. Las consecuencias de una fuga de datos pueden ser devastadoras. Para las empresas, la filtración de información confidencial puede

resultar en la pérdida de ventaja competitiva, robo de propiedad intelectual y sanciones económicas. Para las personas, la exposición de datos personales, como números de seguro social o información de tarjetas de crédito, puede dar lugar al robo de identidad y al fraude.

Además, las empresas pueden enfrentarse a consecuencias legales si no cumplen con las normas de protección de datos, como el Reglamento General de Protección de Datos (RGPD) en Europa o la Ley de Privacidad del Consumidor de California (CCPA) en Estados Unidos. Las multas y sanciones por incumplimiento pueden ser sustanciales, lo que agrava aún más el impacto de una filtración de datos.

Las comunicaciones interceptadas plantean una amenaza similar. Si se transmite información confidencial a través de canales no seguros, puede ser interceptada por terceros no autorizados. Esto es particularmente peligroso en entornos empresariales, donde las conversaciones confidenciales sobre estrategias, planes financieros o desarrollo de productos podrían ser explotadas por competidores o actores maliciosos.

Phishing e ingeniería social

El *phishing* y la *ingeniería social* son tácticas engañosas que utilizan los cibercriminales para manipular a las personas para que divulguen información confidencial o realicen acciones que comprometan la seguridad. Estos ataques suelen explotar la psicología humana en lugar de las vulnerabilidades técnicas, lo que dificulta su detección y defensa. El phishing suele implicar correos electrónicos, mensajes de texto o sitios web fraudulentos diseñados para parecer legítimos, engañando a las víctimas para que revelen información confidencial, como nombres de usuario, contraseñas o datos de tarjetas de crédito. Por ejemplo, un mensaje de correo electrónico puede parecer que proviene de una fuente confiable, como un banco o un servicio en línea, y pedirle al destinatario que haga clic en un enlace para actualizar la información de su cuenta. Una vez que la víctima ingresa sus credenciales en el sitio falso, el atacante captura estos datos y los usa con fines maliciosos.

La ingeniería social, por otra parte, abarca una gama más amplia de tácticas que van más allá del phishing. Implica manipular a individuos para que infrinjan los procedimientos de seguridad normales, a menudo haciéndose pasar por alguien de confianza o en una posición de autoridad. Un ejemplo común es una llamada telefónica de un atacante que se hace pasar por un miembro del departamento de TI y solicita a la víctima que proporcione credenciales de inicio de sesión para “resolver un problema técnico”.

Robo de identidad

El *robo de identidad* ocurre cuando un atacante obtiene acceso no autorizado a la información personal de alguien y la utiliza para hacerse pasar por la víctima, a menudo para cometer fraude

u otros delitos. Esto puede incluir el robo de datos personales como números de Seguro Social, información de tarjetas de crédito o credenciales de cuentas en línea. Una vez que tienen esta información, los atacantes pueden abrir nuevas cuentas de crédito, realizar compras no autorizadas o incluso obtener acceso a servicios médicos y gubernamentales en nombre de la víctima.

El phishing y la ingeniería social son a menudo los pasos iniciales del robo de identidad, ya que estas técnicas se utilizan para recopilar la información personal necesaria para hacerse pasar por la víctima.

Para prevenir el robo de identidad es necesario combinar la vigilancia con medidas de seguridad proactivas. Las personas deben utilizar contraseñas seguras y únicas para cada una de sus cuentas y habilitar la autenticación multifactor siempre que sea posible. El control regular de los extractos bancarios, los informes de crédito y la actividad de las cuentas también puede ayudar a detectar transacciones o cambios no autorizados en una etapa temprana.

Estafas y scareware

Las estafas y el scareware son tácticas maliciosas que utilizan los cibercriminales para engañar a las personas y aprovecharse de sus miedos, lo que suele derivar en pérdidas económicas o en la vulneración de información personal. Este tipo de ataques se basan en la manipulación y el miedo, más que en métodos técnicos de piratería informática, lo que hace que sea difícil identificarlos y evitarlos.

El término “estafa” hace referencia a una amplia gama de esquemas fraudulentos diseñados para engañar a las personas para que revelen dinero, información personal o acceso a cuentas confidenciales. Los estafadores suelen hacerse pasar por organizaciones legítimas, como bancos, agencias gubernamentales o empresas conocidas, para ganarse la confianza de la víctima. Un ejemplo común es la "estafa de soporte técnico", en la que el estafador se comunica con la víctima y afirma que su computadora ha sido infectada con un virus. Luego, el estafador ofrece solucionar el problema a cambio de una tarifa o le pide a la víctima que descargue un software que le otorga acceso remoto a su dispositivo. Una vez que tiene acceso, puede robar información confidencial o exigir el pago de servicios que nunca fueron necesarios.

Por otro lado, el *scareware* es un tipo específico de malware que se aprovecha del miedo para manipular a las víctimas para que realicen determinadas acciones. Por lo general, se manifiesta como mensajes emergentes, alertas en la computadora o en un teléfono inteligente, advirtiendo falsamente que el dispositivo ha sido infectado con un virus o que sus datos están en riesgo. El mensaje de scareware puede parecer provenir de una empresa de antivirus o un servicio de seguridad legítimos e insta al usuario a descargar software o comprar una “versión completa” de un producto para solucionar el problema inexistente. En realidad, la descarga del software

sugerido puede llevar a la instalación de malware, spyware o ransomware reales, lo que compromete aún más el dispositivo y la información personal del usuario.

Para protegerse contra este tipo de ataques, es importante permanecer escéptico ante ofertas no solicitadas, advertencias y solicitudes de pago o información personal.

Acuerdos de confidencialidad (NDA)

Los *acuerdos de confidencialidad* (NDA, por sus siglas en inglés) son contratos legales que protegen la información confidencial compartida entre las partes. Se utilizan comúnmente en entornos comerciales para evitar la divulgación no autorizada de datos confidenciales, como secretos comerciales, planes comerciales o tecnología patentada. Un NDA generalmente describe el alcance de la información confidencial, las obligaciones de las partes involucradas y las consecuencias de incumplir el acuerdo.

Los acuerdos de confidencialidad desempeñan un papel fundamental a la hora de mantener la confidencialidad de la información cuando se colabora con terceros, como contratistas, consultores o posibles socios comerciales. Al firmar un acuerdo de confidencialidad, estas partes se comprometen a no divulgar ni hacer un uso indebido de la información que se les proporciona durante el curso de la relación comercial. Esta protección legal ayuda a garantizar que los datos confidenciales permanezcan seguros y no se utilicen en detrimento de la empresa.

