



La seguridad informática

Objetivos

- Advertir la importancia que tiene el plan de seguridad informática, saber sus partes y entender las metodologías de diseños.
- Conocer los mecanismos de seguridad más importantes en cualquier organización y sus características.
- Plantear las líneas generales de los procesos de auditoría informática y, en especial, aquellos asociados a los de seguridad informática.
- Concretar metodologías en el control de acceso a través de permisos de usuarios y profundizar en ellas.
- Dominar herramientas que permitan la gestión del control de acceso a través de permisos.
- Ahondar en las tareas de monitorización de una red mediante la aplicación de estrategias de configuración e implementación y el conocimiento de herramientas para su explotación.
- Reflexionar sobre las intenciones que se persiguen en el análisis de intrusión y las herramientas más comunes.

Contenidos

- 1.1. Planificación de la seguridad informática
- 1.2. Servicios y mecanismos de seguridad
- 1.3. Desarrollo de auditorías
- 1.4. Permisos y derechos de usuarios
- 1.5. Monitorización del tráfico de red
- 1.6. Ataques a una red. Test de intrusión
- 1.7. Kali Linux. Auditoría y seguridad informática

Introducción

Es totalmente indudable que la seguridad de los sistemas informáticos de cualquier organización se ha convertido en uno de los pilares más sensibles y vulnerables, y se hace imprescindible la búsqueda de mecanismos para fortalecerla. El plan de seguridad se convierte en una herramienta fundamental en el tratamiento de la información, en la explotación de los recursos tecnológicos y en el desarrollo de nuevas aplicaciones y tecnologías para la implantación de sistemas más avanzados.

La proliferación de las nubes, de los servidores remotos, de las aplicaciones contratadas como servicios, de dispositivos cada vez más vulnerables, del desarrollo tan rápido de los sistemas operativos, de la ingesta de software de cualquier tipo y para cualquier usuario, etc., están teniendo un impacto en la explotación de las tecnologías de la información y de la sociedad de la comunicación que abre un universo de inmensas estrategias maliciosas que pueden acabar con cualquier organización.

Cada una de las diferentes unidades de esta obra se desarrolla basándose en las fases de elaboración de una correcta planificación de la seguridad informática. Asuntos como las estrategias para el análisis de riesgos y las herramientas para su detección; el análisis de sus posibles impactos en el sistema y las herramientas para estos análisis; políticas de seguridad y qué factores van a intervenir en el plan de contingencias y herramientas para la detección de estos factores y el establecimiento de dichas políticas, mecanismos tecnológicos para llevarlas a cabo, sus auditorías y las herramientas más potentes del mercado actual son apartados que se desarrollan como introducción.

Se profundiza en la fase de identificación de usuarios y monitorización del tráfico de red, así como en la gestión de contraseñas en sistemas operativos libres y propietarios, y el uso adecuado de herramientas de análisis del tráfico para la detección de posibles anomalías funcionales, de vulnerabilidades y de intrusión.

■ 1.1. Planificación de la seguridad informática

La organización CN-Cert definía la *seguridad informática* en su método Magerit como «la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles».

La falta de seguridad puede deberse al desconocimiento de las posibles amenazas o a la falta de conocimiento de las medidas de seguridad que existen para paliarlas. Se debe tener claro qué hay que proteger, de qué se quiere salvaguardar y cómo hacerlo.

Los elementos que proteger son los datos, el software, el hardware y los elementos fungibles. Para ello, el inventario es una herramienta importante. Debe recoger toda la información necesaria acerca de los diferentes activos de la organización. Estos activos están

sujetos a diferentes tipos de ataques: alteración o manipulación, intercepción o monitorización, fabricación o suplantación e interrupción o denegación de servicio.



Figura 1.1. El plan de seguridad informática es un documento fundamental para el control y la seguridad en la explotación de un entorno tecnológico que maneja información. Este plan se convierte en una herramienta que establece las medidas que todo el personal de una organización debe cumplir con carácter obligatorio.

En cualquier organización es posible que se produzcan incidentes que dañen sus activos. El desencadenante de dicho incidente se denomina **amenaza**, y la posibilidad de que se materialice sobre un activo es una **vulnerabilidad**. Las vulnerabilidades se miden por la probabilidad de que una amenaza ocurra y la frecuencia con la que lo puede hacer.

En caso de una amenaza, se hace necesario estimar la degradación del activo afectado. Dicha consecuencia se denomina **impacto**. El impacto puede ser cuantitativo (por ejemplo, pérdidas económicas) o cualitativo (por ejemplo, la imagen de la empresa, o su responsabilidad legal frente al impacto). La posibilidad de que se produzca un impacto en la organización es lo que se conoce como **riesgo**.

■ ■ ■ 1.1.1. Análisis de riesgos e impactos

Lo primero que se debe hacer es identificar los posibles daños o peligros con el fin de definir las medidas que tomar. Se han de tener en cuenta el valor de los activos, la frecuencia de la amenaza y su desconocimiento, la consecuencia del daño, la eficacia de las medidas de seguridad y su coste.

El **análisis de riesgo** lo puede hacer personal interno o externo, apoyándose en el uso de metodologías diseñadas con antelación. Algunas conocidas son Magerit (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas), Marion, Mehari, modelo de McCumber, etcétera.



Figura 1.2. Tras analizar y reducir los riesgos, se procede a la identificación de las posibles amenazas y vulnerabilidades, así como de riesgos potenciales, sus probabilidades y consecuencias, con el fin de buscar alternativas que los eviten, los minimicen o los asuman cuando la probabilidad de que ocurran sean bajísimas o el coste de eliminarlos sea excesivamente elevado.

El **impacto** es la consecuencia negativa que una organización padece cuando una función se ve interrumpida y ello conlleva un tiempo de recuperación permitido tal que no acarree su inactividad total. El daño producido por un impacto puede ser más o menos crítico. El análisis de impacto persigue identificar cada una de las funciones críticas, priorizando las estrategias de recuperación para minimizar el tiempo de recuperación.



Figura 1.3. Primero se definen los tipos de impactos: pérdida de rentabilidad, aumento de gastos, peligro para los individuos o impacto comercial, de imagen y jurídico. Luego, se identifican las funciones críticas y las dependencias entre ellas a través de cuestionarios normalizados. Más tarde, se determina el impacto causado por la interrupción de cada función crítica y los recursos mínimos necesarios para su recuperación.

■ ■ ■ 1.1.2. Plan de contingencias

Una vez que se han analizado los riesgos y se han detectado los impactos, es de vital importancia desarrollar un plan de actuación frente a cualquier amenaza, analizando las posibles vulnerabilidades y estableciendo políticas de actuación para prevenirlas. Este

plan de actuación a favor de la seguridad informática se denomina *plan de contingencias de la seguridad informática*.

En el plan de contingencias se describe cómo se debe actuar ante eventos que produzcan riesgos en la continuidad del negocio, con medidas técnicas, organizativas y humanas precisas para minimizar el número de decisiones que tomar durante una contingencia, definiendo *contingencia* como algo que puede suceder o no.



Figura 1.4. Las fases del plan de seguridad informática comienzan en el análisis de riesgos e impactos. Posteriormente, se elabora el plan de contingencias, que después se evalúa a través de las diferentes auditorías programadas para luego establecer las políticas de seguridad necesarias.

Un plan de contingencias está compuesto por el plan de respaldo, con las medidas que desarrollar antes del incidente; el plan de emergencias, con las normas de actuación durante el incidente, y el plan de recuperación, con las normas que seguir después de materializarse la amenaza.

Tras el diseño del plan de contingencias, se efectúan las pruebas que se consideren oportunas para detectar las deficiencias y corregirlas. El plan será evaluado y mantenido, y será modificado para adaptarse en todo momento a las necesidades de los sistemas.

■ ■ 1.1.3. Políticas de seguridad

Las **políticas de seguridad** son pautas y procedimientos que dan soporte a la seguridad conforme a requisitos legales y de negocio. Deben revisarse, actualizarse y darse a conocer a todo el personal de la organización para su fiel cumplimiento.

Para implementar la política de seguridad se usan metodologías para definir qué se puede hacer y qué no, con el fin de establecer mecanismos que estarán diseñados para prevenir y detectar la intrusión, así como recuperar el sistema.

Los **mecanismos de prevención** se realizan antes de que ocurra un incidente para evitarlo, e incluyen tanto elementos físicos como lógicos. Se desarrollan para anticiparse a los efectos de amenazas accidentales o deliberadas vinculadas a las catástrofes

originadas por incendios, inundaciones o terremotos que pueden provocar cortes eléctricos, en las comunicaciones o destrucción de soportes informáticos, que deben estar protegidos físicamente por sistemas de alimentación ininterrumpida y por otros de detección y protección contra incendios e inundaciones. El acceso físico a los elementos que componen todo el sistema estará gestionado por un control de acceso eficiente para evitar cualquier alteración de la información o robo de soportes con información confidencial.

Los **mecanismos de protección lógicos** pretenden evitar la intrusión en el sistema a través de la implantación de protección de cortafuegos, software para contrarrestar los programas con malas intenciones, y controles de identificación y autenticación.

Los **mecanismos de detección** se desarrollan para detectar cambios en el sistema con el objetivo de alertar de algún intento de la intrusión. Se usan herramientas que monitorean y avisan de cambios realizados asegurando la integridad de la información almacenada en los sistemas de almacenamiento.

Los **mecanismos de recuperación** se ponen en marcha cuando ya ha tenido lugar el ataque, para devolver el sistema al estado normal. Las herramientas de análisis forense investigan su alcance, cómo se ha producido y qué actividades se han llevado a cabo durante el mismo. El uso de copias de seguridad es fundamental en esta etapa, en la que resulta imprescindible usar mecanismos que aseguren la recuperación y continuidad de toda la información y que interrumpan la actividad del sistema el mínimo tiempo posible.

