

Tecnológico Nacional de México

Instituto Tecnológico de Reynosa



Equipo conformado por:

Bermudez Dominguez Juan Carlos 19580585  
Castillo Jr Gregorio 19580589

Flores Acosta Sheila Lizeth 19580595

Morales Calixto Daniel Alexander 19580867

Gongora Raga Perla Elizabeth 19580603

Perez Romero Julio Alberto 19580633

La seguridad informática

# Índice

[Índice 1](#_Toc135416389)

[4.1 Protocolos SNMP 2](#_Toc135416390)

[4.2 Corta fuegos físicos y lógicos 8](#_Toc135416391)

[4.3 Sniffers 18](#_Toc135416392)

[4.4 Correo no deseado 21](#_Toc135416393)

[4.5 Comprobación de integridad de archivos y directorios 27](#_Toc135416394)

[4.6 Analizador de puertos 34](#_Toc135416395)

[4.7 Monitoreo de red 37](#_Toc135416396)

[4.8 Herramientas de auditoria 42](#_Toc135416397)

[4.8.1 Prueba de penetración 42](#_Toc135416398)

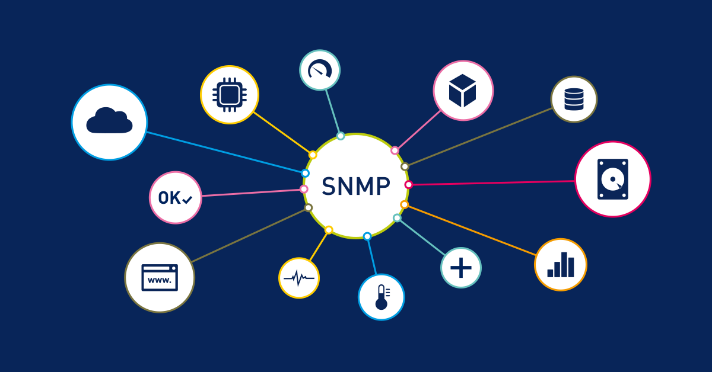
[4.8.2 Hacking ético 47](#_Toc135416399)

[4.9 Trampas y simulador de sesión 50](#_Toc135416400)

[Bibliografía 53](#_Toc135416401)

# 4.1 Protocolos SNMP

SNMP (Simple Network Management Protocol) es un conjunto de protocolos estándar utilizados para gestionar y supervisar dispositivos de red. Proporciona un mecanismo para recopilar información, configurar parámetros y controlar el rendimiento de los dispositivos de red.



Su utilidad en la gestión de redes proviene del hecho de que permite recopilar la información sobre los dispositivos conectados a la red de una forma estandarizada en una gran variedad de tipos de hardware y software.

Casi ningún administrador de red renuncia a SNMP; más bien al contrario: la mayoría confía firmemente en este protocolo porque es admitido por muchos tipos de dispositivos de múltiples fabricantes diferentes, permitiéndoles conseguir una supervisión integral gracias a la tecnología SNMP.

**Versiones**

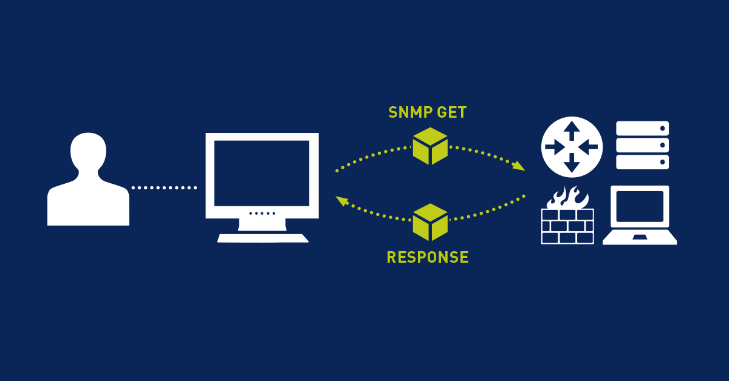
1. SNMPv1 (Simple Network Management Protocol versión 1): Es la versión original de SNMP. Proporciona capacidades básicas de gestión de redes, como la supervisión de dispositivos y la recopilación de información de rendimiento. Sin embargo, tiene limitaciones de seguridad y funcionalidad.
2. SNMPv2 (Simple Network Management Protocol versión 2): Esta versión mejoró las capacidades de SNMPv1 al introducir nuevas funciones, como la capacidad de realizar operaciones en grupos de objetos y la inclusión de notificaciones trap mejoradas. También se divide en SNMPv2c (Community-Based SNMPv2) y SNMPv2u (User-Based SNMPv2).
3. SNMPv3 (Simple Network Management Protocol versión 3): Es la versión más segura y completa de SNMP. Incluye mejoras en autenticación, cifrado y control de acceso. SNMPv3 proporciona una mayor seguridad al agregar capacidades de autenticación y privacidad a las versiones anteriores.

SNMPv3 tiene tres niveles de seguridad diferentes:

* NoAuthNoPriv: significa sin autenticación, sin privacidad. No se requiere autenticación y los mensajes no están encriptados. Por razones obvias, esto solo debe usarse en redes cerradas y seguras.
* AuthNoPriv: significa con autenticación, sin privacidad. Aunque los mensajes no están encriptados durante la transmisión, deben ser autenticados para actuar sobre ellos. Teóricamente, un actor malintencionado podría interceptar los datos enviados entre el agente y el administrador durante transmisiones autorizadas, pero no introducir solicitudes Get o Set adicionales.
* AuthPriv: significa con autenticación y con privacidad. Esta es la implementación de SNMPv3 más segura. Los mensajes SNMP deben autenticarse y todos los datos se cifran durante la transmisión. De esta forma, un actor malicioso no podría ver los datos generados por solicitudes legítimas ni enviar sus propias solicitudes Get o Set.

Normalmente, en una red suele haber, al menos, un ordenador o servidor que ejecuta un software de supervisión. Se trata de la entidad gestora. También es probable que la red tenga otros dispositivos, que podrían ser muchos o incluso muchísimos, como switches, routers, estaciones de trabajo, racks de servidores, impresoras, máquinas de café o cualquier otro dispositivo que deba ser analizado. Son los dispositivos gestionados.

Los mensajes SNMP se envían y reciben entre los administradores y los agentes. Por lo general, el administrador de SNMP de la red se instala en la entidad administradora, y los agentes SNMP, en los dispositivos administrados.



Básicamente, la transferencia de mensajes SNMP se puede comparar con la típica comunicación cliente servidor, ofreciendo tecnologías tanto de extracción (pull) como de inserción (push). La tecnología pull es el tipo de comunicación más común, en la cual un cliente, como el software de gestión de red de la entidad administradora, envía una solicitud para obtener una respuesta de un servidor o dispositivo administrado. Por el otro lado, la tecnología push permite que el dispositivo administrado “hable” y envíe un mensaje SNMP ante un evento.

En la terminología SNMP, por ejemplo, una solicitud GET de un administrador SNMP (cliente) sigue el modelo de extracción, mientras que un agente SNMP (servidor) “inserta” una trampa SNMP sin ninguna solicitud previa.

**Tipos de mensajes SNMP**

Existen diferentes tipos de mensajes SNMP que se pueden usar para configurar la supervisión de la red a través de SNMP:

* GetRequest: se trata del mensaje que envía un administrador SNMP para solicitar datos, y es el que se usa con mayor frecuencia. El dispositivo objetivo devuelve el valor solicitado con un mensaje de respuesta.
* GetNextRequest: el administrador de SNMP puede enviar este tipo de mensaje para descubrir qué información está disponible desde el dispositivo. Al comenzar en OID 0, el administrador puede continuar enviando una solicitud de los siguientes datos disponibles hasta que no haya más. De esta manera, los usuarios pueden descubrir todos los datos disponibles en un determinado dispositivo, incluso aunque no hayan tenido ningún conocimiento previo del sistema o dispositivo de respuesta.
* GetBulkRequest: aparece por primera vez en SNMP 2, y se trata de una versión más nueva y optimizada de GetNextRequest. La respuesta solicitada contendrá tantos datos como permita la solicitud. Esencialmente, es una forma de efectuar varias GetNextRequest a la vez, permitiendo a los usuarios generar una lista de todos los datos y parámetros disponibles.
* SetRequest: es un comando iniciado por el administrador para establecer o modificar el valor de un parámetro a través de SNMP en el dispositivo o sistema del agente. Este tipo de mensaje se puede usar para administrar o actualizar la configuración u otros ajustes. ¡Pero hay que tener cuidado! Un SetRequest incorrecto podría afectar seriamente a los sistemas y las configuraciones de red.
* Response: la respuesta es el mensaje que un agente de dispositivo envía tras una solicitud del administrador. Cuando se envía en respuesta a un tipo GetRequest, el paquete contiene los datos o valores solicitados. En el caso de un SetRequest, el paquete responde indicando el nuevo valor establecido a modo de confirmación de que el SetRequest se ha completado con éxito.
* Trap(v2): el agente SNMP envía (“expulsa”) una trampa sin que el administrador lo haya solicitado. De hecho, las trampas se envían bajo determinadas condiciones, como en caso de un error o al sobrepasar un umbral preestablecido. Las trampas son una excelente idea en términos de supervisión proactiva, pero si los usuarios desean beneficiarse de su uso, es posible que primero tengan que configurarlas con la ayuda del administrador de SNMP.
* InformRequest: este tipo de mensaje se agregó en SNMP v2 para dar al administrador la posibilidad de confirmar que ha recibido un mensaje de captura de un agente. Algunos agentes están configurados de modo que sigan enviando una trampa hasta recibir la confirmación de un mensaje de informe.
* Report: los mensajes Report (“informe”) necesitan SNMP v3 y permiten que un administrador de SNMP determine qué tipo de problema detectó el agente SNMP remoto. Dependiendo del error detectado, el motor de SNMP puede intentar enviar un mensaje corregido. De no ser posible, puede enviar una indicación del error a la aplicación en cuyo nombre se emitió la solicitud SNMP fallida.

**Impacto en el rendimiento**

El protocolo SNMP, puede tener un impacto dentro del rendimiento de la red. Cuando este se utiliza, los dispositivos en red realizan envío de información sobre su estado y rendimiento a servidores que gestionan la red. Estos pueden ser equipos específicos, o aplicaciones software. Pero, al fin y al cabo, esta tarea genera más tráfico adicional en la red, aumentando la carga del servidor de gestión. Afectando así al rendimiento de la red y como esta es capaz de desempeñarse dentro de la infraestructura.

En cambio, se debe destacar que el impacto de SNMP depende en gran parte de la cantidad de dispositivos que se encuentren conectados y a los cuales se les realiza la monitorización. También se debe tener en cuenta, el tipo de información que se les solicita. El conjunto de todo esto, hace que se produzca cierta variedad de tráfico, el cual puede tener este significativo impacto en el rendimiento de la red. En cambio, si estamos realizando la monitorización de un número más limitado de equipos y la información recopilada es muy básica, lo más probable es que no notemos que afecte en nada al rendimiento de la red.

En todo caso, hoy en día existen diferentes técnicas para tratar de minimizar el impacto del SNMP en el rendimiento. Una de ellas es la limitación de la cantidad de información que se recopila de los dispositivos, lo cual reduce de forma considerable la carga en la red y en el servidor que se encarga de gestionar la misma. También es importante asegurarse que se utiliza la versión más reciente de este protocolo, la cual es probable que sea mucho más eficiente y segura que versiones más antiguas.