Sin embargo, es importante reconocer que los acuerdos de confidencialidad no son infalibles. Si bien brindan un marco legal para proteger la información, no evitan todas las posibles filtraciones o usos indebidos. Garantizar el cumplimiento de un acuerdo de confidencialidad requiere vigilancia y monitoreo regular, así como una sólida cultura interna de confidencialidad y seguridad de los datos.

Clasificación de la información

El uso de acuerdos de confidencialidad está intrínsecamente vinculado a la *clasificación de la información*. Un proceso de clasificación exhaustivo ayuda a determinar qué información es lo suficientemente crítica como para garantizar su protección mediante un acuerdo de confidencialidad. Por ejemplo, la información altamente confidencial, como las estrategias comerciales exclusivas o los secretos comerciales, siempre debe regirse por acuerdos de confidencialidad estrictos para evitar su uso indebido o su exposición accidental.

La clasificación de la información es un proceso sistemático de categorización de datos en función de su nivel de sensibilidad y el impacto potencial de su divulgación no autorizada. Este proceso ayuda a las organizaciones a identificar y proteger sus activos de información más críticos mediante la aplicación de controles de seguridad adecuados. Los niveles de clasificación más

comunes incluyen *público*, *interno*, *confidencial* y *altamente confidencial*.

La información pública es aquella que se puede compartir libremente sin ningún riesgo para la organización, como los materiales de marketing o los comunicados de prensa. La información interna está destinada a ser utilizada dentro de la organización, pero no supone un riesgo significativo si se divulga. Sin embargo, la información confidencial podría causar daños si se expone; dicha información incluye los registros de los empleados, los estados financieros y los datos de los clientes. La información altamente confidencial es la más sensible y su divulgación podría tener graves consecuencias, como secretos comerciales o estrategias comerciales críticas.

Clasificar la información correctamente es esencial para implementar medidas de seguridad eficaces. Por ejemplo, la información altamente confidencial debe almacenarse en entornos seguros y con acceso controlado y transmitirse únicamente a través de canales cifrados. Los empleados deben recibir capacitación sobre cómo manejar y proteger los datos en función de su nivel de clasificación, asegurándose de que la información sensible no quede expuesta inadvertidamente.

Además de proteger los datos dentro de la organización, la clasificación de la información es vital para cumplir con los requisitos legales y reglamentarios. Muchas regulaciones exigen protecciones específicas para ciertos tipos de datos, como información personal o registros financieros. Una clasificación adecuada ayuda a las organizaciones a cumplir con estos requisitos y evitar posibles sanciones por incumplimiento.

Protección de la comunicación por correo electrónico

El *spam* por correo electrónico se refiere a mensajes no solicitados, a menudo irrelevantes o inapropiados, que se envían a un gran número de destinatarios. Estos mensajes suelen contener anuncios, intentos de phishing o contenido malicioso, como enlaces a programas maliciosos. El spam no solo satura las bandejas de entrada, sino que también plantea importantes riesgos de seguridad, ya que se utiliza con frecuencia como vector de ciberataques.

El *filtrado de spam* detecta y bloquea el correo electrónico no deseado o potencialmente dañino antes de que llegue a la bandeja de entrada del destinatario. Los filtros de spam utilizan una variedad de técnicas para identificar el spam, incluido el análisis del contenido del correo electrónico, la verificación de la reputación del remitente y el uso de algoritmos de aprendizaje automático para detectar patrones comúnmente asociados con el spam. Estos filtros pueden operar en varios niveles, incluido el servidor de correo electrónico, el software del cliente y los servicios de terceros.

El filtrado de *listas negras* y *listas blancas* es otro método mediante el cual los correos electrónicos provenientes de fuentes o dominios de spam conocidos se bloquean en función de su reputación,

mientras que los remitentes confiables eluden los filtros.

Los filtros de spam son fundamentales para proteger a los usuarios de intentos de phishing, malware y otras amenazas basadas en correo electrónico. Al impedir que los mensajes potencialmente peligrosos lleguen a la bandeja de entrada, reducen el riesgo de que los usuarios hagan clic en enlaces maliciosos, descarguen archivos adjuntos infectados o sean víctimas de ataques de ingeniería social.

Sin embargo, los filtros de spam no son perfectos. A veces, los correos electrónicos legítimos pueden clasificarse incorrectamente como spam, un problema conocido como *falsos positivos*. Por el contrario, algunos mensajes de spam pueden evadir la detección y llegar a la bandeja de entrada, conocidos como *falsos negativos*. Para minimizar estos problemas, los usuarios pueden revisar periódicamente su carpeta de spam en busca de mensajes legítimos y ajustar la configuración de su filtro de spam en consecuencia.

Los *archivos adjuntos* de correo electrónico son una forma habitual de compartir documentos, imágenes y otros archivos, pero también suponen importantes riesgos de seguridad si no se gestionan adecuadamente. Los archivos adjuntos maliciosos son un método habitual que utilizan los ciberdelincuentes para distribuir malware, ransomware y otro software dañino.

Una de las reglas más importantes a la hora de manejar archivos adjuntos en correos electrónicos es tener cuidado, especialmente si el correo electrónico es inesperado o proviene de un remitente desconocido. Incluso si el correo electrónico parece provenir de una fuente conocida, es esencial verificar la legitimidad del mensaje antes de abrir cualquier archivo adjunto.

Evite siempre abrir archivos adjuntos con tipos de archivos sospechosos. Los formatos de archivo más comunes que se utilizan en archivos adjuntos maliciosos incluyen `.exe` (archivos ejecutables), `.vbs` (archivos de Visual Basic Script), `.js` (archivos de JavaScript) y `.bat` (archivos por lotes). Estos tipos de archivos pueden ejecutar código potencialmente peligroso en su sistema.

Otra práctica fundamental es mantener actualizado el antivirus y las herramientas de seguridad del correo electrónico. Los programas antivirus modernos están equipados para analizar los archivos adjuntos del correo electrónico en busca de amenazas conocidas y avisarle si detectan alguna actividad maliciosa.

Compartir información de forma segura

Compartir información a través del correo electrónico, el almacenamiento en la nube y los servicios de mensajería se ha convertido en una parte habitual de la comunicación personal y profesional. Sin embargo, la comodidad de estas plataformas también conlleva riesgos de seguridad, especialmente cuando se manejan datos sensibles o confidenciales.