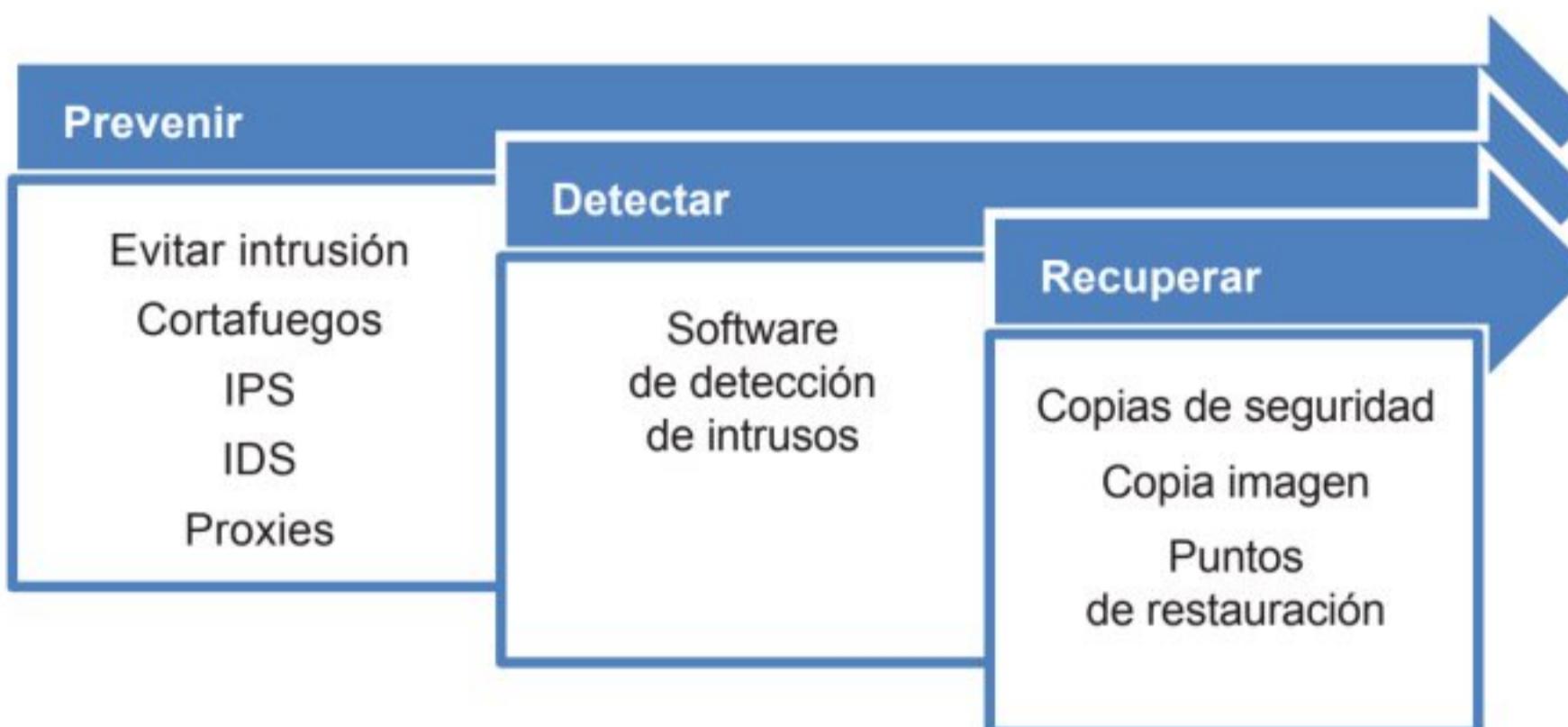


Figura 1.5. Mecanismos para prevenir, detectar y recuperar la normalidad del funcionamiento del sistema en caso de una intrusión no planificada.

Actividad propuesta 1.1

Elaboración de un plan de seguridad informática

En esta actividad se propone elaborar un plan de seguridad informática. Busca algunos ejemplos que se puedan localizar en internet y plantea un plan de seguridad básico para una empresa de manipulación, compra y venta de alimentos compuesta por una topología con diferentes dispositivos de red y servidores. Todos estos elementos están alojados en

diferentes salas de computadores. Hay aproximadamente doscientos empleados que trabajan en diferentes secciones, y cada uno de ellos hacen un uso diferente del sistema informático. Los apartados que deben aparecer en el plan de seguridad son:

- Políticas de seguridad informática de los usuarios que usan las diferentes tecnologías.
- Sistema de seguridad informática.
- Apertura y cierre de las salas.
- Consideraciones al operar con el equipamiento.
- Control de acceso, identificación de los usuarios y requisitos de las contraseñas.
- Prohibiciones en el uso de aplicaciones.

■ 1.2. Servicios y mecanismos de seguridad

La seguridad se puede dividir, a grandes rasgos, en seguridad física y seguridad lógica. La **seguridad física** hace referencia a la protección de la organización frente a accesos no autorizados y ataques físicos a los equipos e instalaciones. La **seguridad lógica** aplica mecanismos y barreras que protegen la información desde su propio medio. Algunos de los mecanismos más usados son:

- Limitar el acceso a determinados programas o ficheros mediante el uso de cifrado o mediante claves.
- Otorgar los privilegios mínimos y necesarios a todos los usuarios del sistema, evitando dar permisos de más.
- Aplicar una gestión de la explotación del software eficiente por parte de los usuarios del sistema.
- Controlar qué información entra y sale del sistema de información, y gestionar eficientemente la autorización de los usuarios para tales efectos.

Los tres pilares de la seguridad de la información corresponden a los requisitos de confidencialidad, de integridad y de disponibilidad. Además, existen otros que complementan los anteriores, que son el de autenticación, el de no repudio y el de trazabilidad.

A continuación, se detalla el significado de cada requisito:

1. Requisito de confidencialidad: solo los usuarios autorizados conocen la información, lo cual evita el acceso malintencionado o no autorizado. Los recursos a los que se recurre para garantizar la confidencialidad son:



Figura 1.6. La seguridad informática se sustenta en tres pilares fundamentales: la confidencialidad, la disponibilidad y la integridad.

- Gestión de privilegios: los usuarios que estén autorizados operarán solo con la información que se requiere, ni más ni menos.
- Cifrado de la información: evita que pueda ser legible por usuarios no autorizados que hayan interceptado la información almacenada o transmitida.

2. Requisito de integridad: solo el personal autorizado podrá modificar la información, ya que esta debe ser siempre exacta y completa. Para garantizar la integridad, se llevan a cabo algunos de estos procedimientos:

- Monitorización del tráfico de red para detectar posibles intrusiones.
- Auditorías de sistemas para evaluar y modificar las políticas de seguridad.
- Implementación de sistemas de control de cambios a través del uso de los ficheros log.
- Implementación de procesos eficientes de copias de seguridad y de recuperación.

3. Requisito de disponibilidad: solo accesible por los usuarios autorizados. La información debe estar disponible cuando sea necesario. Se implementan políticas de control como:

- Acuerdo de nivel de servicio o SLA.
- Disponibilidad de sistemas a través de redundancia y alta disponibilidad, por ejemplo, usando平衡adores de carga de tráfico para minimizar el impacto de DDoS.

4. Requisito de autenticación: garantiza que el usuario es quien dice ser.

5. Requisito de no repudio: asegura que ninguna de las partes involucradas en el manejo de cierta información pueda negar su participación.

6. Requisito de trazabilidad: registra las acciones y en qué momento se han llevado a cabo por parte de un usuario o proceso en el sistema.

Nota técnica



El acuerdo de nivel de servicio o SLA (Service Level Agreement) se refiere a aquel entre un proveedor que provee de un servicio y un cliente que lo usa, con el fin de pactar el nivel de calidad del mismo (disponibilidad horaria, documentación disponible o personal que da soporte al servicio).

Actividad propuesta 1.2

Cambiar la contraseña de root

Cambia la contraseña de la cuenta de usuario root en tu máquina Linux. Para ello, ejecuta el comando `passwd root`. Evidentemente, se debe ser superusuario root para poder modificar la contraseña. Introduce una contraseña más segura, con 14 caracteres, que combine letras mayúsculas, minúsculas y caracteres especiales, por ejemplo, `p4Alm5Z63kc@t3`.

Primero, memorízala y cámbiala. Es de vital importancia no anotarla en ningún lugar.



Figura 1.7. Los mecanismos de autenticación e identificación aseguran que solo los usuarios autorizados puedan acceder a las áreas permitidas de todo el sistema e impiden accesos ilegítimos. Ejemplos son las contraseñas, una propiedad que solo una persona conoce de sí misma, una tarjeta inteligente o de identidad propia, firmas digitales, técnicas biométricas, etcétera.

La gestión controlada de contraseñas es un proceso muy importante en la función de autenticación e identificación. Las premisas que seguir en la gestión de identificadores y contraseñas son:

- No deben ser almacenadas ni deben ser facilitadas a terceros.
- Deben ser sustituidas cuando sea posible y han de evitarse secuencias lógicas, nombres, teléfonos o fechas señaladas.
- Han de contener mayúsculas, minúsculas, letras, números y signos de puntuación. Su longitud mínima recomendable es de 14 caracteres.
- Se deberían cambiar una vez al mes y no se deberían emplear las usadas con anterioridad.

Los elementos de identificación más usados son:

- **Tarjetas con bandas magnéticas:** poseen una banda en la que se almacena información para identificar al usuario mediante tecnología magnética. Se suelen usar para el control de acceso a edificios y tienen un coste muy bajo.
- **Tarjetas inteligentes:** poseen un pequeño circuito integrado que almacena y procesa datos confidenciales. A diferencia de las de bandas magnéticas, tienen más capacidad de memoria y son más seguras. Existen dos tipos, las microprocesadas y las de memoria. Las primeras no almacenan una gran cantidad de datos, pero tienen una memoria protegida a la que solo puede acceder su fabricante, lo que garantiza mayor veracidad en la información que guarda. Las segundas almacenan mayor cantidad de información, pero, al ser fácilmente regrabables, no se garantiza la veracidad de la información almacenada, por lo que se hace necesario usar sistemas de cifrado propios.

- **Criptografía:** se cifra y descifra información para que no sea comprensible por terceros, lo que permite la confidencialidad de la información y la integridad de la misma. Para ello, se usan algoritmos para el cálculo de unos valores alfanuméricos llamados clave. Estos pueden ser privados o públicos y posibilitan diferentes metodologías de cifrado.
- **Firma electrónica:** la componen un conjunto de datos que identifican al individuo o entidad que firma un documento. Se basa en criptografía de clase asimétrica. Existen firmas electrónicas avanzadas que permiten autenticar a la persona y garantizar que la información es veraz. Para ello, serán necesarios prestadores de servicios de certificación que expidan certificados electrónicos, los certificados digitales.
- **Kerberos:** es un protocolo de seguridad que deja que los equipos de una red no se gura revelen su identidad de forma fiable a través del uso de criptografía simétrica, lo que impide que se envíen por la red contraseñas que puedan ser interceptadas por terceros. Cuenta con una base de datos con todas las contraseñas de los usuarios y de los servidores. Las de los usuarios se cifran; las de los servidores se generan aleatoriamente y se cifran posteriormente. Todos los usuarios o servicios que vayan a utilizar Kerberos deben registrarse.
- **Tecnologías de identificación biométricas:** se registra digitalmente algún rasgo físico o del comportamiento humano. Estos rasgos biométricos se comparan con un patrón ya almacenado en una base de datos. Si no se encuentra coincidencia, no se autentica al individuo. Este tipo de tecnología se usa para identificar personas, nunca para autenticar procesos u otro tipo de agentes. Los rasgos deben ser universales y únicos, es decir, todo individuo poseerá dicha propiedad y una única instancia posible de la misma. Los más usados son los patrones faciales, de la retina y de las venas, así como la forma de la mano, las huellas dactilares y el reconocimiento de voz e iris.

Actividad propuesta 1.3

Tecnología de identificación biométrica con Windows Hello

La herramienta Windows Hello permite iniciar sesión usando reconocimiento facial o de huellas digitales en sistemas Windows. Habilita Windows Hello para poder iniciar sesión usando la cámara para reconocimiento de la cara. Si dispones de un dispositivo USB para la detección de huellas dactilares, procede a habilitarlo y usa este sistema de identificación.

Elabora un documento explicando la instalación y configuración, así como la explotación de este servicio de Windows.

■ 1.3. Desarrollo de auditorías

La auditoría informática es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema asegura los activos, manteniendo su integridad y cumpliendo con los objetivos, haciendo un uso eficaz, eficiente y efectivo de los recursos.