En definitiva, el SNMP sí tiene un impacto en el rendimiento. Pero depende de diferentes factores, y de cómo este se encuentra configurado dentro de la red para tratar todos los datos que recopila de los dispositivos conectados.

**Cómo se aplican los protocolos SNMP en un servidor Ubuntu**

1. Instalar el paquete SNMP: Abre una terminal en tu servidor Ubuntu y ejecuta el siguiente comando para instalar el paquete SNMP:

*sudo apt-get install snmp snmpd*

1. Configurar el archivo de configuración del agente SNMP: El archivo de configuración del agente se encuentra en /etc/snmp/snmpd.conf. Puedes editarlo usando un editor de texto como nano o vi. Por ejemplo:

*sudo nano /etc/snmp/snmpd.conf*

En este archivo, puedes definir la configuración de seguridad, las comunidades SNMP y los permisos de acceso. Por ejemplo, puedes establecer las comunidades SNMP y las restricciones de acceso permitiendo o restringiendo ciertas direcciones IP.

1. Reiniciar el servicio SNMP: Después de realizar los cambios en el archivo de configuración, reinicia el servicio SNMP para que los cambios surtan efecto. Puedes hacerlo ejecutando el siguiente comando:

*sudo service snmpd restart*

1. Verificar el funcionamiento: Puedes verificar que SNMP esté funcionando correctamente utilizando herramientas de gestión SNMP o comandos como snmpwalk para obtener información del servidor. Por ejemplo:

*snmpwalk -v2c -c comunidadSNMP direcciónIPdelServidor*

Asegúrate de reemplazar "comunidadSNMP" por la comunidad SNMP configurada y "direcciónIPdelServidor" por la dirección IP del servidor Ubuntu.

Con estos pasos, habrás configurado el servidor Ubuntu para utilizar los protocolos SNMP. Podrás utilizar un sistema de gestión de red (NMS) para supervisar y controlar el servidor, recopilando información y configurando parámetros según tus necesidades.

# 4.2 Corta fuegos físicos y lógicos

Los cortafuegos, tanto físicos como lógicos, son elementos de seguridad utilizados en redes de computadoras para protegerlas de amenazas y asegurar la integridad y confidencialidad de los datos.

**Cortafuegos físicos**

Un cortafuegos físico es un dispositivo de hardware dedicado que se coloca en la red entre la conexión externa (como el enrutador de Internet) y la red interna. Su función principal es filtrar el tráfico de red en función de reglas predefinidas para permitir o bloquear ciertos tipos de comunicaciones. Estos dispositivos inspeccionan el tráfico a nivel de paquetes y toman decisiones sobre qué paquetes se permiten o se bloquean según las reglas configuradas. Los cortafuegos físicos a menudo proporcionan una capa adicional de seguridad al bloquear el acceso no autorizado desde el exterior de la red.

**Características de los cortafuegos físicos**

1.- Hardware dedicado: Los cortafuegos físicos son dispositivos de hardware independientes diseñados específicamente para funcionar como cortafuegos. Están construidos con componentes especializados para un rendimiento óptimo y una gestión eficiente del tráfico.

2.- Ubicación en la red: Los cortafuegos físicos se colocan estratégicamente en la red, generalmente entre la conexión externa (como el enrutador de Internet) y la red interna. Esto les permite supervisar y filtrar todo el tráfico que entra y sale de la red.

3.- Filtrado de paquetes: Los cortafuegos físicos inspeccionan los paquetes de datos a nivel de red y transportes (como las capas de IP y TCP/UDP) y toman decisiones en función de reglas predefinidas. Pueden bloquear o permitir paquetes según criterios como las direcciones IP, los puertos y los protocolos.

4.- Rendimiento: Los cortafuegos físicos están diseñados para ofrecer un rendimiento rápido y eficiente, ya que su hardware está optimizado para el procesamiento de tráfico de red a gran escala. Pueden manejar altas tasas de transferencia de datos y ofrecer latencia mínima.

**Ventajas de los cortafuegos físicos**

1.- Alto rendimiento: Los cortafuegos físicos están diseñados específicamente para el procesamiento eficiente del tráfico de red. Pueden manejar grandes volúmenes de datos y ofrecer un rendimiento rápido sin afectar significativamente la velocidad de la red.

2.- Mayor seguridad: Al estar ubicados físicamente en la red, los cortafuegos físicos proporcionan una capa adicional de seguridad al bloquear el acceso no autorizado desde el exterior. Esto los hace especialmente efectivos para proteger redes empresariales y entornos de alto riesgo.

3.- Configuración simplificada: Los cortafuegos físicos suelen ser más fáciles de configurar y administrar, ya que están diseñados con una interfaz de usuario intuitiva y un conjunto limitado de opciones de configuración. Esto es especialmente útil para usuarios con menos experiencia técnica.

**Desventajas de los cortafuegos físicos**

1.- Costo: Los cortafuegos físicos suelen ser más costosos que los cortafuegos lógicos, ya que requieren la adquisición de hardware dedicado. Además, pueden requerir gastos adicionales para licencias y actualizaciones de software.

2.- Menor flexibilidad: Los cortafuegos físicos tienen una funcionalidad y configuración más limitada en comparación con los cortafuegos lógicos. Pueden carecer de algunas características avanzadas de seguridad y personalización que se encuentran en las soluciones basadas en software.

**1.- Cisco ASA (Adaptive Security Appliance)**

Es un dispositivo de seguridad de red de Cisco que ofrece funciones de cortafuegos, prevención de intrusiones, VPN (Red Privada Virtual) y filtrado de contenido. Proporciona un alto rendimiento y escalabilidad, con opciones de conectividad flexibles.

**Características del Cisco ASA**

1.- Cortafuegos de capa de aplicación: El Cisco ASA ofrece una inspección profunda a nivel de aplicación para identificar y bloquear amenazas basadas en protocolos específicos, como HTTP, FTP, SMTP, entre otros. Esto permite una seguridad más granular y precisa.

2.- Prevención de intrusiones (IPS): El ASA incorpora una funcionalidad de prevención de intrusiones, lo que significa que puede detectar y bloquear activamente actividades maliciosas o comportamientos sospechosos en la red.

3.- VPN (Red Privada Virtual): El Cisco ASA admite conexiones VPN seguras para permitir el acceso remoto a la red y establecer conexiones seguras entre sedes. Esto garantiza la confidencialidad y la integridad de los datos transmitidos a través de redes no seguras, como Internet.

4.- Filtrado de contenido: El ASA puede realizar filtrado de contenido basado en políticas para bloquear el acceso a sitios web no deseados o potencialmente peligrosos. Esto ayuda a mantener un entorno de navegación seguro y controlado.

**Ventajas del Cisco ASA**

1.- Amplia gama de características de seguridad: El Cisco ASA combina múltiples funciones de seguridad, como cortafuegos, IPS, VPN y filtrado de contenido, en un solo dispositivo. Esto simplifica la administración y ofrece una solución integral para la protección de la red.

2.- Escalabilidad y flexibilidad: El ASA está disponible en diferentes modelos y tamaños, lo que permite adaptarse a diferentes entornos y tamaños de red. Además, ofrece opciones de conectividad flexibles para adaptarse a las necesidades de la red.

3.- Gestión centralizada: Cisco ofrece herramientas de administración centralizada, como Cisco Security Manager, que permiten configurar, monitorear y administrar de manera eficiente múltiples dispositivos ASA desde una ubicación central.

**Desventajas del Cisco ASA**

1.- Costo: El Cisco ASA puede tener un costo inicial significativo, especialmente para implementaciones a gran escala. Además, puede haber costos adicionales asociados con licencias y actualizaciones de software.

2.- Curva de aprendizaje: El ASA tiene una interfaz de configuración y administración compleja, lo que puede requerir una curva de aprendizaje para los administradores de red que no están familiarizados con los dispositivos de Cisco.



**2.- Fortinet FortiGate**

Fortinet FortiGate es una solución de seguridad integral que combina un cortafuegos de alto rendimiento con características de prevención de intrusiones, antivirus, filtrado web y control de aplicaciones. A continuación, se presentan algunas características, ventajas y desventajas de Fortinet FortiGate:

**Características de Fortinet FortiGate**

1.- Cortafuegos de alto rendimiento: FortiGate ofrece un rendimiento de alto nivel con inspección de paquetes a alta velocidad y baja latencia. Esto permite proteger eficientemente las redes incluso en entornos con altos volúmenes de tráfico.

2.- Prevención de intrusiones (IPS): FortiGate incluye capacidades de prevención de intrusiones que detectan y bloquean ataques y actividades maliciosas en tiempo real. Utiliza firmas y técnicas de detección avanzadas para proteger la red contra amenazas conocidas y desconocidas.

3.-Filtrado web y control de aplicaciones: FortiGate puede filtrar y bloquear contenido web no deseado o peligroso, como sitios maliciosos o de phishing. También permite controlar y limitar el acceso a aplicaciones y servicios en línea, mejorando así la seguridad y la productividad.

4.- VPN (Red Privada Virtual): FortiGate soporta conexiones VPN seguras para permitir el acceso remoto y establecer conexiones seguras entre sedes. Esto proporciona una comunicación encriptada y protege la confidencialidad de los datos transmitidos.

**Ventajas de Fortinet FortiGate**

1.- Funcionalidad integral: FortiGate combina múltiples funciones de seguridad en un solo dispositivo, lo que facilita la administración y reduce la complejidad. Esto elimina la necesidad de implementar múltiples soluciones independientes y simplifica la gestión de la seguridad de la red.

2.- Administración centralizada: Fortinet ofrece una plataforma de administración centralizada llamada FortiManager, que permite la configuración, supervisión y administración de múltiples dispositivos FortiGate desde una ubicación central. Esto simplifica y agiliza la administración de la seguridad de la red.

3.- Actualizaciones y protección en tiempo real: Fortinet cuenta con servicios de seguridad en la nube (FortiGuard) que proporcionan actualizaciones regulares de firmas de amenazas, protección contra malware y otras actualizaciones de seguridad. Esto asegura que los dispositivos FortiGate estén actualizados y protegidos contra las últimas amenazas.

**Desventajas de Fortinet FortiGate**

1.- Curva de aprendizaje inicial: La configuración y gestión de FortiGate puede requerir una curva de aprendizaje inicial, especialmente para los administradores de red menos familiarizados con la solución. La complejidad de la interfaz puede ser un desafío para los nuevos usuarios.

2.- Costo: FortiGate puede tener un costo inicial más elevado en comparación con soluciones de cortafuegos más básicas. Además, pueden existir costos adicionales asociados con licencias, servicios de soporte y actualizaciones.



**Cortafuegos lógicos**

Un cortafuegos lógico, también conocido como cortafuegos de software, es una aplicación o conjunto de aplicaciones que se ejecutan en un servidor o dispositivo informático y actúan como una barrera de seguridad. Estos cortafuegos se basan en reglas y configuraciones de software para controlar el tráfico de red. Los cortafuegos lógicos pueden ser implementados en sistemas operativos o en software de seguridad específico y se utilizan para proteger tanto las redes locales como los sistemas individuales. Además de filtrar el tráfico de red, también pueden realizar otras funciones de seguridad, como detección de intrusiones, prevención de ataques de denegación de servicio (DoS) y encriptación de datos.