Al compartir información por correo electrónico, es importante utilizar el cifrado para proteger el contenido de los mensajes. Las transmisiones de correo electrónico estándar no son intrínsecamente seguras y, sin cifrado, pueden ser interceptadas y leídas por terceros no autorizados. El uso de servicios que ofrecen cifrado integrado, como Gmail con su modo confidencial, y herramientas de terceros como PGP (Pretty Good Privacy) para cifrar el contenido del correo electrónico, puede ayudar a proteger la información confidencial de la exposición. Además, evite compartir información confidencial, como contraseñas o detalles financieros, directamente en el cuerpo de un mensaje de correo electrónico. En su lugar, considere el uso de métodos seguros para compartir archivos o archivos adjuntos cifrados.

Los *servicios de almacenamiento en la nube*, como Google Drive, Dropbox o Microsoft OneDrive, son populares para compartir documentos y archivos y colaborar en ellos. Al utilizar estos servicios, asegúrese de que los permisos de acceso estén configurados correctamente para evitar el acceso no autorizado.

Los *servicios de mensajería* como WhatsApp, Signal y Telegram se utilizan con frecuencia para comunicarse rápidamente y compartir archivos. Muchas de estas plataformas ofrecen cifrado de extremo a extremo, lo que garantiza que solo el remitente y el destinatario puedan leer los mensajes. Sin embargo, es importante verificar que el cifrado esté habilitado, ya que algunos servicios pueden ofrecerlo como una función opcional. Para datos muy confidenciales, puede ser más apropiado utilizar un correo electrónico seguro o un almacenamiento en la nube cifrado en lugar de aplicaciones de mensajería.

Verifique siempre la identidad de los destinatarios antes de compartir información confidencial. Los cibercriminales suelen utilizar tácticas de ingeniería social para hacerse pasar por contactos de confianza y engañar a las personas para que compartan datos confidenciales.

La mensajería instantánea cifrada se ha convertido en una herramienta fundamental para la comunicación segura y privada tanto en el ámbito personal como profesional. A diferencia de los servicios de mensajería tradicionales, que pueden transmitir mensajes en texto sin formato, la mensajería cifrada garantiza que el contenido de las conversaciones esté protegido contra el acceso no autorizado, incluso si se intercepta durante la transmisión.

El *cifrado de extremo a extremo* (E2EE) es la piedra angular de la mensajería instantánea segura. Garantiza que solo el remitente y el destinatario puedan leer el contenido de un mensaje. Ni siquiera el proveedor de servicios puede acceder a los mensajes para descifrarlos, ya que las claves de cifrado se almacenan solo en los dispositivos que participan en la conversación.

Además de E2EE, algunas aplicaciones de mensajería ofrecen funciones como mensajes que desaparecen y seguridad de pantalla para mejorar la privacidad. Los mensajes que desaparecen se eliminan automáticamente después de un período específico, lo que reduce el riesgo de que la

información confidencial se almacene en su dispositivo o en el dispositivo del destinatario de forma indefinida.

También es importante mantener actualizadas las aplicaciones de mensajería cifrada para protegerlas contra vulnerabilidades y ataques que podrían socavar su seguridad. Los desarrolladores lanzan actualizaciones periódicamente para corregir fallas de seguridad y mejorar los protocolos de cifrado, por lo que mantener actualizadas las aplicaciones es esencial para mantener el más alto nivel de protección.

Por último, ten en cuenta los metadatos que las aplicaciones de mensajería cifrada pueden seguir recopilando, como información sobre cuándo y con quién te comunicas. Si bien algunas aplicaciones, como Signal, minimizan la recopilación de metadatos, otras pueden retener más información. Para obtener el mayor nivel de privacidad, elige aplicaciones que sean transparentes en cuanto a sus políticas de recopilación de datos y prioricen la seguridad del usuario.

Al utilizar servicios de mensajería instantánea encriptada de manera responsable y comprender sus características de seguridad, puede asegurarse de que sus conversaciones privadas permanezcan confidenciales y seguras frente a espías y actores maliciosos.

Ejercicios guiados

1. Explique cómo los acuerdos de confidencialidad (NDA) ayudan a proteger la información confidencial en entornos comerciales. ¿Cuáles son algunas de las limitaciones de los NDA?

2. ¿Cuál es la relación entre el phishing, la ingeniería social y el robo de identidad, y cómo pueden las personas protegerse de estas amenazas?

3. ¿Por qué es importante la clasificación de la información para la protección de datos y cuáles son los niveles de clasificación más comunes?

Ejercicios exploratorios

1. Investigue una filtración o violación de datos de alto perfil reciente que involucre a una organización conocida. Describa cómo ocurrió la filtración, qué información confidencial se expuso y el impacto que tuvo en la empresa y sus clientes. Analice qué medidas implementó la organización después de la filtración para mejorar su seguridad y prevenir incidentes futuros.

2. Investigue la eficacia de los diferentes modelos de clasificación de información que utilizan las organizaciones, como el sistema de clasificación del gobierno de los EE. UU. (por ejemplo, Confidencial, Secreto, Alto secreto) o los modelos comerciales (por ejemplo, Público, Interno, Confidencial, Altamente confidencial). Compare cómo estos modelos ayudan a gestionar la seguridad de los datos y el cumplimiento de las normas legales. Analice las ventajas y los posibles inconvenientes de cada modelo en diferentes contextos organizacionales.

 Esta obra está bajo la licencia CC BY-NC-ND 4.0.

Resumen

Esta lección cubre varios aspectos de la seguridad digital, haciendo hincapié en la importancia de proteger la información confidencial y reconocer amenazas como el phishing y la ingeniería social. Explica cómo las filtraciones de datos y las comunicaciones interceptadas pueden provocar pérdidas financieras, daños a la reputación y consecuencias legales, y destaca el papel de los acuerdos de confidencialidad (NDA) para salvaguardar la información confidencial. El análisis también se extiende al robo de identidad, detallando cómo los atacantes utilizan datos personales robados para hacerse pasar por víctimas y las tácticas empleadas en estafas y ataques de scareware que manipulan a las víctimas a través del miedo y el engaño. También se destaca la importancia de la clasificación de la información para aplicar medidas de seguridad adecuadas y garantizar el cumplimiento de las regulaciones, lo que ilustra cómo las organizaciones pueden proteger sus activos críticos de manera eficaz.

Respuestas a los ejercicios guiados

1. Explique cómo los acuerdos de confidencialidad (NDA) ayudan a proteger la información confidencial en entornos comerciales. ¿Cuáles son algunas de las limitaciones de los NDA?