Las tareas que se acometen son:

- **Revisión de los sistemas:** se evalúan los planes de implantación de sistemas y sus mejoras.
- **Revisión de las instalaciones informáticas:** se revisan las políticas y procedimientos del personal, según estándares, seguridad, redes de comunicación y copias de seguridad.
- **Revisión de las aplicaciones:** se comprueba la explotación por parte de los usuarios, su utilidad y uso, y se eliminan las aplicaciones que no se utilizan o son obsoletas, a la par que se actualizan todas aquellas que se requieran por explotación y en soluciones de vulnerabilidades.



Figura 1.8. La auditoría informática se lleva a cabo por profesionales de la informática capacitados para recoger y agrupar los posibles riesgos y evaluar las políticas de seguridad que se han establecido con anterioridad para modificarlas en caso de fracaso. Se hace un análisis global de la situación, de rendimientos, de red y cifrados, de comunicaciones, de hardware, de software, de vulnerabilidades, etcétera.

Las áreas que deben ser revisadas en una auditoría son, principalmente, las siguientes:

- Comprobar que se cumplen las normas vigentes, por lo que se hace necesario conocer los requerimientos legales establecidos.
- Velar por la eficacia y eficiencia del sistema informático. Se verifica la calidad de los sistemas de información y se proponen mejoras cuando proceda.
- Verificar la seguridad de los sistemas de información, de los equipos, de las comunicaciones y redes, del comercio y correo electrónico.
- Mantener las instalaciones y los equipos.
- Controlar la seguridad física (control de accesos físicos y protección ante desastres naturales y del entorno).
- Vigilar accesos lógicos y gestión de privilegios.
- Programar copias de seguridad y planes de continuidad.
- Usar mecanismos de cifrado y firma electrónica.
- Proteger el sistema contra código malicioso.

A partir de los resultados obtenidos mediante auditorías, se establecen las responsabilidades y procedimientos para evitar y minimizar cualquier tipo de amenaza, así como para proceder a su posterior recuperación. En esto consiste el diseño de una política de seguridad. Atendiendo al recurso que se desea proteger, se distingue entre medidas de seguridad física y medidas de seguridad lógica:

- **Medidas físicas** (seguridad física): protegen el hardware, analizando su ubicación y amenazas físicas. Se estudia la ubicación correcta de los dispositivos hardware, las medidas preventivas contra incendios o inundaciones y el control de acceso físico para evitar robos o manipulación de sistemas de almacenamiento.
- **Medidas lógicas** (seguridad lógica): velan por el software del sistema, ya sea el propio sistema operativo o los programas instalados. Protegen en toda instancia la información o datos de usuario: contraseñas, permisos de usuario, cifrado de datos y de las comunicaciones, actualizaciones, copias de seguridad, filtrado de conexiones, etcétera.

Según el momento en el que se ponen en marcha estas medidas de seguridad, existe la seguridad pasiva y la seguridad activa:

- **Seguridad pasiva:** las medidas son correctivas y minimizan los efectos causados por una amenaza. Son posteriores a la amenaza, y son la seguridad física y las copias de seguridad.
- **Seguridad activa:** se hacen día a día para evitar cualquier ataque. Son todas las de seguridad lógica.

Clara es una herramienta con interesantes novedades que permite realizar auditorías de la seguridad de una forma bastante cómoda y que se adapta a la normativa actual. Es una aplicación desarrollada para Windows.

Lynis es otra herramienta de seguridad muy completa que posibilita realizar auditorías del sistema Linux. Se distribuye bajo licencia GNU GPL v3 y es gratuita.

Actividad resuelta 1.1

Análisis de la herramienta Lynis

Instala la herramienta Lynis en tu sistema Linux. Indica paso a paso la información que muestra el programa.

Solución

Para instalar este producto basado en distribuciones Debian, se ejecuta el comando

```
apt-get install lynis
```

La herramienta se ejecutará con el comando

```
lynis -c o lynis -Q,
```

lo que permite hacer un escaneo rápido. La aplicación muestra en la pantalla la información obtenida en cada fase de escaneo.

Primero, enseña un resumen del sistema y el estado de la aplicación e indica si existen nuevas actualizaciones. Revisa las herramientas ya instaladas en el sistema para actualizar e

instalar las que no estén. Luego, analiza el gestor de arranque detectado en el sistema, los servicios que se arrancan al iniciar y otros aspectos del núcleo del sistema operativo.

Luego se ve información de la memoria y de los procesos que se están ejecutando. En caso de que existan procesos que no se estén usando y estén consumiendo memoria principal, estos son señalados como posibles procesos zombies.

Más tarde, exhibe información sobre los usuarios, grupos y los sistemas de autenticación usados en el sistema.

A continuación, analiza los escudos del sistema, sistemas de ficheros y los soportes de almacenamiento masivo. Los servicios de nombre de dominio y el gestor de paquetes de la distribución también se pueden ver, además de todo lo relacionado con dispositivos de red, impresoras compartidas, servidores de correo y estado del cortafuegos. Se muestra también información sobre servidores web instalados, servidores SSH, SNMP, bases de datos del sistema, controladores de dominio LDAP, programas desarrollados en PHP, servidores proxy con squid e información del login del sistema.

A continuación, analiza el estado del proceso inetd, identificación y tareas programadas, información de la cuenta, criptografía del sistema y elementos relacionados con la virtualización.

Finaliza con otros aspectos de seguridad como frameworks, integridad de archivos y analizadores de malware.

Actividad propuesta 1.4

Auditorías con la herramienta Lynis

Una vez instalada y ejecutada, confecciona una auditoría del sistema completa. Captura la información que muestra por pantalla, obtén la información más relevante y confecciona un documento técnico.

1.4. Permisos y derechos de usuarios

La mayoría de los sistemas operativos cuentan con sistemas de archivos que permiten asignar derechos de acceso a cada uno de los archivos alojados en el sistema de almacenamiento para cada usuario o grupos de usuarios. Con este tipo de control por asignación de permisos, se puede restringir o permitir el acceso de un determinado usuario a cada uno de los archivos, tanto para su visualización como para su modificación, ejecución o eliminación. Además, se contará con herramientas que permitan controlar la creación de ficheros por parte de los usuarios y limitar el espacio en disco disponible para cada usuario.

Los sistemas gestores de bases de datos también cuentan con herramientas avanzadas para la gestión de usuarios y control de auditorías. A través de conceptos como *usuario*, *privilegio*, *perfil* o *rol*, se puede llevar a cabo un control completo sobre qué puede consultar un usuario determinado sobre el esquema completo de la base de datos, desde solo poder acceder a una columna de una tabla hasta poder crear, modificar y eliminar innumerables objetos en el sistema.



Figura 1.9. Proporcionar inicios de sesión únicos de forma segura que no revelen credenciales y que puedan gestionar, controlar y filtrar operaciones privilegiadas, así como configurar el modo en que el usuario explota los recursos son mecanismos esenciales para fortalecer los sistemas de acceso. Además, permiten auditar las acciones de cada uno de los usuarios en la explotación de los recursos del sistema.

■ ■ ■ 1.4.1. La gestión de usuarios y contraseñas en Linux

El fichero /etc/passwd contiene la lista de los usuarios locales en el equipo. Cualquier atacante con acceso a este fichero puede leer la información que contiene. Cada línea representa un usuario y está compuesta por los campos

login:contraseña:UID:GID:comentario: directorio-personal:Shell-del-usuario

A continuación, se detalla la descripción de cada campo:

- **Nombre del usuario:** es el identificador del usuario. Debe ser único en todo el sistema.
- **Contraseña cifrada:** Si hay una x, la contraseña se almacena en el fichero /etc/shadow. Si es un signo de exclamación, la cuenta está bloqueada.
- **Identificador de usuario:** es un número que identifica a cada usuario de forma única en todo el sistema. Al usuario root le corresponde el UID=0. Para los procesos demonios se usa el rango 1-100, y para los usuarios creados por el administrador, se utilizan números superiores a 500.
- **Identificador de grupo:** igual que con los usuarios, cada grupo tiene un número que lo identifica de forma única.
- **Descripción:** almacena información descriptiva del usuario.
- **Directorio personal:** es el directorio personal de trabajo del usuario.
- **Shell-usuario:** se trata del Shell por defecto que el usuario tiene asignado. También se puede incluir cualquier otro comando, por ejemplo, uno que prohíba su conexión.

El fichero /etc/group contiene la definición de los grupos de usuarios y los usuarios que pertenecen a cada uno de ellos. Está compuesto por cuatro campos

group:contraseña:GID:lista-de-usuarios

La descripción de estos campos es:

- **Nombre del grupo:** nombre único del grupo.
- **Contraseña:** está asociada al grupo. Se usa para controlar que un usuario pueda cambiar de un grupo a otro a través del comando `newgrp`.
- **Identificador de grupo:** almacena el número que identifica de forma única a cada grupo.
- **Lista de usuarios:** la lista de nombres de usuarios, separados por comas, ya creados en el sistema y que pertenecen a dicho grupo.

El fichero `/etc/shadow` contiene cada una de las contraseñas cifradas de cada usuario e información sobre su validez. Cada línea se compone de nueve campos de la forma

`login:contraseña-cifrada:duración:limitación-cambio:obligación-cambio:
antes-vencimiento:después-vencimiento:días-desactivado:reservado`

Donde cada uno de los campos se usan para:

- **Login:** identificador del usuario.
- **Contraseña:** contraseña cifrada. Sus valores iniciales indican qué algoritmo se ha usado para cifrarla, por ejemplo, a través de MD5 (`1`), blowfish (`$2a$`), SHA-256 (`5`), SHA-512 (`6`), etcétera.
- **Duración:** número de días desde el 1/1/1970 hasta el último cambio de contraseña.
- **Limitación-cambio:** número de días sin poder cambiar la contraseña. Con 0, la contraseña puede ser cambiada en cualquier momento.
- **Obligación-cambio:** número de días a partir de los cuales se debe cambiar la contraseña.
- **Antes-vencimiento:** número de días antes del vencimiento de la contraseña durante los cuales se debe avisar al usuario.
- **Después-vencimiento:** número de días después del vencimiento de la contraseña tras los cuales se desactiva la cuenta.
- **Días-desactivado:** número de días desde el 1/1/1970 hasta el momento en el que se desactivó la cuenta.
- **Reservado:** reservado para futuras ampliaciones.

La gestión de usuarios en sistemas Linux se apoya en la edición de estos ficheros, de tal forma que, añadiendo una línea en `/etc/passwd`, en `/etc/shadow`, en `/etc/group`, en `/etc/skel`, o cambiando los permisos y propietario del directorio personal y la contraseña cifrada, se dará de alta a un nuevo usuario.

Para facilitar estas tareas, existen los comandos `useradd`, `groupadd`, `usermod`, `groupmod`, `userdel` y `groupdel`, que permitirán crear, modificar y eliminar usuarios y grupos, respectivamente.

Al crear un usuario con `useradd`, se deben especificar todas sus opciones básicas. Si no se indica nada, se le asignarán las opciones por defecto contenidas en el fichero `/etc/defaults/useradd`. Para adjudicarle una contraseña, se usa el comando `passwd` con la sintaxis `passwd nombre-usuario`.