**Características cortafuegos lógicos**

1.- Software basado en sistemas: Los cortafuegos lógicos se implementan como aplicaciones o servicios que se ejecutan en sistemas operativos o dispositivos informáticos. Utilizan el poder de cómputo del sistema en el que se ejecutan.

2.- Flexibilidad y escalabilidad: Debido a su naturaleza basada en software, los cortafuegos lógicos ofrecen una mayor flexibilidad y escalabilidad. Pueden ser instalados y configurados en una amplia variedad de sistemas, desde servidores dedicados hasta computadoras personales.

3.- Funcionalidades adicionales: Además del filtrado de paquetes, los cortafuegos lógicos pueden proporcionar características de seguridad adicionales, como detección de intrusiones, prevención de ataques de denegación de servicio, inspección de contenido y encriptación de datos.

4.- Configuración y administración centralizada: Los cortafuegos lógicos se gestionan mediante una interfaz de administración centralizada. Esto permite una configuración más sencilla y una administración centralizada de las políticas de seguridad en toda la red.

**Ventajas de los cortafuegos lógicos**

1.- Flexibilidad y escalabilidad: Los cortafuegos lógicos son altamente flexibles y se pueden instalar en una variedad de sistemas, desde servidores dedicados hasta máquinas virtuales y dispositivos de usuario final. También se pueden escalar fácilmente para adaptarse a las necesidades cambiantes de la red.

2.- Funcionalidades adicionales: Los cortafuegos lógicos a menudo ofrecen características de seguridad avanzadas, como detección de intrusiones, prevención de ataques de denegación de servicio (DoS) y filtrado de contenido. Esto proporciona una protección más completa y personalizable para la red.

**Desventajas de los cortafuegos lógicos**

1.- Rendimiento limitado: A diferencia de los cortafuegos físicos, los cortafuegos lógicos dependen del poder de cómputo del sistema en el que se ejecutan. Pueden tener un rendimiento inferior en comparación con los cortafuegos físicos, especialmente en redes con un alto volumen de tráfico.

2.- Mayor complejidad de configuración: Los cortafuegos lógicos pueden requerir una configuración más compleja y una administración más detallada, especialmente en entornos de red grandes y complejos. Esto puede implicar un mayor tiempo y esfuerzo por parte de los administradores de red.

**1.- iptables**

Es una herramienta de cortafuegos basada en software para sistemas operativos Linux. Proporciona un conjunto de reglas y filtros configurables para controlar el tráfico de red. iptables es altamente personalizable y se puede integrar en scripts y configuraciones de red complejas.

**Características de iptables**:

1.- Reglas y filtros personalizables: iptables permite crear reglas y filtros personalizados para controlar el tráfico de red. Esto incluye la capacidad de permitir o bloquear conexiones basadas en direcciones IP, puertos, protocolos y otros criterios.

2.- Inspección profunda de paquetes: iptables es capaz de realizar una inspección profunda de paquetes, lo que significa que puede analizar y tomar decisiones basadas en el contenido de los paquetes de red. Esto permite una mayor granularidad en la aplicación de políticas de seguridad.

3.- Seguimiento de conexiones: iptables tiene la capacidad de rastrear el estado de las conexiones de red, lo que permite aplicar reglas específicas en función del estado de una conexión (como establecida, nueva, relacionada, etc.). Esto ayuda a garantizar que solo se permitan conexiones válidas y autorizadas.

**Ventajas de iptables**

1.- Amplia disponibilidad y compatibilidad: iptables es una herramienta ampliamente utilizada y está disponible en la mayoría de las distribuciones de Linux. Esto lo convierte en una opción popular para implementar cortafuegos en sistemas basados en Linux.

2.- Personalización y flexibilidad: iptables ofrece un alto nivel de personalización y flexibilidad. Los administradores de red pueden crear reglas específicas para adaptarse a las necesidades de seguridad de su red y ajustarlas según sea necesario.

3.- Escalabilidad: iptables puede manejar tanto redes pequeñas como grandes sin problemas. Es altamente escalable y puede adaptarse a diferentes entornos de red sin comprometer el rendimiento.

**Desventajas de iptables**

1.- Curva de aprendizaje inicial: iptables tiene una curva de aprendizaje inicial pronunciada, especialmente para aquellos que no están familiarizados con su sintaxis y configuración. Requiere conocimientos técnicos y tiempo para comprender y utilizar eficazmente todas sus características.

2.- Configuración compleja: Configurar iptables puede ser complejo, especialmente para escenarios de red más complicados. Requiere una comprensión profunda del funcionamiento de las redes y las reglas de iptables para garantizar una configuración correcta y segura.

**2.- Windows Firewall**

Es el cortafuegos incorporado en los sistemas operativos Windows. Ofrece una protección básica contra amenazas de red al filtrar el tráfico entrante y saliente. Windows Firewall se puede configurar a través del Panel de control y ofrece opciones para personalizar las reglas de filtrado.

**Características de Windows Firewall**

1.- Filtrado bidireccional: Windows Firewall puede filtrar tanto el tráfico entrante como el saliente. Esto permite controlar qué conexiones se permiten desde y hacia el equipo protegido.

2.- Reglas personalizables: Windows Firewall permite crear reglas personalizadas para definir el comportamiento del cortafuegos. Las reglas se pueden configurar en función de aplicaciones, puertos, direcciones IP y otros criterios.

3.- Perfiles de red: Windows Firewall ofrece perfiles de red para adaptar las configuraciones del cortafuegos a diferentes entornos de red, como redes domésticas, redes de trabajo y redes públicas. Esto permite ajustar la seguridad según las necesidades específicas de cada red.

**Ventajas de Windows Firewall**

1.- Integración nativa: Windows Firewall viene preinstalado en los sistemas operativos Windows, lo que significa que no se requiere una instalación adicional. Esto hace que sea fácil de utilizar y no implica costos adicionales.

2.- Configuración sencilla: Windows Firewall ofrece una interfaz de usuario intuitiva y una configuración sencilla. Permite a los usuarios configurar rápidamente las reglas de filtrado y establecer excepciones según sus necesidades.

3.- Actualizaciones automáticas: Windows Firewall se actualiza automáticamente junto con las actualizaciones regulares de seguridad de Windows. Esto garantiza que el cortafuegos esté actualizado con las últimas protecciones contra amenazas conocidas.

**Desventajas de Windows Firewall**

1.- Limitaciones de funcionalidad: Aunque Windows Firewall ofrece protección básica, puede carecer de algunas características avanzadas que se encuentran en soluciones de cortafuegos de terceros. Por ejemplo, puede tener una capacidad limitada para realizar inspección profunda de paquetes o filtrado de contenido.

2.- Complejidad en entornos empresariales: En entornos empresariales más grandes y complejos, Windows Firewall puede resultar limitado en términos de administración centralizada y capacidad de implementación a gran escala. Para estos casos, se suelen utilizar soluciones de cortafuegos empresariales más robustas.

**Pasos básicos para configurar un cortafuegos utilizando iptables en Ubuntu Server**

En Ubuntu Server, puedes configurar un cortafuegos utilizando el software iptables, que es una herramienta de filtrado de paquetes integrada en el kernel de Linux. Iptables te permite definir reglas para permitir o denegar el tráfico de red entrante y saliente en tu servidor.

1.- Accede a tu servidor Ubuntu utilizando SSH o directamente en la terminal.

2.- Verifica si iptables está instalado ejecutando el siguiente comando:



Si no está instalado, puedes instalarlo con el siguiente comando:



3.- Crea un script para configurar tus reglas de iptables. Puedes crear un archivo de script con cualquier nombre y extensión (por ejemplo, firewall.sh) utilizando tu editor de texto favorito. Asegúrate de que el archivo sea ejecutable.

4.- Define tus reglas de firewall en el script. Aquí tienes algunos ejemplos de reglas básicas:

Permitir el tráfico entrante en el puerto 80 (HTTP):



Permitir el tráfico saliente para conexiones establecidas y relacionadas:

sudo iptables -A OUTPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT

Denegar todo el tráfico entrante por defecto:



5.- Guarda y cierra el archivo de script.

6.- Ejecuta el script de iptables para aplicar tus reglas:



# 4.3 Sniffers

Los sniffers, también conocidos como analizadores de red o capturadores de paquetes, son herramientas o dispositivos utilizados para capturar y analizar el tráfico de red. Permiten observar los paquetes de datos que se transmiten a través de una red y analizar su contenido.

**Características**

1.- Captura de paquetes: Los sniffers capturan los paquetes de datos que circulan por la red, lo que les permite analizar el contenido de dichos paquetes.

2.- Análisis de protocolos: Pueden desglosar y analizar los protocolos de red utilizados, como TCP/IP, HTTP, FTP, etc.

3.- Filtrado de paquetes: Permiten aplicar filtros para capturar únicamente los paquetes de interés, como aquellos que contienen ciertos datos o que se originan o dirigen a direcciones específicas.

4.- Interfaz gráfica o de línea de comandos: Los sniffers pueden ofrecer una interfaz gráfica intuitiva o una interfaz de línea de comandos para interactuar con ellos y visualizar los resultados del análisis.

**Funcionamiento**

Los sniffers operan en el nivel de la interfaz de red del sistema operativo o a través de dispositivos especializados. Al capturar los paquetes de datos que pasan por la red, analizan los encabezados y los contenidos de los paquetes para obtener información valiosa, como direcciones IP, puertos, protocolos, datos transmitidos y más.

**Ventajas**

1.- Solución de problemas de red: Los sniffers ayudan a identificar y diagnosticar problemas en una red, como cuellos de botella, congestiones o errores de configuración.

2.- Monitoreo de red: Permiten monitorear el tráfico de la red en tiempo real, lo que es útil para detectar actividades anormales o sospechosas.

3.- Análisis de protocolos: Los sniffers pueden analizar los protocolos de red utilizados y proporcionar información detallada sobre el funcionamiento de la red.

**Desventajas**

1.- Potencial de uso malicioso: Los sniffers pueden utilizarse para interceptar información sensible, como contraseñas o datos personales, si se utilizan de manera malintencionada.

2.- Privacidad y seguridad: Al capturar el tráfico de red, los sniffers pueden plantear preocupaciones sobre la privacidad y la seguridad de los datos transmitidos.

3.- Requiere conocimientos técnicos: Utilizar eficazmente los sniffers y comprender los resultados del análisis requiere conocimientos técnicos y experiencia en redes.

4.- Wireshark: Wireshark es una herramienta de captura y análisis de paquetes de red de código abierto. Es ampliamente utilizado y está disponible para diferentes sistemas operativos.

**Algunos ejemplos de sniffers populares**

1.- tcpdump: tcpdump es una utilidad de línea de comandos disponible en sistemas operativos basados en Unix. Permite la captura y análisis de paquetes de red en tiempo real.

2.- Cain & Abel: Cain & Abel es una suite de herramientas de seguridad que incluye un sniffer de red. Además de la captura de paquetes, ofrece funciones de descifrado de contraseñas y otros ataques relacionados con la seguridad.

3.- Ettercap: Ettercap es un sniffer y un ataque de intermediario (man-in-the-middle) de código abierto. Permite la interceptación y análisis de paquetes, así como la realización de ataques como el envenenamiento de ARP.

4.- Microsoft Network Monitor: Es una herramienta de análisis de red proporcionada por Microsoft. Permite la captura y análisis de paquetes en entornos de Windows.