   Los NDA protegen la información confidencial al obligar legalmente a las partes involucradas a mantener la confidencialidad de los datos compartidos y a no divulgarlos ni utilizarlos indebidamente. Describen el alcance de la información confidencial, las obligaciones de las partes y las consecuencias de incumplir el acuerdo. Este marco legal ayuda a garantizar que los datos confidenciales, como secretos comerciales o planes comerciales, no se compartan con personas no autorizadas ni se utilicen en contra de los intereses de la empresa. Sin embargo, los NDA tienen limitaciones, ya que no pueden evitar infracciones accidentales o intencionales por parte de personas que tienen acceso a la información. El cumplimiento requiere vigilancia, monitoreo y una sólida cultura interna de seguridad de datos.

2. ¿Cuál es la relación entre el phishing, la ingeniería social y el robo de identidad, y cómo pueden las personas protegerse de estas amenazas?

   El phishing y la ingeniería social son tácticas que utilizan los atacantes para manipular a las personas para que revelen información personal, que luego puede usarse para el robo de identidad. El phishing generalmente implica correos electrónicos o mensajes de texto fraudulentos que parecen provenir de fuentes legítimas, engañando a las víctimas para que brinden información confidencial como nombres de usuario y contraseñas. La ingeniería social abarca una gama más amplia de tácticas, como la suplantación de identidad o el uso de pretextos, para engañar a las personas para que rompan los protocolos de seguridad. Para protegerse, las personas deben tener cuidado con las solicitudes de información no solicitadas, evitar hacer clic en enlaces sospechosos, usar contraseñas seguras y únicas, habilitar la autenticación multifactor y monitorear regularmente sus cuentas para detectar actividad sospechosa.

3. ¿Por qué es importante la clasificación de la información para la protección de datos y cuáles son los niveles de clasificación más comunes?

   La clasificación de la información es esencial para la protección de datos porque ayuda a las organizaciones a identificar y aplicar las medidas de seguridad adecuadas a los diferentes tipos de datos en función de su sensibilidad. Al categorizar la información en niveles como pública, interna, confidencial y altamente confidencial, las organizaciones pueden controlar el acceso y garantizar que los datos confidenciales se gestionen de forma segura. Por ejemplo, la información altamente confidencial, como secretos comerciales o estrategias comerciales críticas, debe almacenarse en entornos seguros y con acceso controlado y transmitirse a través de canales cifrados. La clasificación adecuada también ayuda a las organizaciones a cumplir

con los requisitos legales y reglamentarios, lo que reduce el riesgo de violaciones de datos y sanciones por incumplimiento.

Respuestas a los ejercicios exploratorios

1. Investigue una filtración o violación de datos de alto perfil reciente que involucró a una organización conocida. Describa cómo ocurrió la filtración, qué información confidencial se expuso y el impacto que tuvo en la empresa y sus clientes. Analice qué medidas implementó la organización después de la filtración para mejorar su seguridad y prevenir incidentes futuros.

   Un ejemplo es la filtración de datos de Facebook en 2018, donde la información personal de aproximadamente 87 millones de usuarios se compartió indebidamente con la firma de consultoría política Cambridge Analytica. La filtración se produjo debido a políticas laxas de intercambio de datos, donde una aplicación de terceros recopiló datos de los usuarios y luego los compartió sin consentimiento. Los datos expuestos incluían detalles personales de los usuarios, me gusta e incluso mensajes privados. El impacto en Facebook fue grave, lo que provocó un escrutinio legal, una caída significativa en el valor de las acciones y la pérdida de la confianza de los usuarios. En respuesta, Facebook implementó políticas de intercambio de datos más estrictas, mejoró sus prácticas de privacidad de datos e introdujo más transparencia en las formas en que las aplicaciones de terceros acceden a la información de los usuarios.

2. Investigue la eficacia de los diferentes modelos de clasificación de información utilizados por las organizaciones, como el sistema de clasificación del gobierno de EE. UU. (por ejemplo, Confidencial, Secreto, Alto secreto) o los modelos comerciales (por ejemplo, Público, Interno, Confidencial, Altamente confidencial). Compare cómo estos modelos ayudan a gestionar la seguridad de los datos y el cumplimiento de las normas legales. Analice las ventajas y los posibles inconvenientes de cada modelo en diferentes contextos organizacionales.

   El sistema de clasificación del gobierno de EE. UU. está diseñado para proteger la información de seguridad nacional al categorizarla como Confidencial, Secreta o Alto secreto en función del daño potencial que podría causar su divulgación no autorizada. Este modelo es altamente estructurado y eficaz para gestionar datos gubernamentales confidenciales, pero puede ser complejo de implementar y mantener. Los modelos comerciales, como Público, Interno, Confidencial y Altamente confidencial, son más flexibles y más fáciles de aplicar en varias industrias. Ayudan a las empresas a proteger la información confidencial y cumplir con regulaciones como GDPR o CCPA. Sin embargo, si no se gestionan adecuadamente, estos modelos pueden generar inconsistencias en el manejo de datos y una protección insuficiente de activos críticos.

025.3 Protección de la privacidad

Referencia al objetivo del LPI

Security Essentials version 1.0, Exam 020, Objective 025.3

Peso

2

Áreas de conocimiento clave

- Comprensión de la importancia de la información personal.
- Comprensión de cómo la información personal puede usarse con fines maliciosos.
- Comprensión de los conceptos de recopilación de información, elaboración de perfiles y seguimiento de usuarios.
- Administrar la configuración de privacidad del perfil en plataformas de redes sociales y servicios en línea.
- Comprensión del riesgo de publicar información personal.
- Comprensión de los derechos con respecto a la información personal (por ejemplo, GDPR)

Lista parcial de archivos, términos y utilidades

- Acoso cibernético
- Cookies HTTP, huellas digitales del navegador, seguimiento de usuarios
- Bloqueadores de scripts y bloqueadores de anuncios en navegadores web
- Perfiles en servicios online y redes sociales
- Contactos y configuración de privacidad en redes sociales

Linux Professional Institute

Lección 1

Certificado:	Fundamentos de seguridad
Versión:	1.0
Tema:	025 Identidad y privacidad
Objetivo:	025.3 Protección de la privacidad
Lección:	1 de 1

Introducción

La enorme cantidad de datos que se comparten en los servicios en línea y las plataformas de redes sociales facilita que los cibercriminales aprovechen vulnerabilidades y accedan a información confidencial. Muchas personas comparten detalles personales (sin saberlo) que pueden usarse en su contra, como su ubicación, información de contacto o incluso datos financieros. Esta exposición puede tener consecuencias graves, como robo de identidad, pérdidas financieras y acceso no autorizado a cuentas personales y profesionales.