Actividad propuesta 1.5

Gestión de usuarios en Linux mediante el uso de comandos

Usando las técnicas desarrolladas en este apartado, procede a generar diferentes usuarios y grupos, y a asignarles privilegios sobre diversos directorios y ficheros. Procede de la siguiente manera:

- Crea cuatro cuentas de usuarios con contraseñas cifradas (*usuario01*, *usuario02*, *usuario03* y *usuario04*). Usa el comando `useradd` y cifra las contraseñas a través de alguna herramienta que genere contraseñas cifradas.
- Crea dos grupos de usuarios, llamados *ventas* y *jefeventas*. Los dos primeros usuarios estarán en el primer grupo (*ventas*), y los otros dos, en el segundo.
- Crea dos directorios (llamados *general* y *exclusivo*) e incluye cuatro ficheros en él.
- Asigna a los usuarios *usuario01* y *usuario03* los siguientes privilegios con el comando `chmod`, según la información expuesta a continuación:

	Lectura	Escritura	Ejecución
Fichero 1	Sí	No	No
Fichero 2	Sí	Sí	No
Fichero 3	Sí	Sí	Sí
Fichero 4	Sí	No	No
Directorio general	Sí	Sí	No
Directorio 2 exclusivo	Sí	No	No

Para *usuario02*, solo hay permiso de lectura sobre el directorio exclusivo, y todos los permisos sobre el directorio general.

El usuario *usuario04* tiene todos los permisos en todos los ficheros y directorios.

1.4.2. La seguridad de las contraseñas

El objetivo es establecer una interfaz entre los programas y los distintos métodos de autenticación, con el fin de que sea transparente para dichos programas. Esta interfaz se basa en el uso de módulos de autenticación, de tal forma que, sin modificar el propio sistema, se pueden usar diferentes métodos para la identificación y autenticación (lectores de huellas, voz, imagen, etc.). Se pueden explotar opciones de contraseñas de un solo uso, restricciones de acceso en determinados horarios o establecer políticas de autenticación más complejas para determinados usuarios y grupos. Los módulos PAM (Pluggable Authentication Module) pueden imponer otras exigencias más estrictas para el cambio de contraseña.

LDAP es un protocolo que ofrece el acceso a un servicio de directorio implementado sobre un entorno de red para gestionar la explotación de los recursos de la misma. Se puede ejecutar sobre TCP/IP o sobre cualquier otro servicio de transferencia orientado a la conexión.

Se pueden modificar todos los campos de /etc/shadow con el comando `passwd`. Se puede hacer lo mismo con el comando `chage`. Algunas opciones disponibles son:

- **-l:** bloquea la cuenta al añadir el símbolo '!' delante de la contraseña cifrada.
- **-u:** desbloquea la cuenta. No es posible activar una cuenta que no tenga contraseña; en tal caso, se debe utilizar la opción `-f`.
- **-d:** suprime la contraseña de la cuenta.
- **-n cantidad:** duración mínima en días de la contraseña.
- **-x cantidad:** duración máxima en días de la contraseña.
- **-w cantidad:** número de días antes de un aviso.
- **-i cantidad:** periodo de gracia antes de la desactivación si ha vencido la contraseña.
- **-S:** estado de la cuenta.

Actividad resuelta 1.2

Configurar una contraseña con `passwd`

Crea una cuenta de usuario llamado `jefe_venta`. Esta cuenta de usuario debe esperar a 10 días después de la inserción de una nueva contraseña para poder cambiarla; su contraseña será válida durante 60 días; se le avisará 3 días antes de que deba cambiarla; si no cambia la contraseña después de los 60 días, dispone de 7 días antes de que sea bloqueada.

Solución

```
passwd -n 10 -x 60 -w 3 -i 7 jefe_venta
```

Actividad propuesta 1.6

La gestión de contraseñas con PAM

PAM (Pluggable Authentication Modules) es un mecanismo para la autenticación centralizada de usuarios que deja gestionar las políticas de seguridad de las diferentes aplicaciones que hagan uso de él.

Instala los paquetes `slapd` y `ldap-utils` en tu máquina Linux. Modifica el contenido del archivo `/etc/hosts` con el fin de almacenar la relación de la dirección IP estática del servidor con los nombres lógicos previstos.

A continuación, instala la librería `libnss-ldap`. Sigue los pasos de configuración.

Después, configura cómo autenticar usuarios. Para ello, usa el script `auth-cliente-config` para modificar los archivos de configuración de PAM y NSS.

Actualiza la configuración de las políticas de autenticación predeterminadas de PAM.

■ 1.5. Monitorización del tráfico de red

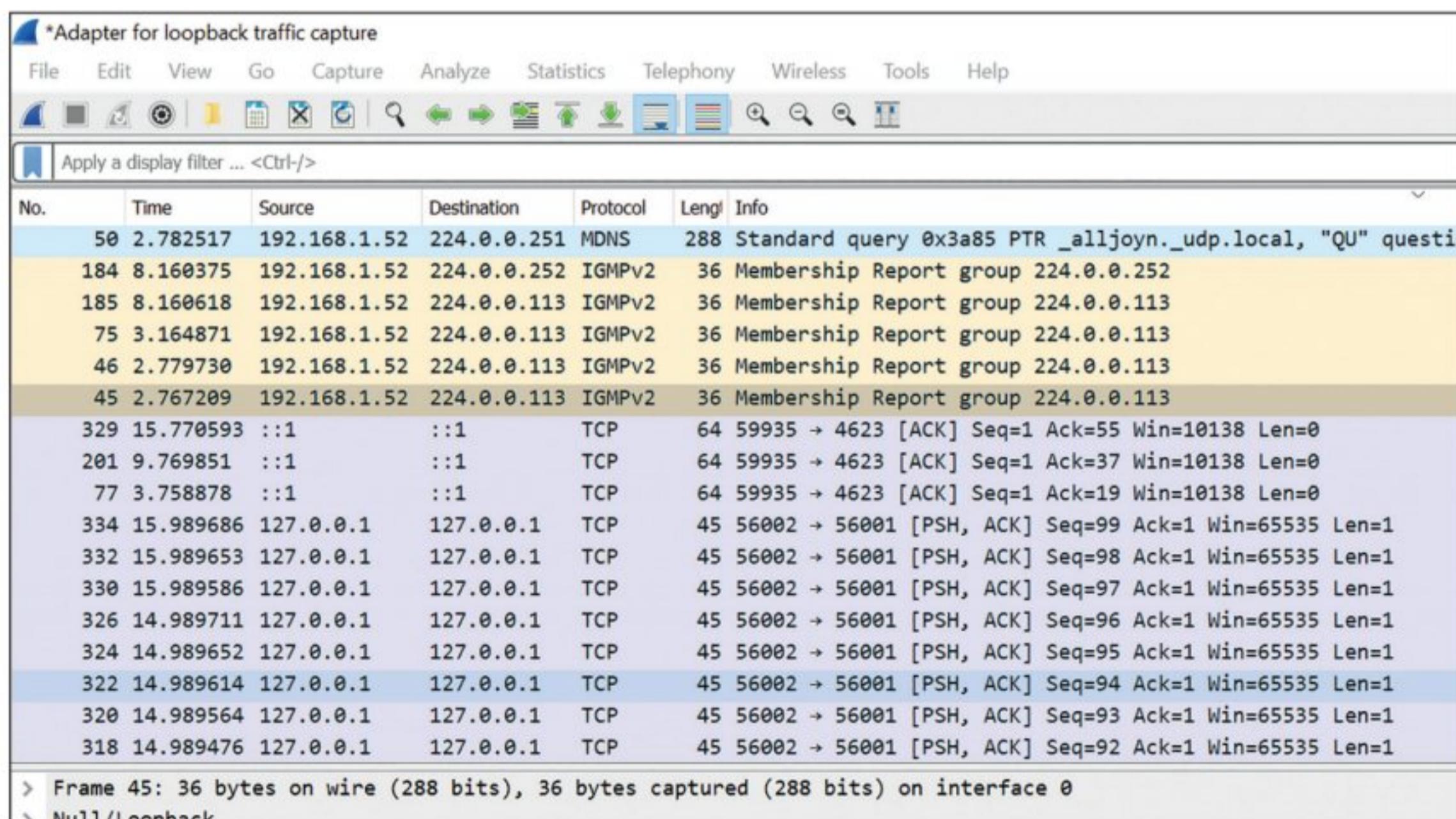
Un sistema de monitorización tiene como objetivo la detección de elementos de red que están sobrecargados o que no trabajan adecuadamente por diversos problemas.

Wireshark es un analizador open-source de protocolos diseñado por Gerald Combs, disponible tanto para plataformas Windows como Unix. Originalmente, se llamaba **Ethereal**, y era muy usado desde el punto de vista didáctico para el estudio de comunicaciones y resolución de problemas de red. Actualmente, se ha convertido en uno de los mejores analizadores de red y cuenta con una amplia gama de filtros que facilitan la definición de búsqueda para más de 1000 protocolos. Captura todos los paquetes de datos y visualiza su contenido campo a campo. Existe una versión en línea de comandos denominada **Tshark** muy similar a la herramienta **Tcpdump**.

■ ■ 1.5.1. La herramienta Wireshark

A continuación, se va a detallar el uso de esta potente y famosa aplicación que permite realizar análisis muy avanzados sobre qué ocurre en una red mediante la monitorización de los paquetes de datos que se transfieren entre los diferentes dispositivos de red.

La herramienta se puede descargar desde su web oficial (www.wireshark.org). Una vez instalada, se obtiene una pantalla como la que se muestra en la Figura 1.10.



The screenshot shows the Wireshark interface with the following details:

- Title Bar:** *Adapter for loopback traffic capture
- Menu Bar:** File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help
- Toolbar:** Includes icons for opening files, saving, zooming, and various analysis tools.
- Search Bar:** Apply a display filter ... <Ctrl-/>
- Table:** Displays captured network frames. The columns are No., Time, Source, Destination, Protocol, Length, and Info. The first frame (No. 50) is highlighted in blue.
- Frame Details:** Shows the details for Frame 45, including bytes on wire (288 bits), bytes captured (288 bits), and interface 0.

Figura 1.10. Este analizador de protocolos, a través de la información que muestra sobre los paquetes de datos que se interceptan, permite detectar cualquier problema de comunicación en la red, de mal funcionamiento de los dispositivos e, incluso, intentos de intrusión. Para ello, se hace necesario conocer los diferentes protocolos, principalmente los de enlace, de red y de transporte, y el contenido de sus campos.

En la parte de la izquierda se seleccionará qué tarjeta de red se quiere analizar. Una vez que se presiona el botón start, comienza el inicio de la captura de paquetes. Los campos que se muestran son los siguientes:

- **No (Número):** indica el número de paquete/trama que se está capturando.
- **Time:** señala el tiempo transcurrido en cada paquete capturado.
- **Source:** muestra la dirección IP de la máquina origen que envía los paquetes a nuestra interfaz de red.
- **Destination:** enseña la dirección IP de la máquina destino a la que le va a llegar dicho paquete de datos.
- **Protocol:** marca qué protocolo se está usando en dicha conexión.
- **Length:** deja ver el tamaño del paquete de datos.
- **Info:** exhibe información sobre el comportamiento del protocolo usado.

Para usar filtros, se usa el cuadro de texto Filter. Por ejemplo, si se quisiera filtrar todo el tráfico en la red que sea http y que está enviado la información por el método POST, se escribiría

```
http.request.method=="POST"
```

Este filtro resulta interesante, ya que existen sitios web que envían las credenciales usando el protocolo http por el método POST. Esta vulnerabilidad puede ser usada por un atacante con vistas a interceptar las credenciales transmitidas.