**Los pasos básicos para usar tcpdump**

Para utilizar un sniffer en la terminal de Ubuntu Server, puedes utilizar la herramienta tcpdump, que es ampliamente utilizada y está disponible en la mayoría de las distribuciones de Linux.

1.- Abre una terminal en tu servidor Ubuntu.

2.- Asegúrate de tener los permisos de superusuario. Puedes utilizar el comando sudo antes de cada comando de tcpdump o ejecutar sudo -i para iniciar una sesión de superusuario.

3.- Ejecuta el siguiente comando para capturar todos los paquetes en una interfaz de red específica (por ejemplo, eth0):



Esto mostrará en tiempo real todos los paquetes capturados en la interfaz eth0. Puedes reemplazar "eth0" con el nombre de la interfaz de red que deseas monitorear.

4.- También puedes aplicar filtros para capturar paquetes específicos. Por ejemplo, si solo deseas capturar paquetes con una dirección IP de origen específica, puedes utilizar el siguiente comando:



Reemplaza <dirección IP> con la dirección IP específica que deseas filtrar.

5.- Puedes guardar la captura de paquetes en un archivo para su posterior análisis. Para hacerlo, redirecciona la salida de tcpdump a un archivo. Por ejemplo:



Esto guardará la captura de paquetes en un archivo llamado "captura.pcap" en el directorio actual.

# 4.4 Correo no deseado

Llamamos correo no deseado al correo que no queremos recibir, A veces con el correo no deseado se manda malware para que se propague. En ocasiones se confunde, correo no deseado con spam, el spam es correo no deseado publicitario. Se llama spam o correo basura a los mensajes no solicitados, no deseados o de remitente desconocido y que son sumamente molestosos. El correo no deseado es cualquier comunicación que nos llega por cualquier medio no habiendo sido solicitada y que no era esperada por el usuario que la recibe.

Se usa para describir el envío de correos electrónicos masivos a destinatarios que no los solicitan y cuyas direcciones, por lo general, se consiguen a través de Internet. La palabra inglesa "spam" proviene del nombre de la carne enlatada comercializada por la empresa Hormel Foods. La asociación de esta palabra con los correos electrónicos abusivos surge de un episodio de la serio Monthy Python que se desarrolla en un restaurante cuya especialidad es Spam. Las personas que envían correos electrónicos masivos se llamas "spammers", una palabra que ahora tiene una connotación peyorativa.

¿Cómo trabajan?

Los spammers recogen direcciones de correo electrónico de Internet en foros, páginas Web, grupos de discusión, etc; gracias a programas de software llamados robots que exploran varias páginas y almacenan en una base de datos todas las direcciones de correo electrónico que aparezcan en ellos. El spammer solo tiene que iniciar una aplicación que envía el mensaje de publicidad a cada dirección de manera sucesiva.

Tomar precauciones para minimizar la cantidad de correo no deseado que recibes es importante, no sólo porque es molesto, sino también porque pone en riesgo tu computadora e incluso tu identidad electrónica.

Efectos del spam.

Los mayores incovenientes del spam:

* El espacio que ocupa en las casillas de correo de las víctimas.
* Dificultad para consultar los mensajes personales o profesionales que están mezclados con los mensajes publicitarios y el riesgo cada vez mayor de eliminar por error o no leer los mensajes importantes.
* Pérdida de tiempo en clasificar y eliminar mensajes no solicitados.
* La naturaleza violenta o insultante de los textos o imágenes que acompañan estos mensajes y que pueden resultar chocantes para los jóvenes.
* El ancho de banda que consume en la red.

Características comunes de los correos no deseados.

Las formas de correo no deseado más habituales son:

* Direcciones de correo electrónico falsas y mensajes de un destinatario no confirmado: los correos se envían desde una dirección de correo que se parece muchísimo a otra que nos puede ser conocida o de confianza. Suelen incluir enlaces donde clicar y ni que decir tiene que mejor no hacerlo.
* Phishing: algunos spammers envían mensajes fraudulentos con los que compartas datos personales (tu contraseña, tu tarjeta de crédito, etc.).
* Mensajes de premios conseguidos: muchas veces se trata de empresas que gestionan bases de datos de millones de correos que tratan de conseguir que alguien “pique” y abra su correo con cualquier oscuro fin.
* Mensajes con promesas infalibles: de tipo laboral, sexual, médicas, etc. Hacer clic en estos mensajes sólo puede traerte complicaciones.
* Mensajes de contenido personal: te ofrecen encontrar el “ligue” de tu vida, contactos etc. o te dan la enhorabuena porque has ganado un premio.

El spam también genera costos administrativos adicionales para proveedores de servicios de Internet (ISP) que se reflejan en el costo de sus suscripciones. Estos costos adicionales están relacionados principalmente con:

* La configuración de sistemas antispam.
* La concienciación de los usuarios.
* La capacitación del personal.
* El uso de recursos adicionales (servidores de filtrado, etc).

¿Cómo combatir el correo no deseado?

Los spammer generalmente usan direcciones falsas, por lo que es inútil responder; una respuesta puede mostrarle al spammer que la dirección está activa. Asímismo, cuando recibe un correo no deseado o correo basura en la parte inferior de la página hay un vínculo que pueda darle la opción de no recibir más este tipo de mensaje, de ser así, es muy probable que el vínculo brinde al spammer la posibilidad de identificar direcciones activas. Por lo que se recomienda que eliminar el mensaje.

También existen sistemas antispam basados en reglas modernas que permiten detectar y eliminar mensajes no deseados cuando sea necesario. El software antispam se divide en dos categorías:

* Sistemas antispam para clientes: utilizados por el cliente del sistema de mensajería. Estos presentan filtros de identificación que se basan en reglas predefinidas o filtros de aprendizaje.
* Sistemas antispam del servidor: pueden filtrar el correo antes de que llegue al destinatario. Este tipo de sistema es el mejor, ya que permite detectar el correo basura en el nivel más alto y evitar la congestión de las redes y las direcciones de correo.

Correo masivo de diferentes medios.

* Spam en publicaciones:

Es una técnica de correo basura relativamente nueva, surge en lugares como publicaciones de los blogs. Consiste en dejar un comentario en una entrada, que por lo general no tiene nada que ver con la misma, sino que tiene enlaces a sitios comerciales o promociona algún producto. Akismet es un complemento para WordPress que detecta automáticamente los comentarios con tendencia a ser correo masivo.

* Spam en el correo electrónico:

El correo masivo supone actualmente la mayor parte de los mensajes electrónicos intercambiados en Internet, siendo utilizado para anunciar productos y servicios de dudosa calidad. Rolex y eBay son los asuntos de los mensajes que compiten por el primer lugar en las clasificaciones de spam. Usualmente los mensajes indican como remitente del correo una dirección falsa; por esta razón, no sirve de nada contestar a los mensajes de spam, las respuestas serán recibidas por usuarios que no tienen nada que ver con ellos.

* Spam en foros:

Es cuando un usuario publica algo que no tiene nada que ver con el tema de conversación. En otros casos, un mensaje que no contribuye de ninguna forma al tema, es considerado spam. Una tercera forma de spamming en foros es cuando una persona publica repetidamente mensajes acerca de un tema en particular en una forma indeseable para la mayor parte del foro. También, cuando una persona publica mensajes únicamente con el fin de incrementar su rango, nivel o número de mensajes en el foro. Cuando un usuario publica comentarios que contienen enlaces o algún tipo de referencia hacia algún sitio web o foro similar, de igual contenido o incluso ajeno al mismo, así como cualquier otro objetivo típico de publicidad con el objetivo de atraer más usuarios al mismo.

* Spam en las redes sociales:

Nueva forma de correo basura que consiste en enviar publicidad, ofertas de empleo, publicidad directamente a los usuarios de redes sociales profesionales sin que estos lo hayan solicitado. Por ejemplo, el envío de invitaciones no solicitadas a los contactos de usuarios de Facebook; y la "respuesta automática" con publicidad que aleatoriamente se hace desde MSN Hotmail cuando alguien envía un mensaje al buzón de la corporación.

* Spam en redes de IRC:

Tan antiguo como el propio protocolo de IRC, el correo basura en redes de charlas en línea toma auge a raíz de la masificación de dicho medio de comunicación. Los mensajes no deseados en redes de IRC tienen un costo, por lo que son objetivo principal de redes de distribución de contenidos. Los mensajes más habituales suelen tener por objetivo la visita de otros canales de chat, la visita de webs y la difusión en general de contenidos de pago. Recientemente se constata la aparición de una nueva modalidad de spam que busca que el usuario perceptor de la publicidad use la telefonía móvil para contratar servicios de elevado coste.

* Spam en correo postal:

Las técnicas de bombardeo publicitario han llegado también a los medios convencionales de comunicación. La enorme bajada relativa de los costes de impresión en papel, desde unos folletos de una sola página hasta un catálogo publicitario de varias decenas ha hecho que también el envío de correo no solicitado llegue por medio de un correo postal. De forma análoga a como ocurre en los medios electrónicos, donde un usuario interesado en un producto que remite sus datos a unas empresas especializadas en el buzoneo masivo e indiscriminado de publicidad. Es habitual encontrar en el buzón postal, publicidad no solicitada introducida masivamente por empresas especializadas o por los propios distribuidores finales. Estas acceden a los buzones tanto en la vía pública, así como buzones situados en zonas privativas.

* Spam en la vía pública:

En la vía pública son también comunes las prácticas de spam, sobre todo en las ciudades, la colocación de publicidad en lugares no preparados para ello supone un grave deterioro del medio urbano: paredes, postes, vehículos son invadidos por publicidad no solicitada que no en pocos casos acaba en el suelo. Las corporaciones municipales pierden mucho dinero por estas prácticas ilegales exentas de control fiscal y además invierten grandes cantidades de dinero en la retirada y limpieza del material publicitario dispersado en el medio.

* Spam en los wikis:

En los wikis, los usuarios frecuentan a hacer spam en las discusiones de otros usuarios, blogs (tanto crearlos como comentarlos) o en comentarios en la página de discusión de un artículo. Principalmente, esto se trata de vandalismo, pero algunas veces los usuarios están pidiendo ayuda para que otro wiki progrese. La mala intención no aparece siempre, como ven, pero no deja de ser molesto para los demás.

* Spam en los chats:

En los chats de redes sociales, grupos, etc; el spam consiste en poner repetitivamente lo mismo o escribir sobre el mismo tema de forma en la cual no se puedan leer los mensajes de los otros miembros del chat, causando una montaña de mensajes del mismo remitente.

Consejos para evitar el correo no deseado.