Mantener la confidencialidad de la información personal requiere ser proactivo en la gestión de cómo y dónde se comparten sus datos. Esto implica configurar los ajustes de privacidad en las cuentas de redes sociales y otros servicios en línea para limitar lo que es visible para los demás.

Igualmente importante es saber cómo se recopila, perfila y rastrea la información en línea. Los sitios web y los anunciantes suelen utilizar técnicas como las cookies HTTP, la identificación del navegador y el seguimiento de usuarios para crear perfiles detallados de los usuarios. Reconocer estos métodos de seguimiento y saber cómo mitigarlos (utilizando navegadores centrados en la privacidad, desactivando las cookies de terceros o empleando herramientas de protección contra el seguimiento) puede ayudar a mantener su anonimato y proteger su información personal.

Esta lección lo guiará a través de los pasos esenciales para administrar su configuración de privacidad de manera efectiva, comprender los riesgos asociados con la exposición de datos personales y navegar por las complejidades de la recopilación de información en línea y el seguimiento de usuarios.

La importancia de la información personal

La información personal incluye cualquier dato que pueda utilizarse para identificar o conocer más sobre una persona. Esto incluye nombres, direcciones, números de teléfono, direcciones de correo electrónico, números de seguridad social, detalles financieros e incluso comportamientos en línea como el historial de navegación y la actividad en las redes sociales. Si bien compartir cierta información personal es necesario para utilizar servicios en línea o participar en actividades cotidianas, comprender su importancia y las posibles consecuencias de su uso indebido es crucial para mantener la privacidad y la seguridad.

La información personal es valiosa no solo para las personas, sino también para las empresas, los gobiernos y los ciberdelincuentes. Las empresas utilizan los datos personales con fines de marketing, para personalizar los anuncios y mejorar la experiencia de los usuarios. Sin embargo, estos datos también pueden recopilarse, compartirse o venderse sin el consentimiento de la persona, lo que genera problemas de privacidad. Los gobiernos utilizan la información personal con fines administrativos y de seguridad, pero también puede utilizarse indebidamente para la vigilancia o para controlar y manipular a las poblaciones. Los ciberdelincuentes, por otro lado, ven la información personal como un objetivo lucrativo para cometer fraudes, robos de identidad y otras actividades maliciosas. Esto puede provocar pérdidas financieras, calificaciones crediticias dañadas y un proceso largo y estresante para recuperar la propia identidad y proteger las cuentas afectadas. Más allá del daño financiero, la información personal puede explotarse para el acoso, el ciberacoso y el hostigamiento, lo que pone a las personas en riesgo tanto en línea como en su vida personal.

Otro aspecto son los riesgos potenciales asociados con las filtraciones y violaciones de datos. Las filtraciones de datos ocurren cuando se expone información confidencial debido a fallas de seguridad o ciberataques. Estos incidentes pueden dar lugar al acceso no autorizado a datos personales, lo que resulta en robo de identidad, fraude financiero y otras consecuencias graves. Mantener actualizados los programas y sistemas, utilizar contraseñas seguras y únicas y habilitar la autenticación multifactor son algunas de las prácticas que pueden ayudar a mitigar el riesgo de filtraciones de datos.

Para proteger la información personal, es esencial comprender cómo la recopilan, almacenan y utilizan las distintas entidades. Al suscribirse a servicios en línea, las personas deben revisar las políticas de privacidad y tener en cuenta qué datos aceptan compartir.

El riesgo de publicar información personal

Uno de los principales riesgos asociados con la publicación de información personal es el robo de identidad. Los cibercriminales pueden usar detalles como su nombre, fecha de nacimiento o dirección para hacerse pasar por usted y obtener acceso a sus cuentas financieras, crédito o incluso servicios gubernamentales. Si tienen suficiente información, pueden solicitar tarjetas de crédito o préstamos y realizar compras fraudulentas en su nombre, lo que puede derivar en pérdidas financieras y una calificación crediticia dañada. Las consecuencias del robo de identidad pueden ser duraderas y requerir mucho tiempo y esfuerzo para resolverlas y restablecer su situación financiera.

Además del fraude financiero, la información personal compartida en línea puede hacer que usted sea vulnerable a ataques de phishing. Los estafadores suelen utilizar datos personales para crear correos electrónicos o mensajes convincentes que parecen provenir de fuentes legítimas, como su banco, empleador o una agencia gubernamental. Estos mensajes suelen tener como objetivo engañarlo para que proporcione información más confidencial, como contraseñas o números de cuenta, o para que descargue software malicioso en sus dispositivos. Cuanta más información tengan los atacantes, más fácil será crear una estafa convincente que podría dar lugar a graves violaciones de seguridad.

La información personal también puede ser utilizada para el acoso y el hostigamiento, tanto en línea como en la vida real. Compartir su ubicación, planes de viaje o incluso sus rutinas diarias puede exponerlo a atención no deseada o convertirlo en un blanco fácil para aquellos con intenciones maliciosas. Los acosadores cibernéticos pueden usar esta información para rastrear sus movimientos, intimidarlo o difundir información errónea sobre usted. Esto puede derivar en enfrentamientos en el mundo real, poniendo en riesgo su seguridad física. Incluso información aparentemente inocua, como los nombres de sus familiares o las escuelas a las que asistió, puede usarse para crear un perfil suyo que los acosadores y hostigadores pueden explotar.

Los individuos malintencionados pueden utilizar información de las redes sociales para cometer acoso cibernético (o cybermobbing), lo que provoca graves consecuencias para la salud mental y emocional de sus víctimas. El acoso cibernético se refiere a ataques repetidos e intencionales, como insultos, humillaciones y amenazas, llevados a cabo a través de plataformas digitales como redes sociales y aplicaciones de mensajería, a menudo utilizando perfiles falsos para ocultar la identidad del agresor.

Existen plataformas, que suelen encontrarse en la red oscura, que recopilan datos personales robados y los venden a los cibercriminales. Estas plataformas, conocidas como “corredores de datos” o “mercados clandestinos”, recopilan información procedente de violaciones de datos, ataques de phishing y otras actividades ilícitas, creando extensas bases de datos que incluyen todo tipo de datos, desde direcciones de correo electrónico y contraseñas hasta números de la

seguridad social, detalles de tarjetas de crédito e incluso historiales médicos. Los cibercriminales pueden comprar estos conjuntos de datos para cometer robos de identidad, fraudes financieros u otras actividades maliciosas.

Además, una vez que se publica información personal en línea, es difícil eliminarla o controlar su difusión. Incluso si eliminas una publicación o una cuenta, pueden quedar copias de tu información en otros sitios web, en los cachés de los motores de búsqueda o en el dispositivo de otra persona.