La cadena que usar en el cuadro de texto Filter puede estar compuesta por muchas opciones diferentes. Se usan los operadores && (and) y || (or) para desarrollar expresiones lógicas más complejas. Se emplea el operador == para evaluar si una expresión es igual a otra, y el operador != para evaluar si son diferentes. Cuando la expresión es una cadena, debe ir entre comillas dobles. Las opciones más usadas son:

- **Protocolo.port:** este operador se usa para indicar el puerto usando cierto protocolo. Por ejemplo, tcp.port==80.
- **Protocolo.srcport:** este operador se usa para señalar el puerto de origen. Por ejemplo, tcp.srcport==51.
- **Protocolo.dstport:** este operador se usa para marcar el puerto de destino. Por ejemplo, udp.dstport==51.
- **ip.src:** este operador se usa para enseñar la dirección IP de origen. Por ejemplo, ip.src==192.168.43.143.
- **ip.dst:** este operador se usa para exhibir la dirección IP de destino. Por ejemplo, ip.dst==192.168.1.143.
- **Protocolo.host:** este operador se usa para indicar el nombre de host. Por ejemplo, http.host==www.google.es.
- **Protocolo.date:** para filtrar los paquetes con respecto a una fecha. Por ejemplo, http.date=="Wed, 5 Feb 2020 19:30:40 GMT".

- **http.content_type:** para indicar el tipo de archivo. Por ejemplo, http.content_type=="image/jpeg", http.content_type=="text/html" para un archivo html; http.content_type=="text/css" para una hoja de estilo CSS, y http.content_type=="application/zip" para un archivo comprimido .zip.
- **http.request.method:** para señalar el tipo de petición. Por ejemplo, http.request.method=="GET" indicaría el tipo de petición GET, y http.request.method=="POST" indicaría tipo de petición POST.

■ ■ ■ 1.5.2. La herramienta Tcpdump

La herramienta **Tcpdump** permite analizar e interceptar tráfico de red a través de la línea de comandos y usa la librería libpcap. Este comando puede leer información almacenada en un fichero y guardar el tráfico capturado en otro fichero de salida.



Figura 1.11. La herramienta *Tcpdump* se usa para depurar aplicaciones que se usan en la red, hacer depuraciones de la propia red o capturar mensajes de datos enviados a través de protocolos como telnet o http, que son fáciles de interceptar para conseguir información confidencial, ya que no cifran la información.

Lo primero que se debe indicar es la tarjeta de red que se quiere escuchar. Para ello, se usa la opción **-i**, de tal modo que se escribiría

```
tcpdump -i eth0
```

para escuchar la tarjeta de red eth0.

Para parar de esnifar paquetes se pulsa **ctrl+C**. El programa muestra las estadísticas de los paquetes capturados. Para mostrar un listado de las interfaces de red disponibles, se usa la opción **-D**:

```
tcpdump -D
```

En caso de que se quisiera almacenar la información capturada por *tcpdump* en un fichero, solo se tendría que redirigir la salida estándar. Se usaría el parámetro **-w** seguido del nombre del fichero:

```
tcpdump -i eth0 -w trafico200911.log
```

Para leer la información capturada y almacenada en un fichero a través de la opción **-w** (write), se usa el parámetro **-r** (read) de la forma

```
tcpdump -r trafico200911.log
```

Se puede filtrar la captura de paquetes por el protocolo que se vaya a examinar, capturando por tcp, udp, icmp, arp, etc. Para ello, se indica el protocolo después de la interfaz de red que se quiere escuchar:

```
tcpdump -i eth0 tcp
```

Para señalar el puerto por el que se quiere capturar el tráfico de red, se usa el parámetro port seguido del número de puerto. Para filtrar tráfico http por el puerto tcp 80 y por la tarjeta de red eth1, se escribiría

```
tcpdump -t eth1 tcp port 80
```

Para analizar el tráfico de red DNS por el puerto UDP 53,

```
tcpdump -i eth1 udp port 53
```

Si se quiere indicar un host origen, se usa el parámetro src. Cuando se comienza a usar más de un parámetro, es necesario usar los operadores lógicos and y or. Por ejemplo, si se quiere capturar tráfico que venga de la máquina con IP 192.168.43.143 a través del puerto tcp 80, sería necesario usar el operador and porque se deben dar ambas condiciones, es decir, dicha IP y dicho puerto. El comando sería

```
tcpdump -i eth0 src 192.168.43.143 and tcp port 80
```

Para indicar el host destino, se usa el parámetro dst. Por ejemplo, si se quisiera capturar el tráfico tcp por el puerto 8080 que va a la máquina con IP 192.168.1.43, se escribiría

```
tcpdump -i eth0 dst 192.168.1.43 and tcp port 8080
```

Si se quisiera capturar tráfico que viene o va a una determinada máquina, se usa la opción host. Por ejemplo,

```
tcpdump host 192.168.1.143
```

mostraría tanto los paquetes de entrada como los de salida.

Si en vez de dirección IP se quiere indicar direcciones físicas o MAC, se usa la opción ether. El siguiente ejemplo muestra el tráfico con destino a la dirección MAC 8A:B1:11:A0:BC:53

```
tcpdump ether dst 8A:B1:11:A0:BC:53
```

Cuando se quiere indicar una red completa, se añade al parámetro src o dst la opción net. Por ejemplo, para capturar el tráfico con red destino 192.168.43.0/24, se escribiría

```
tcpdump dst net 192.168.43.0 mask 255.255.255.0
```

O también

```
tcpdump dst net 192.168.43.0/24
```

Para mostrar el contenido del paquete usando caracteres ASCII, se utiliza el parámetro -A. Así, el comando

```
tcpdump -i eth1 -A src 192.168.1.43 and tcp 80 or dst  
192.168.43.143 and tcp 80
```

mostraría la información usando caracteres ASCII. Este comando enseñaría el tráfico que escucha la interfaz de red eth1 que viene de la máquina 192.168.1.43 por el puerto tcp 80 y va a la máquina 192.168.43.143 por el puerto 80.

La opción -XX muestra la información en hexadecimal. Por ejemplo,

```
tcpdump -i eth0 -XX src 192.168.43.143 or dst 192.168.1.43
```

muestra los paquetes capturados por la interfaz eth0 en notación hexadecimal que van a la máquina con IP 192.168.1.43 o que vienen de la máquina con IP 192.168.43.143.

Cuando se quiere capturar todo el tráfico, exceptuando alguna condición, se usa el operador not. Por ejemplo, si se quisiera capturar todo el tráfico que viene de la máquina 192.168.1.143, pero no el tráfico udp, se escribiría

```
tcpdump -i eth0 src 192.168.1.143 not udp
```

Las condiciones pueden ser anidadas usando paréntesis. Cuando se escribe una condición múltiple usando paréntesis, será necesario escribir toda la condición entre comillas simples. Por ejemplo, si se desea capturar los paquetes que vienen de la máquina 192.168.1.143 por los puertos http y https, se escribiría

```
tcpdump 'src 192.168.1.143 and (port http or https)'
```

■ 1.6. Ataques a una red. Test de intrusión

Para evaluar la fortaleza de los sistemas de seguridad, se usan herramientas para atacarlos llamadas *test de intrusión* o **pentest**, que pretenden evaluar el estado de los sistemas frente a cualquier ataque de tipo intrusivo.

Estos servicios, conocidos como **servicios de hacking ético**, dan los mismos pasos que un atacante con malas intenciones, buscando vulnerabilidades que aprovechar y realizando ataques controlados sobre los sistemas, que se pueden llevar a cabo remotamente desde el exterior o en el interior de la propia red.

Un test de intrusión se compone de una fase de planificación en la que se define y se identifica los sistemas que auditar, una fase de desarrollo de pruebas que se hacen de forma progresiva hasta conseguir detectar una vulnerabilidad y el proceso de intrusión realizado, y una fase de redacción de todos los resultados obtenidos.

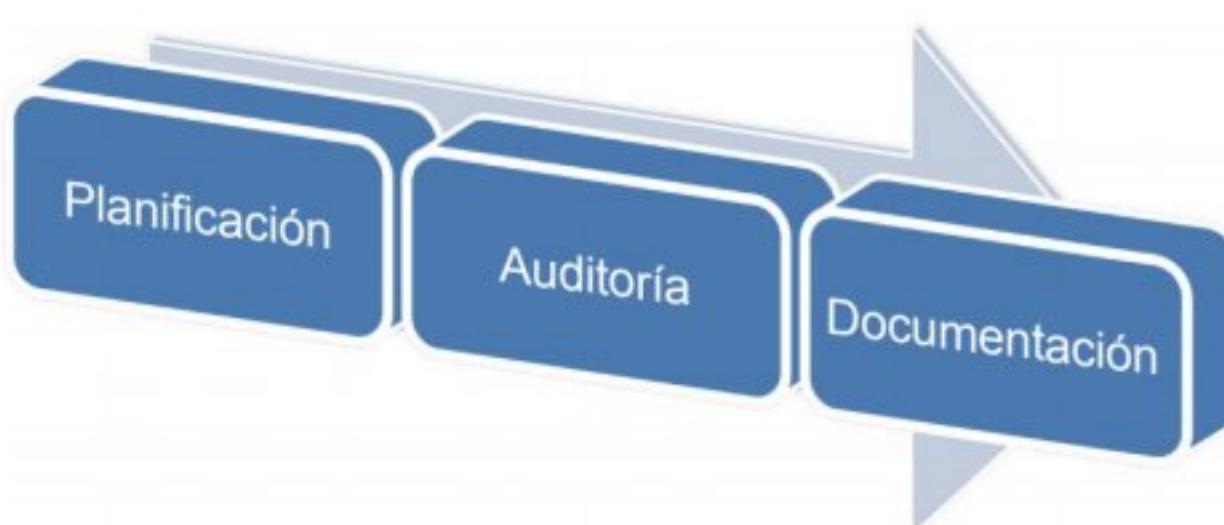


Figura 1.12. Cualquier intrusión no maliciosa, primero se planifica, luego se analiza según las políticas de seguridad y, por último, se emiten informes sobre todos los detalles técnicos de la intrusión planificada.

Para desarrollar estos ataques, se realizan técnicas y se usan herramientas propias del hacking.

Este proceso pasa por las siguientes fases:

- **Análisis de la información pública:** se debe tener un buen conocimiento sobre los sistemas objetivo. Hay que conocer las herramientas para la obtención de la máxima información sobre webs corporativas, metadatos, redes sociales, ofertas de trabajo, listas negras, foros y webs externas.
- **Análisis de seguridad de red:** se recolecta información y políticas de control. Se obtiene la máxima información posible sobre el hardware del que dispone la red y el software explotado en la misma: sondeo de red, mapa de red, escaneo de puertos, identificación de servicios y de los sistemas operativos desplegados.
- **Análisis de seguridad de sistemas:** se buscan vulnerabilidades haciendo un análisis exhaustivo de las actualizaciones y sus configuraciones, identificando las vulnerabilidades no publicadas y analizando los sistemas de autenticación.
- **Análisis de seguridad de aplicaciones:** se estudian las aplicaciones accesibles desde internet buscando mecanismos para comprometer la seguridad de las aplicaciones. Para ello, se hace un inventario de todas las afectadas sin disponer de información sobre credenciales de autenticación ni el código fuente de las mismas. Luego, se lleva a cabo un análisis de la configuración, de los sistemas de autenticación, de los esquemas de autorización, de la gestión de sesiones y de los mecanismos de validación de los datos.
- **Análisis de los sistemas de seguridad:** se analizan dispositivos y herramientas que no están bien configurados y monitorizados: cortafuegos, sistemas de detección/protección de intrusos, software antivirus y antimalware.