* No compartir tu dirección con cualquiera: De la misma manera que no se dice a cualquier persona dónde vivimos, salvo a amigos, familiares y compañeros de trabajo, lo mismo ocurre con la dirección de correo electrónico. Esto significa que no deberías incluir tu dirección de correo electrónico en cualquier formulario que pasa por tu navegador web o por tu bandeja de correo. En resumen, facilitar tu correo electrónico a desconocidos puede hacer que recibas spam.
* Usar una dirección gratuita para suscripciones: Uno de los mejores métodos para evitar que ser molestado con correos electrónicos no deseados en e-mail, es crear uno específico para que todos vayan a parar allí; es decir, crear una cuenta de correo electrónico y usarla sólo para participar en todos aquellos lugares propicios a enviar SPAM como, por ejemplo, foros o sorteos.
* No abrir los correos no deseados: Viendo el asunto del mensaje o el nombre de quien lo envía basta para darse cuenta de que algo no pinta bien, por lo que es mejor no lo abrirlo ya que una de las principales fuentes de infección en ordenadores y dispositivos móviles son los correos no deseados infectados con un archivo o con un enlace que, al hacer clic, instala un programa oculto.
* No contestar a los correos no deseados: No responer a un correo no deseado. Responder a un correo no deseado simplemente confirma que la dirección de correo electrónico es válida y se está utilizando. De esta manera, los remitentes de correo electrónico no deseado pueden enviar más spam o vender a otras personas la lista que tienen
* No dar clic en "dar de baja": Es frecuente que los spammers pongan al final del correo electrónico un enlace que aparentemente sirve para no recibir más de sus correos. Ese enlace pudiera tener como propósito confirmar que el correo electrónico es real, a menos que se esté subscrito a la página que envió el correo y en ese caso sí es seguro hacer clic en dicho enlace.
* No contestar a los correos que soliciten información personal: La mayoría de las empresas legítimas no solicita información personal por correo electrónico. Si una empresa en la que se confía (por ejemplo, su administrador de tarjetas de crédito) escribe para solicitar información personal, es necesario ponerse en contacto por teléfono - NO por mensaje. Utilizar siempre un número que proporcionado por la organización. No utilizar números proporcionados en el correo electrónico. Si la solicitud es legítima, el (la) asistente puede prestar ayuda.
* No enviar mensajes de "cadenas": Los correos electrónicos de "cadenas" pueden ser rumores, o incluso un sistema de distribución de virus. Con ello, se pierde el control de quien tendrá acceso a la dirección de correo electrónico. Además, hay información de que los remitentes de spam utilizan "cadenas" para recopilar direcciones de correo electrónico.
* Utilizar activamente los filtros antispam": Cuando se recibe un correo claramente no deseado de una fuente nada fiable, se debe marcar esa dirección como tal para que el filtro antispam la tenga en el punto de mira. Así, todos sus mensajes irán a la carpeta de spam y mantendrás limpia la bandeja de entrada.

# 4.5 Comprobación de integridad de archivos y directorios

Para comprobar la integridad se puede usar una de las herramientas de seguridad útiles que enumeramos para la protección del sistema interno contra virus, rootkits, malware y detección de actividades no autorizadas es **AIDE**.

**AIDE** ( Advanced Intrusion Detection Environment ) es una herramienta de detección de intrusos de código abierto, pequeña pero potente, que utiliza reglas predefinidas para verificar la integridad de archivos y directorios en sistemas operativos tipo Unix como Linux. Es un binario estático independiente para configuraciones de monitoreo de cliente / servidor simplificadas.

Características

* Utiliza archivos de configuración de texto plano y una base de datos que lo hace fácil de usar
* Admite varios algoritmos de resumen de mensajes como, por ejemplo, md5, sha1, rmd160, tiger;
* Admite atributos de archivo comunes
* Admite potentes expresiones regulares para incluir o excluir selectivamente archivos y directorios a escanear.
* Se puede compilar con un soporte excepcional para la compresión Gzip, Posix ACL, SELinux, XAttrs y los atributos del sistema de archivos extendido.

**Funcionamiento**

AIDE está basada en una base de datos (que es simplemente una instantánea de partes seleccionadas del sistema de archivos), a partir de las reglas de expresión regular definidas en los archivos de configuración. Una vez que esta base de datos se inicializa, puede verificar la integridad de los archivos del sistema. Esta guía mostrará cómo instalar y usar ayuda en Linux.

**Instalación**

Aide está empaquetado en repositorios oficiales de distribuciones de Linux convencionales, para instalarlo ejecute el comando para su distribución utilizando un administrador de paquetes.

# apt install aide              [On Debian/Ubuntu]

# yum install aide [On RHEL/CentOS]

# dnf install aide    [On Fedora 22+]

# zypper install aide [On openSUSE]

# emerge aide              [On Gentoo]

Después de instalarlo, el archivo de configuración principal es **/etc/aide.conf** . Para ver la versión instalada y los parámetros de tiempo de compilación, ejecute el siguiente comando en su terminal:

# aide -v

**Salida de muestra**

Aide 0.14

Compiled with the following options:

WITH\_MMAP

WITH\_POSIX\_ACL

WITH\_SELINUX

WITH\_PRELINK

WITH\_XATTR

WITH\_LSTAT64

WITH\_READDIR64

WITH\_ZLIB

WITH\_GCRYPT

WITH\_AUDIT

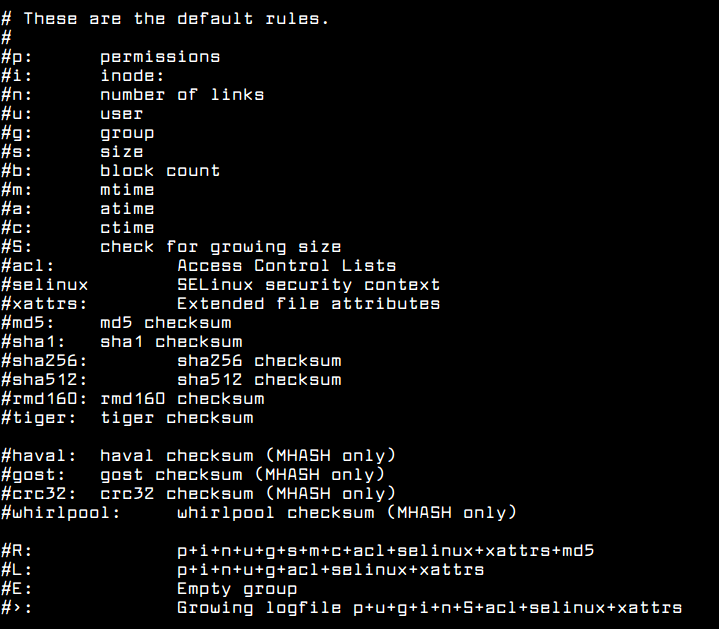
CONFIG\_FILE = "/etc/aide.conf"

Puede abrir la configuración con su editor favorito.

# vi /etc/aide.conf

Tiene directivas que definen la ubicación de la base de datos, la ubicación del informe, las reglas predeterminadas, los directorios / archivos que se incluirán en la base de datos.

**Comprender las reglas de ayuda predeterminadas**



**Reglas predeterminadas de AIDE**

Usando las reglas predeterminadas anteriores, puede definir nuevas reglas personalizadas en el archivo **aide.conf** , por ejemplo.

PERMS = p+u+g+acl+selinux+xattrs

La regla **PERMS** se usa solo para control de acceso, detectará cualquier cambio en el archivo o directorios en función de los permisos de archivo / directorio, usuario, grupo, permisos de control de acceso, contexto SELinux y atributos de archivo.

Esto solo verificará el contenido y el tipo de archivo.

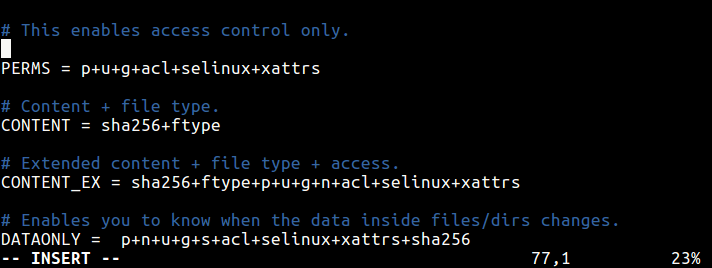
CONTENT = sha256+ftype

Esta es una versión extendida de la regla anterior, verifica el contenido extendido, el tipo de archivo y el acceso.

CONTENT\_EX = sha256+ftype+p+u+g+n+acl+selinux+xattrs

La **siguiente** regla de **DATAONLY** ayudará a detectar cualquier cambio en los datos dentro de todos los archivos / directorios.

DATAONLY =  p+n+u+g+s+acl+selinux+xattrs+sha256



**Configurar reglas de ayuda**

Definición de reglas para ver archivos y directorios

Una vez que haya definido las reglas, puede especificar el archivo y los directorios para ver. Teniendo en cuenta la regla PERMS anterior, esta definición verificará los permisos para todos los archivos en el directorio raíz.

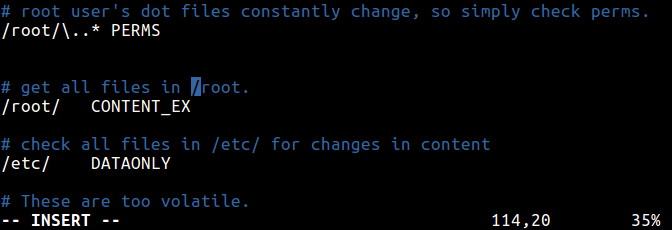
/root/\..\*  PERMS

Esto verificará todos los archivos en el directorio **/ root en** busca de cambios.

/root/   CONTENT\_EX

Para ayudarlo a detectar cualquier cambio en los datos dentro de todos los archivos / directorio bajo **/ etc /** , use esto.

/etc/   DATAONLY



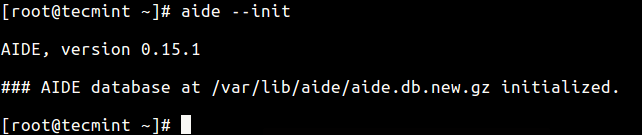
**Configurar reglas de ayuda para el sistema de archivos**

Uso de AIDE para verificar la integridad de archivos y directorios en Linux

Comience por construir una base de datos con las comprobaciones que se realizarán con el indicador --init . Se espera que esto se haga antes de que su sistema esté conectado a una red.

El siguiente comando creará una base de datos que contiene todos los archivos que seleccionó en su archivo de configuración.

# aide --init



**Inicializar base de datos de ayuda**

Luego cambie el nombre de la base de datos a **/var/lib/aide/aide.db.gz** antes de continuar, utilizando este comando.

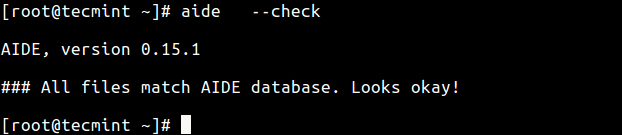
# mv /var/lib/aide/aide.db.new.gz /var/lib/aide/aide.db.gz

Se recomienda mover la base de datos a una ubicación segura, posiblemente en un medio de solo lectura o en otras máquinas, pero asegúrese de actualizar el archivo de configuración para leerlo desde allí.

Después de crear la base de datos, ahora puede verificar la integridad de los archivos y directorios utilizando el indicador --check .

# aide --check

Leerá la instantánea en la base de datos y la comparará con los archivos / directorios encontrados en el disco del sistema. Si encuentra cambios en lugares que no puede esperar, genera un informe que luego puede revisar.