Para mitigar estos riesgos, es fundamental pensar detenidamente antes de publicar cualquier información personal en línea. Limite la cantidad de datos personales que comparte en las plataformas de redes sociales y utilice la configuración de privacidad para controlar quién puede ver sus publicaciones y los detalles de su perfil.

Derechos sobre la información personal – GDPR

Con el aumento del uso de plataformas digitales para actividades personales y profesionales, la protección de la información personal se ha convertido en un problema crítico a nivel mundial. Se han promulgado diversas leyes y reglamentos para dar a las personas un mayor control sobre sus datos personales y garantizar que las organizaciones gestionen estos datos de manera responsable. Uno de los reglamentos más completos e influyentes es el *Reglamento General de Protección de Datos* (GDPR) de la Unión Europea, que establece un alto estándar para la privacidad y seguridad de los datos. Comprender sus derechos con respecto a la información personal según reglamentos como el GDPR es esencial para proteger su privacidad y garantizar que sus datos se gestionen de manera adecuada.

El GDPR, que entró en vigor en mayo de 2018, está diseñado para proteger los datos personales de los ciudadanos y residentes de la UE regulando la forma en que las organizaciones recopilan, almacenan y procesan dicha información. Se aplica a cualquier organización, independientemente de su ubicación, que procese datos personales de personas en la UE. Esto significa que incluso las empresas con sede fuera de la UE deben cumplir con el GDPR si manejan datos de residentes de la UE.

Uno de los derechos fundamentales que establece el GDPR es el derecho a estar informado. Esto significa que las personas tienen derecho a saber qué datos personales se recopilan, cómo se utilizan, con quién se comparten y durante cuánto tiempo se conservarán. Las organizaciones deben proporcionar información clara y transparente sobre sus actividades de procesamiento de datos, normalmente a través de políticas o avisos de privacidad.

Otro derecho fundamental es el derecho de acceso, que permite a las personas solicitar una copia de sus datos personales que obran en poder de una organización. Esto permite a las personas ver

qué información se almacena y verificar que sea precisa y que se esté procesando de conformidad con la ley. Además del derecho de acceso, las personas también tienen el derecho de rectificación, que les permite solicitar correcciones de datos inexactos o incompletos.

El GDPR también establece el *derecho de supresión*, comúnmente conocido como el "derecho al olvido". Este derecho permite a las personas solicitar la eliminación de sus datos personales en determinadas circunstancias, como cuando los datos ya no son necesarios para el fin para el que fueron recopilados o si retiran su consentimiento. Sin embargo, este derecho no es absoluto y puede estar sujeto a limitaciones, como cuando los datos son necesarios para cumplir con obligaciones legales o fines de interés público.

El *derecho a restringir el procesamiento* permite a las personas limitar el uso que se hace de sus datos. Por ejemplo, si una persona cuestiona la exactitud de sus datos, puede solicitar que se restrinja su uso hasta que se resuelva el problema. De manera similar, el *derecho a oponerse* permite a las personas oponerse al procesamiento de sus datos personales para fines específicos, como el marketing directo o la elaboración de perfiles.

Otro aspecto importante del GDPR es el derecho a la portabilidad de los datos. Este derecho permite a las personas obtener sus datos personales en un formato estructurado, de uso común y legible por máquina y transferirlos a otra organización. Esto puede resultar especialmente útil al cambiar de proveedor de servicios o consolidar datos de diferentes plataformas.

Además de estos derechos, el GDPR también exige que las organizaciones implementen medidas de seguridad adecuadas para proteger los datos personales y notifiquen las violaciones de datos a las autoridades pertinentes y a las personas afectadas dentro de las 72 horas posteriores al descubrimiento. Esto garantiza un alto nivel de responsabilidad y capacidad de respuesta en caso de un incidente de seguridad de datos.

Si bien el GDPR es específico de la Unión Europea, su influencia ha llevado a la adopción de normas de protección de datos similares en todo el mundo. Por ejemplo, la *Ley de Privacidad del Consumidor de California* (CCPA) otorga derechos similares a los residentes de California, incluido el derecho a saber qué datos personales se están recopilando y el derecho a solicitar su eliminación. Otras jurisdicciones están siguiendo el ejemplo con sus propias leyes de protección de datos, lo que refleja una tendencia mundial hacia derechos de privacidad de datos más sólidos.

Comprender sus derechos en virtud de estas normas es fundamental para mantener el control sobre su información personal. Si considera que se han violado sus derechos en materia de protección de datos, tiene derecho a presentar una reclamación ante la autoridad de protección de datos pertinente en su país.

Recopilación de información, elaboración de perfiles y seguimiento de usuarios

Los sitios web, los anunciantes y, en ocasiones, las entidades malintencionadas utilizan la recopilación de información, la elaboración de perfiles y el seguimiento de los usuarios para recopilar y analizar datos sobre las actividades en línea de los usuarios. Estas técnicas ayudan a crear perfiles detallados que se pueden utilizar para diversos fines, como la publicidad personalizada, la mejora de la experiencia del usuario o, en algunos casos, la manipulación del comportamiento y la invasión de la privacidad.

Las cookies HTTP son una de las herramientas más comunes para rastrear la actividad del usuario. Las cookies son pequeños archivos de texto que los sitios web que visitan almacenan en el dispositivo del usuario. Pueden recordar detalles de inicio de sesión, rastrear artículos en un carrito de compras o almacenar preferencias del usuario. Aunque las cookies son esenciales para habilitar ciertos servicios, como recordar la configuración de idioma o el estado de inicio de sesión de un usuario, también plantean problemas de privacidad. Los anunciantes suelen utilizar cookies de terceros, establecidas por dominios distintos del que visita el usuario, para rastrear a los usuarios en diferentes sitios web, creando una vista completa de sus hábitos y preferencias de navegación. Estos datos se pueden utilizar para ofrecer anuncios específicos o incluso venderse a otras entidades para un análisis más detallado.

La *huella digital* del navegador es una técnica de seguimiento más sofisticada que recopila varios puntos de datos sobre la configuración del navegador y del dispositivo del usuario. Se puede combinar información como la resolución de pantalla, las fuentes instaladas, los complementos del navegador y los detalles del sistema operativo para crear un identificador único, o "huella digital" (fingerprint), para cada usuario. A diferencia de las cookies, que se pueden eliminar o bloquear, las huellas digitales son más difíciles de evadir porque no dependen de los datos almacenados en el dispositivo del usuario. Este método permite a los rastreadores identificar y seguir a los usuarios en diferentes sitios web sin necesidad de consentimiento explícito, lo que plantea importantes preocupaciones sobre la privacidad.