■ ■ 1.6.1. Búsqueda de información pública

El proceso de recogida de información en internet se conoce como *footprinting*. Generalmente, se buscan huellas del tipo direcciones IP, cuentas de correo de usuarios, credenciales, metadatos, etc. La huella digital, también llamada *fingerprinting*, es un mecanismo para defender los derechos de autor y combatir la copia no autorizada de contenidos, y puede ser usada en seguridad para detectar copias ilegales.

Anubis es una aplicación con un conjunto de herramientas que se usan en la etapa de footprinting y en la de fingerprinting, buscando información posible sobre el objetivo. Anubis permite realizar procesos como Google Hacking, whois, transferencias de zonas y fuzzing HTTP.

- **Google hacking:** usa operadores para filtrar información en el buscador Google.
- **Whois:** busca registros de todos los nombres de dominio registrados.
- **Transferencia de zona:** analiza ataques de transferencia de zona a los servidores de resolución de nombre de dominios (DNS).
- **Fuzzing HTTP:** localiza ficheros y zonas ocultas en un sitio web.

FOCA es otra herramienta centrada en la búsqueda de metadatos o información oculta en documentos alojados en sitios web. Se puede descargar desde <https://www.elevenpaths.com/es/labstools/foca-2/index.html>.

Actividad propuesta 1.7

Obtener información con Maltego

Maltego es una herramienta que permite recopilar información de la organización que se quiere atacar, tanto de la infraestructura como de las personas que trabajan en ella. Es de pago, pero existe una versión gratuita (Community). Hay que registrarse en su página web. Kali Linux tiene instalado este producto por defecto.

Instala la aplicación o ejecútala desde Kali y úsala para obtener información de una organización de interés.

■ ■ ■ 1.6.2. Análisis de vulnerabilidades

Las herramientas de gestión y análisis de vulnerabilidades pretenden obtener una visión de todas las partes del sistema que pueden estar afectadas por una o varias vulnerabilidades, cuyo proceso consiste en identificarlas, evaluar su impacto y corregirlas. Existen multitud de herramientas, como pueden ser **Nmap**, **Nessus** o **Qualys**.



Figura 1.13. Es imprescindible usar herramientas para la detección y corrección de las vulnerabilidades del sistema. Programas como Nessus, Qualys o Nmap sirven para afrontar los problemas que surgen de las inevitables brechas digitales.

■ ■ ■ La herramienta Nessus

Está concebida para gestionar escaneos de las vulnerabilidades independientemente del sistema operativo. Encuentra errores de configuración por falta de actualizaciones o por el propio despliegue. Puede detectar procesos web y puertos con sesiones de usuarios malintencionados.

Para configurar un escaneo, se debe añadir una plantilla base que defina los parámetros que escanear. Una vez configurados dichos parámetros, se le dará un nombre, junto a otros campos, y se ejecutará (de forma automática y periódica, o de forma manual).

Las funciones de análisis más interesantes que es capaz de realizar se muestran en la Figura 1.14.

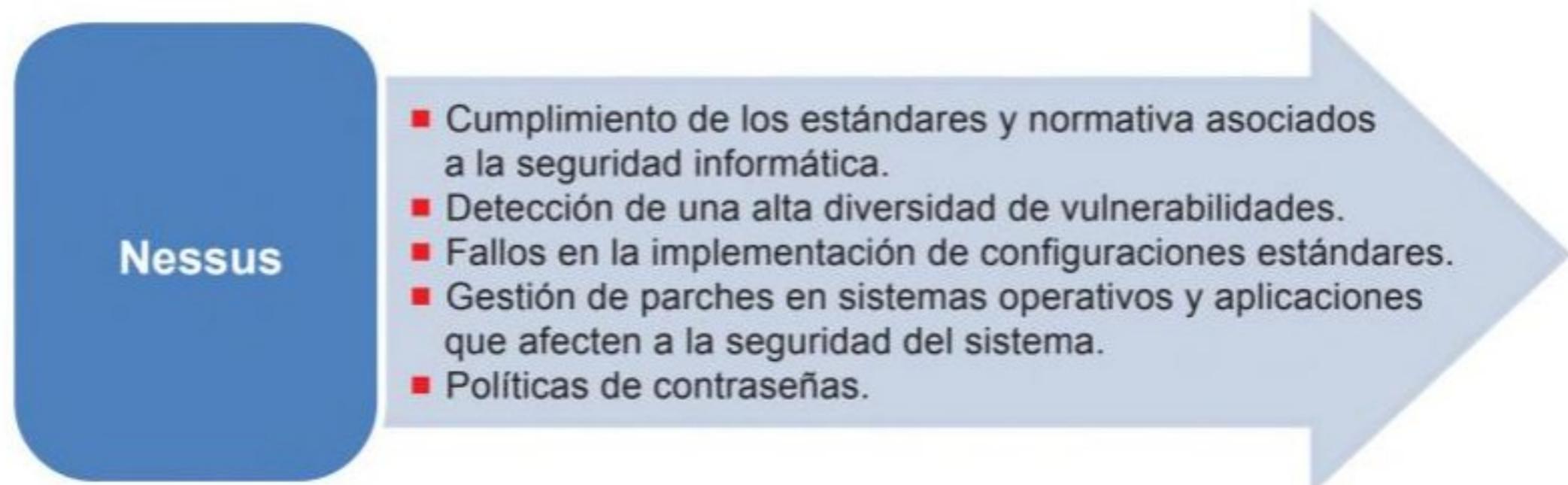


Figura 1.14. Nessus es una herramienta muy potente para el escaneo de vulnerabilidades en la mayoría de los sistemas operativos más usados. Escanea los puertos y ejecuta diversos exploits en búsqueda de penetrar la brecha localizada. Dispone de muchos plugins que le otorgan mucha potencia y escalabilidad.

Actividad propuesta 1.8

Análisis de vulnerabilidades con Nessus

Nessus es una aplicación de pago, pero tiene una versión de prueba que se puede explotar para conocer su uso y su potencia. Está disponible en www.tenable.com. Instala la aplicación e investiga sobre su explotación.

nessus Essentials	nessus Professional	tenable.io
DESCARGA GRATUITA Escanee 16 IP <ul style="list-style-type: none"> ✓ Úsalo en cualquier lugar ✓ Capacitación y orientación gratis ✓ Soporte a través de Tenable Community <p>Ideal para las siguientes personas: educadores, estudiantes e individuos que inician sus carreras en ciberseguridad. Obtenga más información sobre el uso de Essentials en el aula con el programa Tenable for Education.</p> <p>Descargar</p>	SUSCRIPCIÓN Escanee IP ilimitadas <ul style="list-style-type: none"> ✓ Evaluaciones ilimitadas ✓ Úsalo en cualquier lugar, suscripción anual ✓ Evaluación de configuración ✓ Live Results ✓ Informes configurables ✓ Soporte por correo electrónico y de la comunidad ✓ Soporte avanzado disponible con la suscripción <p>Ideal para las siguientes personas: Consultores, evaluadores de penetración y profesionales de seguridad</p> <p>Versión de prueba Más información</p>	SUSCRIPCIÓN Implemente escáneres ilimitados <ul style="list-style-type: none"> ✓ Nessus Scanners ilimitados ✓ Gestionado en la nube ✓ Incluye Priorización Predictiva ✓ Informes y tableros de control avanzados ✓ Control de acceso basado en roles ✓ Soporte avanzado ✓ Escalabilidad empresarial ✓ Precio por activo, suscripción anual <p>Ideal para: administración de vulnerabilidades en organizaciones empresariales, pequeñas y medianas</p> <p>Versión de prueba Más información</p>

Figura 1.15. Nessus es una herramienta de seguridad orientada a la detección de vulnerabilidades a través de escaneo de puertos, inyectando en aquellos abiertos diferentes scripts de ataques.

■■■ La herramienta Qualys

Se utiliza mucho. Ofrece una visión extensa de las posibles vulnerabilidades. Está basada en inventarios, lo que permite gestionar de forma cómoda todos los riesgos y las vulnerabilidades detectadas. Es una aplicación modular que ofrece diferentes grados de funcionalidad adicional. Sus funciones más destacadas se muestran en la Figura 1.16.



- Análisis altamente exhaustivo de las vulnerabilidades.
- Escaneos relacionados con normativas de seguridad.
- Análisis en aplicaciones web y componente de cortafuegos para aplicaciones web.

Figura 1.16. Proporciona seguridad en la nube y ofrece servicios relacionados con la seguridad de los sistemas. Gestiona las vulnerabilidades de los sistemas mediante técnicas SaaS (software as service).

■■■ La herramienta Nmap

Network mapper (**Nmap**) es una herramienta multiplataforma que permite realizar auditorías y seguridad en red. Rastrea y analiza en busca de sistemas para elaborar un inventario de red. La información que se puede mostrar con este comando es la siguiente: hosts activos en la red, sistema operativo que están ejecutando, puertos y servicios abiertos a través de la red, tipos de cortafuegos que se están usando, etc. La versión gráfica de Nmap se llama Zenmap.

Para instalar Nmap en Debian y Ubuntu se usaría el comando `apt-get install nmap`. Para otros, como CentOS, RHEL y Fedora, se usaría `yum install nmap`.

Si se ejecuta el comando sin parámetros, se obtendrá una ayuda sobre las diferentes opciones que se pueden usar. El formato de Nmap es

```
nmap [scan type(s)] [options] {target specification}
```

Como bien indica la ayuda, en *target specification* se pueden pasar nombres de host, direcciones IP, direcciones de red, etc. Escribiendo

```
nmap 192.168.1.43
```

se desea escanear el equipo con dirección IP 192.168.1.43. Con el siguiente comando

```
nmap 192.168.1-43.1-254
```

Se intentan escanear todos los equipos que están en el rango 192.168.1.0/24-192.168.43.0/24.

El resultado del comando muestra el sistema operativo, el filtrado, el tiempo de latencia y los puertos abiertos/cerrados y sus servicios asociados.

Si se desea excluir algún host de un rango, se usa el parámetro --exclude, por ejemplo,

```
nmap 192.168.143.0/24 --exclude 192.168.143.43, 192.168.143.44
```

También se puede utilizar el contenido de un archivo de texto. De este modo, el comando se escribe de un modo más cómodo y simplemente se debe editar el listado en el fichero plano. Para ello, se usa la opción -iL del modo

```
nmap -iL hostEscanear.txt
```

Se puede excluir el contenido de un archivo indicando --excludefile del modo

```
nmap --excludefile hostNoEscanear.txt
```

Si se desea hacer un rastreo rápido de la red, sin que se tenga que detallar para cada host toda la información, hay diferentes opciones.

Por ejemplo, se usaría la opción -sL para que no se envíe ningún paquete al host. Solo se ejecutaría un Resove DNS para localizar el nombre del host:

```
nmap -sL 192.168.143.0/24
```

Si no se quiere efectuar escaneo de puertos, se puede usar la opción -sn.

Para mostrar información extendida sobre el uso de los puertos, se usa la opción -v, de modo que el comando

```
nmap -v 192.168.1.143
```

muestra toda la información de los puertos de la máquina con IP 192.168.1.143.