**Ejecutar comprobación de integridad de archivo**

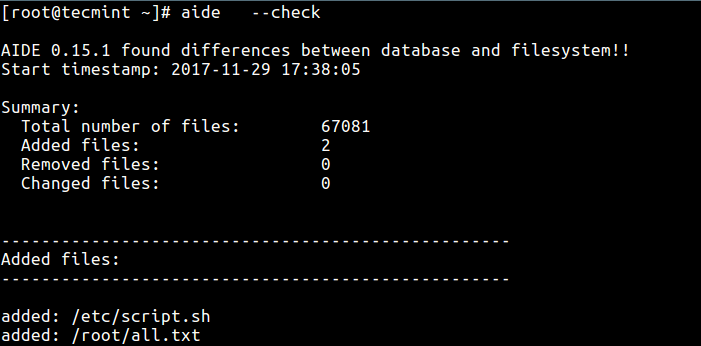
Como no se han realizado cambios en el sistema de archivos, solo obtendrá un resultado similar al anterior. Ahora intente crear algunos archivos en el sistema de archivos, en áreas definidas en el archivo de configuración.

# vi /etc/script.sh

# touch all.txt

Luego ejecute una verificación una vez más, que debe informar los archivos agregados anteriormente. El resultado de este comando depende de las partes del sistema de archivos que configuró para la verificación, puede ser un tiempo extra largo.

# aide --check



**Verificar cambios en el sistema de archivos**

Debe ejecutar verificaciones auxiliares con regularidad y, en caso de cambios en los archivos ya seleccionados o la adición de nuevas definiciones de archivo en el archivo de configuración, actualice siempre la base de datos con la opción --update :

# aide --update

Después de ejecutar una actualización de la base de datos, para usar la nueva base de datos para futuros escaneos, **cámbiele el** nombre a **/var/lib/aide/aide.db.gz** :

# mv /var/lib/aide/aide.db.new.gz  /var/lib/aide/aide.db.gz

# 4.6 Analizador de puertos

Un analizador de puertos, también conocido como escáner de puertos, es una herramienta que se utiliza para examinar los puertos abiertos en un sistema informático o en una red. Los puertos son puntos de entrada y salida que permiten la comunicación entre diferentes dispositivos y aplicaciones.

Un analizador de puertos escanea una gama de puertos en busca de aquellos que están abiertos y disponibles para la comunicación. Esto puede ayudar a identificar posibles vulnerabilidades de seguridad, ya que los puertos abiertos podrían ser utilizados por hackers o malware para acceder a la red o sistema informático.

Algunas herramientas de análisis de puertos también pueden proporcionar información adicional, como el tipo de servicio o protocolo que se está ejecutando en un puerto determinado.

Sin embargo, es importante tener en cuenta que el escaneo de puertos sin permiso previo puede ser ilegal y puede violar la privacidad de otros sistemas. Por lo tanto, es importante usar las herramientas de análisis de puertos con precaución y solo en sistemas que usted tenga permiso para examinar.

**Ventajas:**

* **Identificación de vulnerabilidades:** el análisis de puertos permite detectar puertos abiertos que pueden ser una posible vulnerabilidad en el sistema. Identificar estos puertos permite que los administradores de sistemas o los profesionales de la seguridad de la información tomen medidas para corregir los problemas de seguridad.
* Ayuda en la solución de problemas: el análisis de puertos también puede ser útil en la solución de problemas de red. Si un usuario no puede acceder a un recurso en particular, el análisis de puertos puede ayudar a identificar si el puerto necesario para acceder al recurso está bloqueado o no.
* **Identificación de servicios:** la identificación de los servicios que se ejecutan en un puerto determinado también puede ser útil para los administradores de sistemas. Saber qué servicios están en ejecución puede ayudar a administrar mejor el sistema y garantizar que los servicios necesarios estén disponibles.

**Desventajas:**

* **Vulneraciones de privacidad:** el análisis de puertos puede ser utilizado por los atacantes para identificar posibles objetivos. Si un atacante sabe qué puertos están abiertos en un sistema, puede intentar explotar las vulnerabilidades asociadas a esos puertos para obtener acceso no autorizado.
* **Sobrecarga de tráfico:** el análisis de puertos puede generar una gran cantidad de tráfico de red, lo que puede afectar el rendimiento de la red y los sistemas. Escanear demasiados puertos o escanear demasiado a menudo puede afectar negativamente a la red.
* **Falsos positivos**: el análisis de puertos puede generar falsos positivos, lo que significa que puede identificar un puerto como abierto cuando en realidad está cerrado o bloqueado por un firewall. Esto puede llevar a confusiones y pérdida de tiempo al intentar solucionar problemas inexistentes.

**Características**

* **Escaneo de puertos:** la principal característica de un analizador de puertos es su capacidad para escanear puertos en una red o sistema informático. Un analizador de puertos busca puertos abiertos y disponibles para la comunicación.
* **Identificación de servicios:** una vez que se identifican los puertos abiertos, un analizador de puertos puede determinar qué servicios están en ejecución en esos puertos. Esto ayuda a los administradores de sistemas a mantener un registro de los servicios disponibles en sus sistemas.
* **Análisis de vulnerabilidades:** algunos analizadores de puertos también pueden analizar posibles vulnerabilidades asociadas con los puertos abiertos. Esto puede ayudar a los administradores de sistemas a identificar y solucionar problemas de seguridad en sus sistemas.
* **Información detallada:** los analizadores de puertos pueden proporcionar información detallada sobre los puertos escaneados y los servicios que se ejecutan en ellos. Esta información puede incluir el nombre del servicio, el protocolo utilizado, la dirección IP del sistema, el estado del puerto (abierto o cerrado), entre otros.
* **Flexibilidad:** los analizadores de puertos pueden ser utilizados en una variedad de entornos y sistemas operativos. Algunos analizadores de puertos pueden ser instalados en un sistema local, mientras que otros pueden ser utilizados desde una ubicación remota.
* **Automatización:** algunos analizadores de puertos pueden automatizar el escaneo de puertos y la identificación de servicios en ejecución. Esto ahorra tiempo y esfuerzo para los administradores de sistemas que necesitan monitorear regularmente los puertos en sus sistemas.

Ejemplos de analizadores de puertos

|  |  |  |
| --- | --- | --- |
| **Analizador de puertos** | **Características** | **Plataformas** |
| **Nmap** | Escaneo de puertos, identificación de servicios, detección de sistemas operativos, exploración de vulnerabilidades | Linux, Windows, macOS |
| **Netstat** | Mostrar información sobre las conexiones de red activas y los puertos abiertos, información detallada sobre los puertos en uso y los servicios que se ejecutan en ellos | Linux, Windows, macOS |
| **Tcpdump** | Captura y análisis de paquetes de red, mostrar información detallada sobre los puertos utilizados | Linux, macOS |
| **Wireshark** | Captura y examen del tráfico de red, información detallada sobre los puertos utilizados, los protocolos de red y los datos transmitidos | Linux, Windows, macOS |
| **Hping** | Pruebas de penetración, escaneos de puertos TCP, UDP e ICMP, envío de paquetes personalizados y análisis de respuestas | Linux, Windows, macOS |

Es importante tener en cuenta que la elección de un analizador de puertos depende de las necesidades específicas del usuario y de las características que se buscan. Cada herramienta tiene sus propias ventajas y desventajas, y algunos pueden ser más adecuados para tareas específicas que otros.

# 4.7 Monitoreo de red

El monitoreo de red proporciona la información que los administradores de redes necesitan para determinar, en tiempo real, si una red está funcionando de manera óptima. Con herramientas como el software de monitoreo de redes, los administradores pueden identificar deficiencias y optimizar la eficiencia de manera proactiva, y más.

El objetivo principal del monitoreo de red es asegurarse de que los dispositivos de red, los servicios y las aplicaciones funcionen correctamente y estén disponibles para los usuarios.

¿Qué son los sistemas de monitoreo de red?

Los sistemas de monitoreo de red incluyen herramientas de software y hardware que pueden hacer un seguimiento de diversos aspectos de la red y su funcionamiento, como el tráfico, el uso de ancho de banda y el tiempo de actividad. Estos sistemas pueden detectar dispositivos y otros elementos que componen o tocan la red, además de proporcionar actualizaciones de estado.

Los administradores de red confían en los sistemas de monitoreo de red para detectar rápidamente las fallas de dispositivos o conexiones, o los problemas como los cuellos de botella de tráfico que limitan el flujo de datos. Estos sistemas pueden alertar a los administradores de los problemas por correo electrónico o mensaje de texto, y enviar informes mediante la analítica de red.

Los sistemas de monitoreo de red suelen incluir las siguientes características y funcionalidades:

**Descubrimiento de dispositivos:** Permiten identificar automáticamente los dispositivos conectados a la red, como routers, switches, servidores, impresoras, entre otros. Esto facilita el seguimiento y la gestión de todos los componentes de la red.

**Supervisión en tiempo real:** Monitorizan el tráfico de red en tiempo real para detectar problemas como congestión, latencia, errores de transmisión o pérdida de paquetes. Pueden utilizar protocolos como SNMP para recopilar datos de los dispositivos de red y generar alertas cuando se superan umbrales predefinidos.

**Recopilación de datos de rendimiento:** Recogen métricas y estadísticas sobre el rendimiento de los dispositivos de red, como la utilización del ancho de banda, la carga de la CPU, la memoria y el tiempo de respuesta. Estos datos se utilizan para identificar cuellos de botella, problemas de rendimiento y optimizar la configuración de la red.

**Gestión de eventos y alertas**: Detectan eventos y anomalías en la red y generan alertas para notificar a los administradores sobre posibles problemas. Estas alertas pueden enviarse por correo electrónico, mensajes de texto u otros medios de comunicación para una respuesta rápida y efectiva.

**Análisis y generación de informes:** Analizan los datos recopilados y generan informes detallados sobre el rendimiento, la disponibilidad y la seguridad de la red. Estos informes proporcionan una visión general de la salud de la red, identifican tendencias, ayudan en la toma de decisiones y respaldan el cumplimiento de los acuerdos de nivel de servicio (SLA, por sus siglas en inglés).

**Seguridad de red:** Algunos sistemas de monitoreo también incluyen funcionalidades para la detección de intrusiones, análisis de tráfico malicioso y supervisión de registros de eventos de seguridad. Estas características ayudan a identificar y mitigar amenazas y ataques a la red.

El monitoreo de red ofrece una serie de ventajas y beneficios para las organizaciones. A continuación, se mencionan algunas de las principales ventajas del monitoreo de red:

**Detección temprana de problemas:** El monitoreo de red permite detectar problemas y fallas en la red de forma temprana. Al recibir alertas y notificaciones sobre eventos anormales o umbrales superados, los administradores pueden tomar medidas inmediatas para resolver los problemas antes de que afecten significativamente el rendimiento o la disponibilidad de la red.

**Mejora del rendimiento de la red:** Al analizar y supervisar métricas de rendimiento, como la utilización del ancho de banda, los tiempos de respuesta y la carga de los dispositivos, el monitoreo de red ayuda a identificar cuellos de botella, optimizar la configuración de la red y mejorar la eficiencia general. Esto permite a los administradores tomar decisiones informadas sobre mejoras en la infraestructura o ajustes en la configuración para garantizar un rendimiento óptimo.

**Optimización de recursos:** Mediante el monitoreo de la utilización de recursos de la red, como el ancho de banda y la carga de la CPU, los administradores pueden identificar áreas de ineficiencia y optimizar el uso de los recursos disponibles. Esto puede llevar a una mejor asignación de recursos, ahorro de costos y una mayor eficiencia operativa.

**Incremento de la disponibilidad y reducción del tiempo de inactividad:** Al supervisar constantemente la disponibilidad de los dispositivos y servicios de red, el monitoreo de red ayuda a identificar y solucionar problemas rápidamente, lo que permite minimizar el tiempo de inactividad no planificado. Esto contribuye a una mayor disponibilidad de la red y a una mejor experiencia del usuario.