El *seguimiento de usuarios* abarca una amplia gama de formas de monitorear y analizar el comportamiento en línea. Más allá de las cookies y las huellas digitales, el seguimiento de usuarios puede incluir técnicas como los píxeles de seguimiento, que son imágenes diminutas e invisibles incrustadas en páginas web o mensajes de correo electrónico. Cuando un usuario carga una página o abre un mensaje de correo electrónico que contiene un píxel de seguimiento, este envía información al rastreador, como la dirección IP del usuario, el tipo de dispositivo y la hora exacta en que se vio el contenido. Estos datos se pueden utilizar para monitorear la participación del usuario, realizar un seguimiento de las conversiones para campañas de marketing o recopilar datos para una mayor elaboración de perfiles.

La información recopilada a través de estos métodos de seguimiento se puede utilizar para crear perfiles detallados de usuarios individuales, incluidos sus intereses, sus hábitos e incluso su estatus social y económico. Estos perfiles son valiosos para los anunciantes que buscan ofrecer anuncios muy específicos, pero también plantean cuestiones éticas y de privacidad. Por ejemplo, estos perfiles detallados se pueden utilizar para influir en el comportamiento del usuario, limitar el acceso a contenido o incluso discriminar en función de características percibidas.

Comprender estos conceptos es fundamental para quienes desean proteger su privacidad en línea. Los usuarios pueden tomar medidas como borrar las cookies con regularidad, utilizar navegadores o extensiones centrados en la privacidad que bloqueen los rastreadores y emplear redes privadas virtuales (VPN) para ocultar sus actividades en línea.

En general, si bien la recopilación de información, la elaboración de perfiles y el seguimiento de los usuarios pueden mejorar las experiencias y los servicios en línea, también plantean riesgos importantes para la privacidad personal.

Administrar la configuración de privacidad del perfil

Mantener la privacidad en las plataformas de redes sociales y los servicios en línea es esencial para proteger la información personal de accesos no deseados. Gestionar la configuración de privacidad del perfil de manera eficaz ayuda a controlar quién puede ver sus datos personales, publicaciones y actividades, lo que reduce el riesgo de uso indebido por parte de actores maliciosos o incluso de contacto no deseado por parte de extraños.

Cada plataforma suele ofrecer una serie de configuraciones que permiten a los usuarios determinar qué información es visible para el público, para los amigos o solo para los contactos seleccionados. Por ejemplo, en Facebook, puedes elegir que tus publicaciones sean visibles solo para amigos o incluso para una lista personalizada de personas, mientras que en LinkedIn, puedes controlar quién ve tus conexiones o actualizaciones de perfil. Revisar y actualizar estas configuraciones con regularidad es fundamental, ya que las plataformas suelen actualizar sus políticas y configuraciones de privacidad, a veces con opciones más públicas por defecto sin una notificación clara a los usuarios.

Perfiles en Servicios Online y Redes Sociales

Los perfiles en los servicios en línea y las redes sociales actúan como representaciones digitales de los usuarios y contienen información personal, como nombres, fotos, datos de contacto e intereses. Estos perfiles se pueden utilizar para conectarse con otras personas, compartir contenido y participar en diversas actividades en línea. Sin embargo, también pueden convertirse en fuentes de información para los ciberdelincuentes que buscan robar identidades o realizar ataques dirigidos. Los usuarios deben tener cuidado con los detalles que comparten en sus perfiles

y considerar las posibles implicaciones si esta información cayera en las manos equivocadas. Por ejemplo, compartir demasiada información personal, como su lugar de trabajo o su rutina diaria, puede hacerlo vulnerable a ataques de phishing o incluso a amenazas del mundo real. Es conveniente limitar la cantidad de datos personales visibles en su perfil y asegurarse de que la información confidencial, como su dirección de casa o su número de teléfono, se mantenga privada.

La gestión de contactos y la configuración de privacidad es una parte fundamental para proteger tu experiencia en las redes sociales. Las plataformas como Facebook, Instagram y LinkedIn permiten a los usuarios clasificar sus contactos en diferentes grupos, como amigos, familiares y conocidos, y personalizar la configuración de privacidad para cada grupo. Esto significa que puedes compartir ciertas publicaciones con amigos cercanos y mantenerlas ocultas a los contactos profesionales o al público en general. Además, muchas plataformas te permiten bloquear o silenciar a los contactos que pueden estar acosándote o enviándote spam. Ser selectivo con respecto a quién aceptas como contactos y revisar tu configuración de privacidad con regularidad puede ayudar a evitar el acceso no autorizado a tu información personal y garantizar una experiencia más segura y agradable en las redes sociales.

Los *bloqueadores de scripts* y *bloqueadores de anuncios* son herramientas que ayudan a proteger su privacidad y mejorar su experiencia de navegación al evitar que el navegador cargue contenido no deseado de los sitios web. Los bloqueadores de scripts, como *NoScript* o *uMatrix*, permiten a los usuarios controlar qué scripts pueden ejecutarse en los sitios que visitan. Esto puede evitar la ejecución de scripts maliciosos, que de otro modo podrían rastrear su actividad, robar sus datos o inyectar malware en su sistema. Al deshabilitar scripts innecesarios, los usuarios también pueden mejorar su seguridad y reducir los tiempos de carga de las páginas.

Los bloqueadores de anuncios, como *AdBlock Plus* o *uBlock Origin*, evitan que se muestren anuncios en las páginas web. Si bien los anuncios se utilizan principalmente con fines de marketing, también pueden ser fuentes de seguimiento y recopilación de datos. Muchos anuncios contienen rastreadores que monitorean el comportamiento del usuario en varios sitios y crean perfiles detallados de los hábitos de navegación. El bloqueo de estos anuncios no solo reduce el desorden visual y acelera la navegación, sino que también minimiza la cantidad de datos recopilados sobre usted. Además, los bloqueadores de anuncios pueden evitar que se exponga a anuncios maliciosos (malvertising) que pueden hacer que visite sitios web dañinos o descargue malware en su dispositivo.

Los bloqueadores de scripts y bloqueadores de anuncios mencionados anteriormente están disponibles como extensiones para los navegadores Google Chrome, Firefox y Opera, y su código fuente también está disponible en el repositorio de código público de GitHub.