Para mostrar los puertos TCP abiertos, se usa la opción -sT, y para los puertos UDP abiertos, se usa -sU.

Con el parámetro -p se puede escanear un grupo de puertos. El siguiente comando escanea los puertos bien conocidos de la máquina 192.168.1.143:

```
nmap -p 1-1024 192.168.1.143
```

Si se quiere especificar la lista de puertos, se puede indicar después del indicador U para puertos UDP y T para TCP. Los números de puertos se separan con comas sin espacio. El siguiente ejemplo escanearía los puertos TCP 21, 22, 51, 443, 80 y 8080 y los puertos UDP 22, 443 y del 1000 al 2000 de la máquina 192.168.1.143

```
nmap -p T:21,22,51,443,80,8080,U:22,443,1000-2000 192.168.1.143
```

Con el siguiente comando, se muestra información sobre el sistema operativo, puertos abiertos y otros datos de interés de la máquina local donde se ejecuta el comando:

```
nmap -v -O --osscan-guess localhost
```

Para detectar las versiones de los servicios en ejecución, se usa la opción -sV. Para mostrar una información más extensa, se usa la opción --version-all. El comando siguiente muestra información extensa de la máquina local:

```
nmap -sV --version-all localhost
```

Si existe un cortafuegos que bloquee los paquetes ICMP que usa Nmap para obtener información, se puede indicar que use otros protocolos con la opción –PS (paquete TCP Syn) o –PA (paquete TCP ACK). El siguiente comando muestra si el host está detrás de un cortafuegos:

```
nmap -sA 192.168.1.143
```

Para mostrar rutas e interfaces, se usa la opción --iflist. El siguiente comando muestra todas las interfaces de red de la máquina local y las rutas establecidas:

```
nmap --iflist localhost
```

Actividad propuesta 1.9

Zenmap, una GUI para Nmap

Instala Zenmap en tu máquina Windows. Explica la utilidad de las diferentes pestañas y cómo usar la aplicación.

1.6.3. Eliminar evidencias de un ataque

Cuando se desarrolla cualquier proceso de ataque a un sistema, se deja información almacenada en ficheros, la mayoría de ellos, ficheros de registros o ficheros log.

Los ficheros log contienen mensajes sobre cualquier evento ocurrido en el sistema, desde el núcleo del sistema operativo hasta las aplicaciones, pasando por los servicios en ejecución. Los archivos de registros son muy útiles cuando se quiere detectar y reparar algún problema ocurrido en la explotación de un servicio o un programa. Hay administradores que configuran sus máquinas para que se registren en estos ficheros cualquier cosa que ocurra, por muy insignificante que parezca.

La ventaja de tener esta información almacenada en ficheros log es obvia, no solo por su utilidad de detección y recuperación de problemas de configuración y explotación, sino también porque supone tener registrada cualquier evidencia de intrusión en una máquina de la red. En el caso de hacking no ético, no dan por finalizado el ataque hasta que se elimina cualquier huella por completo.

En los test de intrusión consentidos también se recomienda eliminar todo rastro para no confundir con cualquier delito que se cometa posteriormente al proceso de hacking ético. Se debe dejar el sistema tal como estaba, eliminando usuarios creados, procesos que han permitido accesos, eventos generados, etcétera.

A continuación, se resumen ciertas pautas que se deben llevar a cabo para eliminar cualquier evidencia de una intrusión:

- Existen servicios que pueden monitorizar las actividades llevadas a cabo en la penetración de un sistema. Se deben conocer todos estos servicios y cómo llevan a cabo la monitorización y control de accesos no autorizados.

- En caso de necesidad extrema, se podría eliminar archivos del sistema operativo que conllevarasen la imposibilidad de volver a iniciarse y, por tanto, provocarían la necesidad de reinstalación completa del sistema operativo.
- Se debería usar, siempre que se pueda, una distribución Live. Proceder de este modo evita dejar huellas en la máquina desde la que se llevó a cabo la acción intrusiva.
- Revisar información almacenada en ficheros:
 - Todos los ficheros log, así como todo lo que tenga que ver con software de gestión de eventos.
 - Los ficheros temporales que se generan cuando se lleva una acción en el sistema operativo o en cualquier aplicación.
- Eliminar cualquier huella en:
 - Los procesos de navegación en aquellos sitios web visitados en la máquina atacada.
 - El historial de comandos ejecutados a través del Shell, ya que se puede recrear los comandos usados.
 - La creación o manipulación de cuentas de usuarios, grupos, privilegios o cualquier otro objeto relacionado con la autenticación para burlar los procesos asociados.

Actividad resuelta 1.3

Análisis de inicio de sesiones con lastlog

Averigua el propósito del comando para máquinas Linux llamado `lastlog`. Indica cómo sería el comando para que muestre los inicios de sesión de los últimos cinco días del usuario APosPal.

Solución

Con el comando `lastlog` se puede conocer cuándo tuvo lugar el inicio de sesión más reciente de cada uno de los usuarios que se encuentran configurados en el fichero `/etc/passwd`. Con la opción `--user` de este comando, se puede especificar un determinado usuario en particular. Con la opción `--time`, se pueden obtener los logins ocurridos en un número de días anterior al momento que se ejecuta el comando.

De este modo, ejecutando el comando

```
lastlog --user Antonio
```

se mostrarán los logins efectuados por el usuario Antonio. Con el comando

```
lastlog --time 10
```

se obtiene información de los inicios de sesión efectuados por los usuarios los últimos diez días.

Por tanto, el comando solicitado sería

```
lastlog --user apospal --time 5
```

Actividad resuelta 1.4

Análisis de inicio de sesiones con Utmpdump

Averigua el propósito del comando para máquinas Linux `utmpdump`. Indica qué información de interés es capaz de mostrar.

Solución

La información sobre los logins se encuentra en los ficheros `/var/log/btmp` y `/var/log/wtmp`. Estos ficheros almacenan su información con formato binario, así que no es posible ver su contenido abriendolos con un editor de ficheros planos. La herramienta **Utmpdump** hace una lectura de estos ficheros y muestra información sobre diversos eventos del sistema. Estos eventos son apagado, encendido y reinicio del equipo, la dirección IP de la máquina origen, la terminal que se usó y el núcleo del sistema operativo.

■ 1.7. Kali Linux. Auditoría y seguridad informática

Kali Linux es una distribución GNU/Linux con herramientas orientadas a la auditoría y seguridad informática. Trae preinstalados más de 600 programas para escanear puertos, analizar tráfico, crackear contraseñas y administrar redes inalámbricas.

Puede ser usada en modo Live CD, live-USB, y puede ser instalada como sistema operativo principal y se distribuyen en imágenes ISO compiladas para arquitecturas de 32 y 64 bits.

La imagen se puede instalar desde un DVD o desde una distribución Live en ISO, se puede instalar desde la red y existen imágenes para la descarga de máquinas virtuales prefabricadas con las herramientas instaladas para VMWare, VirtualBOX y otros.

A continuación, se detallan las herramientas más populares de Kali Linux, clasificadas según el objetivo:

- Capturar información: Dmitry, DNSenum, Fierce, Metagoofil, Theharvester, Traceroute.
- Descubrir el objetivo: Nmap, Nping, P0f.
- Enumerar el objetivo: Amap, Nmap, Snmpwalk, Snmpcheck, SmbUser-enum, Zenmap.
- Mapear vulnerabilidades: Nessus, Nmap.
- Explotar el objetivo: Metasploit Framework, Meterpreter.
- Atacar contraseñas: THC Hydra, Tomcat.

El **Metasploit Framework** es una herramienta para programadores desarrollada en el lenguaje de programación Ruby que permite desarrollar y explotar un conjunto de comandos o fragmento de programa para aprovechar vulnerabilidades de algún sistema. Estas abarcan desde problemas en la autenticación hasta el control completo del sistema. Estos fragmentos de código se denominan **exploits**.

■ ■ ■ 1.7.1. Algunas herramientas para capturar información

El proceso de exploración con el fin de conocer lo máximo posible el objeto de ataque conlleva recopilar tanta información como sea posible. A este proceso se lo conoce como *footprinting*. Existen muchas herramientas que permiten la captura de información: Maltego, Dmitry, Dnsenum, Fierce, Metagoofil, etc. A continuación, se explican algunas de ellas.

■ ■ ■ Dmitry

Es un programa en línea de comando que permite capturar información sobre un host.

Ejemplo:

```
dmitry -e -s -w 192.168.143.43 -o /home/dmitry/resultado.txt
```

Tabla 1.1. Opciones del comando `dmitry`

-e	Realiza una búsqueda de todas las posibles direcciones de correo electrónico.
-o	Archivo donde almacenar el resultado.
-s	Busca posibles subdominios.
-w	Realiza una consulta whois a una dirección IP.

■ ■ ■ Dnsenum

Captura información sobre un dominio.

Ejemplo:

```
dnsenum --enum www.paraninfo.es
```

Tabla 1.2. Opciones para el comando `dnsenum`

--enum	Equivale a --thread 5 -s 15 -w.
--threads	Número de hilos para las consultas.
-s	Número máximo de subdominios desde Google.
-w	Realiza consultas whois en direcciones IP de clase C.

■ ■ ■ Fierce

Es un escáner para enumerar espacios IP y nombres de host no continuos dado un dominio.

Ejemplo:

```
fierce -dnsserver dns.informatica.paraninfo.es -dns paraninfo.es  
-wordlist /home/fierce/dns.txt -file /home/fierce/resultado.txt
```

Tabla 1.3. Opciones para el comando `fierce`

-dnsserver	Indica el servidor DNS para las consultas de nombre de host.
-dns	Señala el dominio por escanear.
-file	Archivo en el que se guarda la información localizada.
-wordlist	Lista de palabras para descubrir subdominios. Puede estar en un fichero.

■■■ La herramienta Metagoofil

Es una herramienta diseñada para capturar información mediante la extracción de metadatos desde documentos públicos que la organización que se va a atacar publica en internet.