**Mejora de la seguridad:** El monitoreo de red permite detectar y responder de manera proactiva a eventos de seguridad, como intrusiones, malware o actividades sospechosas. Al analizar el tráfico de red y los registros de eventos, los sistemas de monitoreo pueden identificar patrones de comportamiento anormales y enviar alertas para mitigar posibles amenazas de seguridad.

**Cumplimiento de SLAs:** El monitoreo de red proporciona datos y métricas objetivas sobre el rendimiento y la disponibilidad de la red, lo que facilita el cumplimiento de los acuerdos de nivel de servicio (SLAs) con los clientes internos o externos. Los informes generados por las herramientas de monitoreo pueden respaldar la documentación y evidencia necesaria para demostrar el cumplimiento de los niveles de servicio acordados.

Existen numerosas herramientas de software disponibles para el monitoreo de redes, cada una con sus propias características y enfoques. A continuación, se mencionan algunas de las herramientas de monitoreo de red más populares y ampliamente utilizadas:

**Nagios:** Es una herramienta de monitoreo de código abierto que permite supervisar la disponibilidad y el rendimiento de los dispositivos de red, servicios, servidores y aplicaciones. Nagios es altamente configurable y puede generar alertas y notificaciones cuando se detectan problemas.

**Zabbix:** Es una plataforma de monitoreo de red y gestión de eventos que proporciona una amplia gama de características, incluyendo supervisión en tiempo real, análisis de tendencias, generación de informes y capacidad de escalabilidad. Zabbix admite una variedad de protocolos y ofrece una interfaz gráfica intuitiva.

**PRTG Network Monitor:** Es una herramienta de monitoreo de red todo en uno que permite supervisar una amplia gama de elementos de red, incluyendo ancho de banda, dispositivos, aplicaciones y servicios. PRTG Network Monitor utiliza una interfaz basada en web y proporciona informes detallados y alertas personalizables.

**SolarWinds Network Performance Monitor:** Es una solución de monitoreo de red de gran alcance que ofrece supervisión en tiempo real de dispositivos, interfaces, tráfico, rendimiento y mucho más. Proporciona gráficos intuitivos, alertas configurables y capacidades de generación de informes.

**ManageEngine OpManager:** Es una herramienta de monitoreo de red que ofrece un conjunto completo de características, incluyendo supervisión de dispositivos, aplicaciones, ancho de banda y rendimiento. OpManager incluye alertas personalizables, mapas visuales de red y capacidades de generación de informes.

**Wireshark:** Es una herramienta de análisis de tráfico de red de código abierto que captura y analiza paquetes de datos en la red. Wireshark permite realizar un análisis detallado del tráfico de red para identificar problemas y diagnosticar fallas.

Hay varias herramientas de monitoreo de red gratuitas y de código abierto disponibles para Linux. A continuación, se mencionan algunas de las opciones populares:

**Nagios Core:** Es una solución de monitoreo de red de código abierto ampliamente utilizada. Proporciona capacidades de supervisión en tiempo real, alertas personalizables y una interfaz web para la configuración y visualización de resultados.

**Zabbix:** Es una plataforma de monitoreo de red y gestión de eventos que ofrece una versión gratuita y de código abierto. Zabbix permite supervisar dispositivos, servicios y aplicaciones, y proporciona alertas, informes y análisis de datos.

**Cacti:** Es una herramienta de monitoreo y gráficos de red que permite visualizar métricas de rendimiento a través de gráficos y tablas. Cacti utiliza SNMP para recopilar datos y ofrece una interfaz web para la configuración y visualización de resultados.

**LibreNMS:** Es una plataforma de monitoreo de red de código abierto que permite supervisar dispositivos, interfaces, ancho de banda, rendimiento y más. Proporciona alertas, gráficos, informes y una interfaz web intuitiva.

**Icinga:** Es una solución de monitoreo de red de código abierto que se basa en Nagios pero ofrece una interfaz mejorada y nuevas características. Icinga permite supervisar la disponibilidad y el rendimiento de los servicios y dispositivos de red, y proporciona alertas y notificaciones personalizables.

# 4.8 Herramientas de auditoria

## 4.8.1 Prueba de penetración

Una prueba de penetración (también conocida como "pen test" o prueba de intrusión) es un método de evaluación de seguridad de sistemas informáticos que se lleva a cabo para identificar y explotar vulnerabilidades en la seguridad del sistema.

El objetivo de una prueba de penetración es simular un ataque de un hacker o ciberdelincuente para evaluar la efectividad de las medidas de seguridad y para identificar debilidades en el sistema que puedan ser explotadas por personas malintencionadas.

Durante una prueba de penetración, los expertos en seguridad informática utilizan herramientas y técnicas para intentar penetrar en el sistema, realizar actividades maliciosas y, en última instancia, obtener acceso no autorizado a los datos y recursos del sistema.

El resultado de una prueba de penetración es un informe detallado que identifica las vulnerabilidades encontradas, las técnicas utilizadas para explotarlas y las recomendaciones para corregir las fallas de seguridad detectadas. Esto ayuda a las organizaciones a mejorar su seguridad informática y a protegerse contra posibles ataques.

La prueba de penetración ha evolucionado a lo largo de los años junto con el creciente uso de la tecnología y la creciente necesidad de proteger los sistemas informáticos contra los ataques de ciberdelincuentes.

La primera prueba de penetración documentada fue realizada en la década de 1960 por los ingenieros de la compañía Bell Labs. La prueba se llevó a cabo en el sistema operativo Multics para evaluar su seguridad. Desde entonces, las pruebas de penetración se han utilizado cada vez más para identificar vulnerabilidades en los sistemas informáticos y mejorar la seguridad de las organizaciones.

El aumento de los ataques informáticos en la década de 1990 llevó a un mayor enfoque en la seguridad informática y el uso de pruebas de penetración para identificar y corregir las vulnerabilidades. En la década de 2000, la creciente preocupación por la seguridad cibernética en la industria y el gobierno impulsó la demanda de pruebas de penetración y el desarrollo de mejores herramientas y técnicas para llevarlas a cabo.

Hoy en día, las pruebas de penetración son una práctica común en el campo de la seguridad informática y son utilizadas por organizaciones de todos los tamaños para proteger sus sistemas contra los ataques de ciberdelincuentes.

Los pasos de una prueba de penetración pueden variar dependiendo del alcance y la complejidad de la evaluación, pero generalmente siguen los siguientes pasos:

* Planificación: El primer paso en una prueba de penetración es la planificación. Esto incluye establecer los objetivos de la prueba, definir el alcance y determinar los sistemas que serán evaluados.
* Recopilación de información: En este paso, se recopila información sobre los sistemas que se van a evaluar. Esto incluye información sobre los sistemas operativos, aplicaciones, direcciones IP y otras características que puedan ser útiles para identificar vulnerabilidades.
* Análisis de vulnerabilidades: Una vez que se ha recopilado la información necesaria, se realiza un análisis de vulnerabilidades para identificar posibles debilidades en los sistemas. Esto se hace mediante el uso de herramientas automatizadas y técnicas de análisis manual.
* Explotación: Una vez que se han identificado las vulnerabilidades, se intenta explotarlas para obtener acceso no autorizado a los sistemas. Esto se hace mediante el uso de herramientas y técnicas de ataque que simulan los métodos que un atacante real podría utilizar.
* Informe y recomendaciones: Finalmente, se elabora un informe detallado que describe las vulnerabilidades encontradas, las técnicas utilizadas para explotarlas y las recomendaciones para corregir las fallas de seguridad detectadas. Esto ayuda a las organizaciones a mejorar su seguridad informática y a protegerse contra posibles ataques.

Es importante destacar que una prueba de penetración debe ser realizada por profesionales capacitados y con experiencia en el campo de la seguridad informática para garantizar que se sigan los estándares y prácticas adecuadas, y que se evite cualquier daño o interrupción en el sistema evaluado.

No existe una única agencia o entidad que regule las pruebas de penetración a nivel global, pero hay varios organismos y estándares que establecen las mejores prácticas y los requisitos para llevar a cabo pruebas de penetración de manera segura y efectiva. Algunas de estas organizaciones y estándares son:

* PCI Security Standards Council: Este es un organismo que establece los estándares de seguridad para la industria de pagos en línea y requiere pruebas de penetración regulares como parte del proceso de cumplimiento de PCI.
* National Institute of Standards and Technology (NIST): Esta es una agencia gubernamental de los Estados Unidos que establece los estándares para la seguridad informática y proporciona directrices para la realización de pruebas de penetración.
* ISO/IEC 27001: Este es un estándar internacional que establece los requisitos para un sistema de gestión de seguridad de la información (SGSI) y proporciona orientación sobre la realización de pruebas de penetración.
* Open Web Application Security Project (OWASP): Es una organización que proporciona recursos y herramientas para mejorar la seguridad de las aplicaciones web y que tiene un proyecto específico sobre pruebas de penetración.

Además, algunos países tienen leyes y regulaciones específicas en relación con las pruebas de penetración. Por lo tanto, es importante consultar con expertos en seguridad informática y asesores legales para garantizar que se cumplan todos los requisitos legales y normativos aplicables antes de llevar a cabo una prueba de penetración.

El salario de un profesional que se dedica a hacer pruebas de penetración (pentesting) puede variar significativamente dependiendo de varios factores, como la experiencia, la ubicación geográfica, la industria y el tamaño de la empresa para la que trabaja.

Según información de Glassdoor, el salario base promedio de un especialista en seguridad cibernética en los Estados Unidos es de alrededor de $100,000 al año, mientras que un consultor de seguridad cibernética puede ganar un promedio de $120,000 al año.

Sin embargo, algunos profesionales de seguridad cibernética especializados en pentesting pueden ganar aún más, especialmente si tienen habilidades muy específicas y avanzadas. En algunos casos, los profesionales con experiencia y habilidades especializadas pueden cobrar más de $200 por hora por realizar pruebas de pentesting.

Es importante destacar que el salario y la compensación de los profesionales de la seguridad cibernética dependen de muchos factores y puede variar significativamente de una región a otra y de una empresa a otra. Por lo tanto, es importante investigar y comparar las ofertas de trabajo y los salarios en la industria de seguridad cibernética para obtener una idea más precisa de lo que puede ganar un especialista en pentesting.

La multa por vulnerar un sistema sin permiso varía según la legislación de cada país y la gravedad del delito cometido. En general, la ley considera la vulneración de sistemas informáticos sin permiso como un delito y puede ser sancionado con multas y/o penas de prisión, dependiendo de la jurisdicción y la naturaleza del delito.

En los Estados Unidos, por ejemplo, la Ley de Fraude y Abuso Informático (CFAA) establece penas que van desde multas de hasta $250,000 y penas de prisión de hasta 5 años por la primera ofensa, y penas más severas para delitos más graves o reincidentes. Además, las empresas o individuos afectados por una vulneración de seguridad pueden presentar demandas civiles para recuperar daños y perjuicios.

En otros países, las multas y las penas pueden ser diferentes y variar según la legislación local. Por lo tanto, es importante conocer las leyes y regulaciones locales y nacionales en relación con la vulneración de sistemas informáticos sin permiso y los posibles castigos que se pueden imponer.