Ejercicios guiados

1. Describa cómo la gestión de la configuración de privacidad en las plataformas de redes sociales puede ayudar a proteger su información personal del acceso no autorizado. Incluya ejemplos específicos de configuraciones que usaría en plataformas como Facebook o LinkedIn y explique su importancia para mantener la privacidad.

2. Explique cómo los bloqueadores de scripts y de anuncios pueden mejorar su privacidad y seguridad en línea. Analice la diferencia entre los dos tipos de herramientas y proporcione ejemplos de cómo se puede utilizar cada una de ellas de manera eficaz mientras navega por Internet.

 Esta obra está bajo la licencia CC BY-NC-ND 4.0. |

Ejercicios exploratorios

1. Investiga y compara las configuraciones de privacidad disponibles en dos plataformas de redes sociales diferentes. Identifica al menos tres diferencias clave en la forma en que cada plataforma permite a los usuarios administrar su información personal y controlar quién puede ver su contenido. Explica cómo estas diferencias podrían afectar tu decisión sobre qué tipo de información personal compartir en cada plataforma.

Resumen

Comprender la importancia de la confidencialidad es esencial para proteger los datos personales del acceso no autorizado y el uso indebido. Esto implica no solo estar atento a cómo se comparte la información personal, sino también administrar de manera eficaz la configuración de privacidad en varios servicios en línea y plataformas de redes sociales. Muchas personas exponen información confidencial sin saberlo a través de sus actividades digitales, lo que las hace vulnerables a amenazas como el robo de identidad, los ataques de phishing y la ingeniería social. Al aprender a navegar por la configuración de privacidad y reconocer las amenazas de seguridad comunes, las personas pueden tomar medidas proactivas para proteger sus datos personales y mantener el control sobre su identidad digital.

 Esta obra está bajo la licencia CC BY-NC-ND 4.0. |

Respuestas a los ejercicios guiados

1. Describe cómo la gestión de la configuración de privacidad en las plataformas de redes sociales puede ayudar a proteger tu información personal del acceso no autorizado. Incluye ejemplos específicos de configuraciones que usarías en plataformas como Facebook o LinkedIn y explica su importancia para mantener la privacidad.

   La gestión de la configuración de privacidad ayuda a controlar quién puede ver tu información personal, publicaciones y actividades. Por ejemplo, en Facebook, puedes limitar la visibilidad de tu perfil solo a “Amigos”, lo que evita que extraños vean tus datos personales y publicaciones. Además, con la función “Listas de amigos”, puedes compartir publicaciones solo con grupos seleccionados, como “Amigos cercanos”, y excluir a “Compañeros de trabajo”. En LinkedIn, configurar tu perfil para restringir quién puede ver tu lista de conexiones ayuda a evitar que posibles reclutadores o competidores accedan a tu red. Estas configuraciones son cruciales para mantener la privacidad y reducir el riesgo de contacto no deseado o uso indebido de tu información.

2. Explique cómo los bloqueadores de scripts y de anuncios pueden mejorar su privacidad y seguridad en línea. Analice la diferencia entre los dos tipos de herramientas y proporcione ejemplos de cómo se puede utilizar cada uno de ellos de forma eficaz mientras navega por Internet.

   Los bloqueadores de scripts, como NoScript, evitan que se ejecuten scripts potencialmente maliciosos en los sitios web al permitir que los usuarios elijan qué scripts están habilitados. Esto ayuda a proteger contra el seguimiento no autorizado y la ejecución de código malicioso. Por ejemplo, un bloqueador de scripts puede impedir que se carguen scripts de seguimiento de terceros en un sitio web de noticias, lo que evita el seguimiento de sus hábitos de navegación.

   Los bloqueadores de anuncios, como AdBlock Plus, bloquean los anuncios que a menudo contienen elementos de seguimiento y pueden reducir el riesgo de exposición a publicidad maliciosa.

   Si bien los bloqueadores de scripts controlan los scripts y los bloqueadores de anuncios se centran en bloquear los anuncios visuales, ambas herramientas se pueden utilizar juntas para crear un entorno de navegación más seguro al minimizar la recopilación de datos y prevenir posibles amenazas de seguridad.

Respuestas a los ejercicios exploratorios

1. Investiga y compara las configuraciones de privacidad disponibles en dos plataformas de redes sociales diferentes. Identifica al menos tres diferencias clave en cómo cada plataforma permite a los usuarios administrar su información personal y controlar quién puede ver su contenido. Explica cómo estas diferencias podrían afectar tu decisión sobre qué tipo de información personal compartir en cada plataforma.

   Este ejercicio requiere una investigación sobre las configuraciones de privacidad específicas de ambas plataformas. Por ejemplo, Facebook ofrece un control más granular sobre la visibilidad de las publicaciones con opciones como “Amigos excepto…” o listas “Personalizadas”, mientras que Instagram permite principalmente una configuración de perfil “Público” o “Privado”. Además, Facebook ofrece opciones para limitar quién puede enviar solicitudes de amistad o ver tu lista de amigos, que no están disponibles en Instagram. Estas diferencias afectan el nivel de control que tienen los usuarios sobre su información, lo que potencialmente hace que Facebook sea una plataforma preferible para compartir de forma más controlada, mientras que Instagram puede requerir más precaución en lo que se publica debido a su marco de privacidad más simple.

Pie de imprenta

© 2025 Linux Professional Institute: Learning Materials, “Security Essentials (Version 1.0)”.

PDF generado: 2025-01-20

Esta obra está bajo la licencia de Creative Commons Atribución-NoComercial-SinDerivadas 4.0 Internacional (CC BY-NC-ND 4.0). Para ver una copia de esta licencia, visite

https://creativecommons.org/licenses/by-nc-nd/4.0/

Si bien el Linux Professional Institute se ha esforzado de buena fe para asegurar que la información y las instrucciones contenidas en este trabajo sean precisas, el Linux Professional Institute renuncia a toda responsabilidad por errores u omisiones, incluyendo sin limitación alguna la responsabilidad por daños resultantes del uso o la confianza en este trabajo. El uso de la información e instrucciones contenidas en este trabajo es bajo su propio riesgo. Si cualquier muestra de código u otra tecnología que esta obra contenga o describa, está sujeta a licencias de código abierto o a derechos de propiedad intelectual de otros, es su responsabilidad asegurarse de que el uso que haga de ellos cumpla con dichas licencias y/o derechos.

LPI Learning Materials son una iniciativa del Linux Professional Institute (https://lpi.org). Los materiales y sus traducciones pueden encontrarse en https://learning.lpi.org.

Para preguntas y comentarios sobre esta edición, así como sobre todo el proyecto, escriba un correo electrónico a: learning@lpi.org.