Ejemplo:

```
metagoofil -d www.paraninfo.es -t pdf -l 50 -n 5 -o /home/goofil -f /home/goofil/resultados.html
```

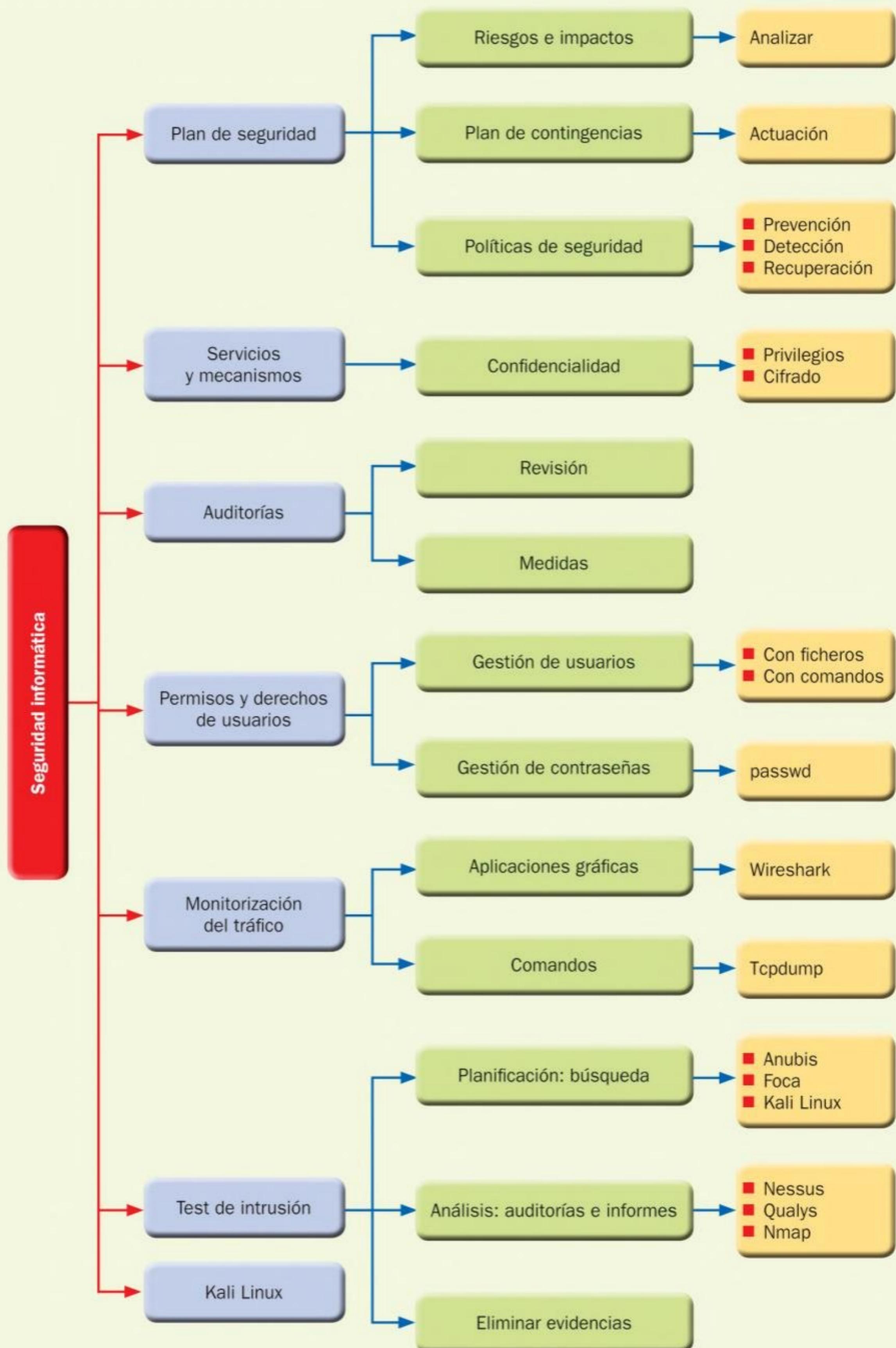
Tabla 1.4. Opciones para el comando `metagoofil`

-d	Dominio que buscar.
-f	Archivo de salida.
-l	Número de resultados de búsqueda.
-n	Número de archivos que descargar.
-o	Directorio de descarga.
-t	Tipo de archivo que descargar.

Actividad propuesta 1.10

Captura de información a través de comandos

Descarga Kali Linux y procede a su instalación. Basándote en los ejemplos que se ofrecen en la explicación de los comandos anteriores, usa los comandos `Dmitry`, `DNSenum`, `Fierce` y `Metagoofil` para capturar información sobre la red (toma como referencia los ejemplos que se ofrecen en el presente apartado).



Actividades de comprobación

- 1.1.** La consecuencia de una amenaza se denomina:
- a) Vulnerabilidad.
 - b) Impacto.
 - c) Riesgo.
 - d) Contingencia.
- 1.2.** El plan de actuación frente a cualquier amenaza se denomina:
- a) Auditoría de impactos.
 - b) Auditoría de riesgos.
 - c) Plan de seguridad informática.
 - d) Plan de contingencias.
- 1.3.** ¿Qué mecanismos se desarrollan para evitar la intrusión del sistema?
- a) Mecanismos de detección.
 - b) Mecanismos de recuperación.
 - c) Mecanismos de protección lógicos.
 - d) Ninguna de las opciones anteriores es correcta.
- 1.4.** Los pilares básicos de la seguridad son:
- a) La confidencialidad, la disponibilidad y la autenticación.
 - b) La confidencialidad, la integridad y la disponibilidad.
 - c) La integridad, la disponibilidad y la autenticación.
 - d) La confidencialidad, la disponibilidad y el no repudio.
- 1.5.** Con respecto a los permisos y derechos de usuarios:
- a) Permiten desarrollar auditorías de seguridad.
 - b) Linux no es un sistema operativo que maneje estos conceptos.
 - c) Microsoft Windows Server no maneja estos conceptos.
 - d) Solo los sistemas gestores de bases de datos manejan estos conceptos.
- 1.6.** Con respecto al fichero /etc/shadow, ¿cuál de las siguientes afirmaciones no es correcta?
- a) Contiene cada una de las contraseñas cifradas, pero pueden estar sin cifrar.
 - b) Se puede indicar el número de días sin poder cambiar la contraseña.
 - c) Se puede indicar el número de días antes del vencimiento de la contraseña.
 - d) Se puede indicar el número de días a partir de los cuales se debe cambiar la contraseña.
- 1.7.** Usando el comando `tcpdump`, ¿cuál sería el comando si se quisiera capturar el tráfico tcp por el puerto 443 que va a la máquina con IP 192.168.143.43?
- a) `tcpdump -i 192.168.143.43 and port tcp 443.`
 - b) `tcpdump net 192.168.143.0/24 and tcp 443.`
 - c) `tcpdump src 192.168.143.43 and port tcp 443.`
 - d) `tcpdump dst 192.168.143.43 and tcp port 443.`
- 1.8.** Usando el comando `nmap`, ¿cuál sería el comando si se quisieran escanear los puertos TCP 80 y 8080 y los puertos UDP 443 de la máquina 172.168.16.1?
- a) `nmap -p 80,8080,443 172.168.16.1.`
 - b) `nmap -v -T 80,8080 -U 443 172.168.16.1.`
 - c) `nmap -p T:80,8080,U:443 172.168.16.1.`
 - d) `nmap -T 80,8080 -U 443 172.168.16.1.`

- 1.9. Con respecto a las cadenas de filtrado que se usa en Wireshark:**
- a) Se usa protocolo.dstport para indicar el nombre del host.
 - b) Se usa ip.src para indicar la dirección IP de destino.
 - c) Se usa http.content_type para indicar el tipo de archivo.
 - d) Se usa protocolo.port para indicar el puerto de origen.
- 1.10. Con respecto al comando `passwd`, ¿cuál de las siguientes afirmaciones no es correcta?**
- a) Se puede indicar el número de días antes de un aviso.
 - b) Se puede indicar la duración mínima en días de la contraseña.
 - c) Se puede indicar la duración máxima de la contraseña.
 - d) Se puede cifrar la contraseña.

Actividades de aplicación

- 1.11.** ¿Cuál es la diferencia fundamental entre la seguridad física y la seguridad lógica?
- 1.12.** ¿A qué requisito corresponde la gestión de privilegios y el cifrado de la información? Justifica tu respuesta.
- 1.13.** Describe el uso del protocolo de seguridad Kerberos.
- 1.14.** Averigua qué otros programas se pueden instalar para la identificación biométrica en sistemas operativos Linux y Windows.
- 1.15.** Resume las medidas adoptadas en la seguridad física y en la seguridad lógica con el fin de compararlas entre ellas.
- 1.16.** Añade un usuario en Linux usando el fichero `/etc/passwd`, por ejemplo, Antonio:1h2o3l4a;501:101:prueba:aospal:bash. Advierte sobre el peligro de la contraseña sin cifrar.
- 1.17.** Crea una cuenta de usuario llamado JefeCompras. Este usuario debe cambiar la contraseña inmediatamente, tendrá validez 30 días y se avisará un día antes de que debe volverla a cambiar. Si no la cambia, se bloqueará la cuenta en tres días. Identifica los elementos de ACL de tipo origen más usados y confecciona un ejemplo en el que se usen.
- 1.18.** Con la herramienta Wireshark funcionando, haz un ping en la consola de comando al dominio google.com. ¿Qué información muestra Wireshark? ¿Qué se puede deducir de dicha información?
- 1.19.** Usando el comando `tcpdump`, ¿cuál sería el comando completo para capturar los paquetes en un fichero llamado `capej19.log` escuchando la tarjeta de red `eth1`, sobre los protocolos `tcp` por el puerto `80`?
- 1.20.** ¿Qué comando usarías si quisieras obtener información sobre el sistema operativo que usa, el tiempo de latencia, los puertos abiertos/cerrados y de filtrado y sus servicios asociados, de las máquinas de la red `172.16.1.64/26`, excepto las máquinas `172.16.1.65`, `172.16.1.66`, `172.16.1.67` y `172.16.1.68`?

■ Actividades de ampliación

- 1.21. Instala la herramienta Clara en tu máquina Windows. Analiza la información mostrada y confecciona un documento técnico sobre la auditoría de tu sistema.
- 1.22. Busca los sitios web de cada una de las siguientes organizaciones/entidades: Agencia Española de protección de datos (AEPD), CCN-CERT, Centro de Seguridad y Protección de Microsoft, CERT, CISECURITY, CNPIC, GDT, F-Secure, INCIBE (Instituto Nacional de Ciberseguridad), NIST, NSA y OWASP. Resume cada uno de ellos.
- 1.23. Busca en internet información sobre diferentes sistemas de monitorización de redes. Analiza sus características y determina cuáles son las especificaciones más usadas.
- 1.24. Instala la herramienta Wireshark. Conéctate a un dominio externo a la red, haz un intento de conexión a la puerta de enlace y haz un ping a la dirección IP de una máquina del segmento de red. Identifica cada uno de los paquetes de datos que se está transmitiendo y analiza los campos más importantes de cada uno de ellos.

Enlaces web de interés

■ **INCIBE** - www.incibe.es

Portal web del Instituto Nacional de Ciberseguridad. Dispone de una colección de recursos orientados a la pequeña y mediana empresa con el fin de fomentar y potenciar la protección de los sistemas y los usuarios.

■ **Microsoft Windows Hello** - www.microsoft.com/es-es/windows/windows-hello

Página web del portal de Microsoft en la que se pueden consultar todas las características de este producto.

■ **CLARA** - www.ccn-cert-cni.es/soluciones-seguridad

*Sitio web del portal del Centro Criptológico Nacional (CN-cert), en el que se pueden consultar las novedades de la herramienta **Clara**, entre otras muchas de gran interés.*

■ **LYNIS** - <https://kali-linux.net/article/lynis>

*Página web del portal Kali Linux en español en la que se puede consultar sobre el desarrollo de auditorías usando la herramienta **Lynis**. Además, es un portal con información sobre muchas de las herramientas que se pueden desplegar en el entorno Kali Linux.*

■ **WIRESHARK** - www.wireshark.org

Portal oficial del producto Wireshark. Se puede encontrar mucha información sobre el uso de esta herramienta de monitorización.

■ **TCPDUMP** - www.tcpdump.org/manpages/tcpdump.1.html

Página web en la que se incluye el manual completo, en inglés, del uso de este comando.

■ **NMAP** - <https://nmap.org>

Portal en el que se puede consultar toda la información relativa a la explotación de la herramienta Nmap.