En cualquier caso, vulnerar un sistema sin permiso es ilegal y puede tener graves consecuencias legales, financieras y de reputación. Siempre es recomendable obtener permiso explícito y por escrito antes de llevar a cabo cualquier prueba de penetración o evaluación de seguridad informática.

## 4.8.2 Hacking ético

El hacking ético (también conocido como "pruebas de penetración" o "pen testing") es una práctica de seguridad informática en la que un profesional de seguridad informática utiliza técnicas de hacking para identificar y explotar vulnerabilidades en sistemas y aplicaciones con el objetivo de evaluar su seguridad y mejorarla.

A diferencia del hacking malicioso, que tiene como objetivo dañar o robar información, el hacking ético se lleva a cabo con el consentimiento del propietario del sistema o aplicación y se realiza para mejorar la seguridad del mismo. Los hackers éticos pueden trabajar para empresas de seguridad informática, consultoras de seguridad o incluso para la propia organización que desea evaluar la seguridad de su sistema.

El hacking ético implica la realización de pruebas de seguridad para identificar posibles vulnerabilidades, analizar los resultados y proporcionar recomendaciones para mejorar la seguridad del sistema. Estas pruebas pueden incluir técnicas como el escaneo de puertos, la identificación de vulnerabilidades de software, el uso de herramientas de explotación, la realización de pruebas de inyección de código, entre otras.

El objetivo final del hacking ético es mejorar la seguridad del sistema y garantizar que los datos de la organización estén protegidos contra posibles ataques cibernéticos.

Aunque los pasos específicos del hacking ético pueden variar según la metodología utilizada, a continuación se presentan algunos de los pasos comunes que se suelen seguir durante un proceso de pruebas de penetración:

Recopilación de información: En este paso, se recopila información sobre el sistema o aplicación objetivo, incluyendo información sobre su arquitectura, tecnologías utilizadas, permisos de acceso, entre otros.

Análisis de vulnerabilidades: En este paso, se utiliza software especializado para identificar vulnerabilidades en el sistema o aplicación objetivo. Esto puede incluir el uso de herramientas de escaneo de puertos, análisis de vulnerabilidades de software, entre otros.

Explotación de vulnerabilidades: Una vez que se han identificado las vulnerabilidades, se lleva a cabo un intento de explotación de las mismas. Esto puede implicar la realización de pruebas de inyección de código, el uso de herramientas de explotación, o la realización de ingeniería social.

Acceso y control del sistema: Si se logra explotar con éxito una vulnerabilidad, el siguiente paso es obtener acceso y control del sistema. Esto puede incluir la obtención de credenciales de inicio de sesión, la elevación de privilegios, entre otros.

Mantenimiento del acceso: Una vez que se ha obtenido acceso al sistema, el objetivo es mantener el acceso a largo plazo. Esto implica la creación de backdoors, la modificación de permisos y configuraciones, entre otros.

Informe de resultados: Por último, se elabora un informe detallado que incluye las vulnerabilidades encontradas, el grado de riesgo de cada una, las recomendaciones para solucionarlas, y cualquier otra información relevante. Este informe se presenta al propietario del sistema o aplicación para que pueda tomar medidas para corregir las vulnerabilidades identificadas.

Es importante destacar que estos pasos pueden variar dependiendo de la metodología de hacking ético utilizada, pero en general, estos son los pasos que se suelen seguir para llevar a cabo pruebas de penetración.

El hacking ético es importante por varias razones:

Mejora la seguridad: Las pruebas de penetración permiten identificar vulnerabilidades en sistemas y aplicaciones antes de que puedan ser explotadas por hackers malintencionados. Al corregir estas vulnerabilidades, se puede mejorar significativamente la seguridad del sistema.

Ahorra costos: Las pruebas de penetración son una inversión rentable ya que pueden ahorrar costos significativos al prevenir pérdidas de datos o interrupciones en el servicio que podrían tener consecuencias económicas negativas.

Cumplimiento de regulaciones: Muchas industrias están reguladas y requieren pruebas de seguridad para garantizar el cumplimiento de las normas de seguridad y privacidad de los datos. Las pruebas de penetración son una forma efectiva de cumplir con estos requisitos.

Protección de la reputación: Una brecha de seguridad puede afectar la reputación de una organización. Las pruebas de penetración pueden ayudar a prevenir estas situaciones al mejorar la seguridad de los sistemas y reducir el riesgo de violaciones de seguridad.

Mantenimiento del liderazgo del mercado: Una organización que demuestra un enfoque proactivo hacia la seguridad y la privacidad de los datos puede tener una ventaja competitiva y mantener su liderazgo en el mercado.

En resumen, el hacking ético es importante porque ayuda a proteger los sistemas y datos de las organizaciones, a reducir costos y a garantizar el cumplimiento de las regulaciones de seguridad y privacidad de los datos. Además, puede ayudar a proteger la reputación de una organización y mantener su liderazgo en el mercado.

# 4.9 Trampas y simulador de sesión

**Herramientas de phishing:** Estas herramientas se utilizan para crear sitios web falsos o enviar correos electrónicos engañosos que imitan legítimamente una página de inicio de sesión con el fin de robar credenciales de inicio de sesión. El phishing es un delito y su uso está prohibido.

**Keyloggers:** Los keyloggers son programas maliciosos que registran y guardan las pulsaciones de teclas de un usuario, lo que incluye las contraseñas y nombres de usuario utilizados durante un inicio de sesión. Su uso sin el consentimiento del propietario del dispositivo es ilegal y éticamente cuestionable.

**Ataques de fuerza bruta:** Estos ataques implican intentos repetidos y automatizados de adivinar contraseñas probando todas las posibles combinaciones hasta encontrar la correcta. Este tipo de ataque es ilegal y se considera una violación de la privacidad y la seguridad de las personas.

**Suplantación de identidad:** Consiste en hacerse pasar por otra persona o entidad para obtener acceso a información confidencial o realizar actividades maliciosas. La suplantación de identidad es una actividad ilegal y altamente irresponsable.

Las trampas y simuladores de inicio de sesión son herramientas que generalmente se utilizan con fines de seguridad, entrenamiento y pruebas en entornos controlados y éticos. A continuación, te explicaré los propósitos legítimos de estas herramientas:

**Pruebas de seguridad:** Las organizaciones y profesionales de seguridad informática pueden utilizar simuladores de inicio de sesión para evaluar la fortaleza de los sistemas de autenticación y detectar posibles vulnerabilidades. Estas pruebas ayudan a identificar y corregir debilidades en el proceso de inicio de sesión antes de que sean explotadas por atacantes reales.

**Entrenamiento y concientización:** Las trampas y simuladores de inicio de sesión pueden ser utilizados para capacitar a los usuarios en la detección de técnicas de phishing y otros ataques de suplantación de identidad. Estas herramientas les permiten experimentar y aprender cómo reconocer y evitar los intentos de engaño en un entorno seguro.

**Investigación y desarrollo:** En algunos casos, los investigadores en seguridad informática pueden utilizar simuladores de inicio de sesión para estudiar técnicas de ataque y desarrollar contramedidas eficaces. Estas actividades generalmente se llevan a cabo en entornos controlados y éticos, respetando la privacidad y los derechos de las personas.

si estás interesado en proteger tus cuentas y datos personales contra ataques de suplantación de identidad y phishing, a continuación, te proporciono algunas medidas de seguridad que puedes implementar:

**Fortalece tus contraseñas:** Utiliza contraseñas únicas y sólidas para cada una de tus cuentas. Asegúrate de que sean lo suficientemente largas y contengan una combinación de letras, números y caracteres especiales. Evita el uso de contraseñas obvias o fáciles de adivinar.

**Habilita la autenticación de dos factores (2FA):** Activa la autenticación de dos factores siempre que sea posible. Esto añade una capa adicional de seguridad al requerir un código único enviado a tu dispositivo móvil o a través de una aplicación de autenticación para completar el proceso de inicio de sesión.

**Mantén tus sistemas actualizados:** Actualiza regularmente tu sistema operativo, aplicaciones y software de seguridad con las últimas actualizaciones y parches de seguridad. Esto ayuda a cerrar posibles brechas y vulnerabilidades conocidas.

**Ten cuidado con los enlaces y archivos adjuntos:** Evita hacer clic en enlaces sospechosos o abrir archivos adjuntos no solicitados en correos electrónicos o mensajes de origen desconocido. Estos pueden contener malware o dirigirte a sitios web fraudulentos de phishing.

**Verifica la autenticidad de los sitios web:** Antes de ingresar tus credenciales de inicio de sesión, asegúrate de que el sitio web sea legítimo. Verifica la URL, busca el candado de seguridad en la barra de direcciones y evita acceder a sitios sensibles a través de enlaces no confiables.

**Utiliza soluciones de seguridad confiables:** Instala y actualiza regularmente un software antivirus y un firewall personal en tus dispositivos para detectar y bloquear posibles amenazas de seguridad.

**Mantén un alto nivel de conciencia:** Mantente informado sobre las últimas técnicas de phishing y ataques de suplantación de identidad. Capacítate y educa a ti mismo y a tus seres queridos sobre cómo identificar y evitar estas amenazas.

# Bibliografía

* Monitoreo de TI para todo tipo de sectores. (s. f.). <https://www.paessler.com/es/solutions/industry>
* Fernández, L. (2023, 10 abril). Descubre para qué sirve el protocolo SNMP y cómo puede ser peligroso. RedesZone. <https://www.redeszone.net/tutoriales/internet/protocolo-snmp-que-es/>
* Smith, M., & LeBlanc, D. (2018). Official (ISC)2 guide to the CISSP CBK. John Wiley & Sons.
* PCI Security Standards Council. (2021). PCI DSS Quick Reference Guide. Recuperado el 15 de mayo de 2023, de https://www.pcisecuritystandards.org/documents/PCI-DSS-v3\_2\_1-Quick-Reference-Guide.pdf
* NIST. (2020). Guide to Conducting Risk Assessments. Recuperado el 15 de mayo de 2023, de https://www.nist.gov/system/files/documents/itl/2020/10/22/NIST\_SP-800-30\_Risk\_Assessment\_Guide.pdf
* International Organization for Standardization. (2013). ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements. Recuperado el 15 de mayo de 2023, de https://www.iso.org/standard/54534.html
* Open Web Application Security Project. (2021). OWASP Testing Guide v4. Recuperado el 15 de mayo de 2023, de <https://owasp.org/www-project-web-security-testing-guide/v41/>
* ¿Qué es el monitoreo de red? (2022, 22 abril). Cisco. https://www.cisco.com/c/es\_mx/solutions/automation/what-is-network-monitoring.html
* OpenAI. (2023). What are network monitoring systems [Knowledge base article]. Retrieved from https://www.openai.com/
* Orovengua, J. (n.d.). Cómo verificar la integridad de archivos y directorios usando “AIDE” en Linux. LinuxParty. https://www.linuxparty.es/57-seguridad/10378-como-verificar-la-integridad-de-archivos-y-directorios-usando-aide-en-linux.html
* ManageEngine. (n.d.). Conociendo ManageEngine OpUtils | ManageEngine LATAM [Video]. https://www.manageengine.com/latam/oputils/escaner-de-puertos.html#:~:text=%C2%BFQu%C3%A9%20es%20el%20esc%C3%A1ner%20de%20puertos%3F&text=Un%20analizador%20de%20puertos%20le,transferencia%20de%20hipertexto%20(HTTP).