Redes

Manual

Vol. 5 (Fundamentos de seguridad de la red)

ALHUBO

Alejandro Huerta Bolaños

Primera Edición

2023

Índice

Tipos de amenazas

Las redes de computadoras cableadas e inalámbricas son esenciales para las actividades cotidianas. Tanto las personas como las organizaciones dependen de las computadoras y de las redes. Las intrusiones de personas no autorizadas pueden causar interrupciones costosas en la red y pérdidas de trabajo. Los ataques a una red pueden ser devastadores y pueden resultar en una pérdida de tiempo y dinero debido a daños o robo de información o activos importantes.

Los intrusos pueden obtener acceso a una red a través de vulnerabilidades de software, ataques de hardware o adivinando el nombre de usuario y la contraseña de alguien. Los intrusos que obtienen acceso modificando software o explotando vulnerabilidades de software se denominan actores de amenazas.

Una vez que el actor de la amenaza obtiene acceso a la red, pueden surgir cuatro tipos de amenazas.

Robo de información

Robo de información es entrar en una computadora para obtener información confidencial. La información se puede utilizar o vender para diversos fines. Por ejemplo: robar la información de propiedad de una organización, como datos de investigación y desarrollo.

Manipulación y pérdida de datos

Manipulación y pérdida de datos está entrando en una computadora para destruir o alterar los registros de datos. Un ejemplo de pérdida de datos es un actor de amenaza que envía un virus que formatea el disco duro de una computadora. Un ejemplo de manipulación de datos es irrumpir en un sistema de registros para cambiar información, como el precio de un artículo.

Robo de identidad

Robo de identidad es una forma de robo de información en la que se roba información personal con el fin de apoderarse de la identidad de alguien. Con esta información, un actor de amenazas puede obtener documentos legales, solicitar crédito y realizar compras en línea no autorizadas. Identificar el robo es un problema creciente que cuesta miles de millones de dólares por año.

Servicio de Disrupción

Servicio de Disrupción is preventing legitimate users from accessing services to which they are entitled. Examples: ataques de denegación de servicio (DoS) en servidores, dispositivos de red o enlaces de comunicaciones de red.

Tipos de vulnerabilidades

La vulnerabilidad es el grado de debilidad en una red o un dispositivo. Algún grado de vulnerabilidad es inherente a los enrutadores, conmutadores, equipos de escritorio, servidores e incluso dispositivos de seguridad. Por lo general, los dispositivos de red que sufren ataques son las terminales, como los servidores y las computadoras de escritorio.

Existen tres vulnerabilidades o debilidades principales: política tecnológica, de configuración y de seguridad. Las tres fuentes de vulnerabilidades pueden dejar una red o dispositivo abierto a varios ataques, incluidos ataques de código malicioso y ataques de red.

Vulnerabilidades Tecnológicas

Vulnerabilidad	Descripción
Debilidad del protocolo TCP/IP	• Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), y el Protocolo de mensajes de control de Internet (ICMP) son inherentes inseguro. • Simple Network Management Protocol (SNMP) y Simple Mail Transfer Protocolo (SMTP) están relacionados con la estructura inherentemente insegura en el que se diseñó TCP.
Debilidades de los sistemas operativos	• Cada sistema operativo tiene problemas de seguridad que deben abordarse. • UNIX, Linux, Mac OS, Mac OS X, Windows Server 2012, Windows 7, Windows 8 • Están documentados en el Equipo de respuesta ante emergencias informáticas (CERT) archivos en http://www.cert.org

Debilidad de los equipos de red	Varios tipos de equipos de red, como enrutadores, firewalls y tienen debilidades de seguridad que deben reconocerse y protegerse en contra. Sus debilidades incluyen la protección con contraseña, la falta de autenticación, protocolos de enrutamiento y agujeros de firewall.

Vulnerabilidades de configuración

Vulnerabilidad	**Descripción**
Cuentas de usuario no seguras	La información de la cuenta de usuario puede transmitirse de forma insegura a través de la , exponiendo nombres de usuario y contraseñas a actores de amenazas.
Cuentas del sistema con contraseñas fáciles de adivinar	Este problema común es el resultado de contraseñas de usuario mal creadas.
Servicios de internet mal configurados	Activar JavaScript en navegadores web permite ataques mediante JavaScript controlado por actores de amenazas al acceder a sitios que no son de confianza. Otras posibles fuentes de deficiencias incluyen una terminal mal configurada servicios, FTP o servidores web (por ejemplo, Microsoft Internet Information Servicios (IIS) y Apache HTTP Server.
Configuraciones predeterminadas no seguras dentro de productos	Muchos productos tienen configuraciones predeterminadas que crean o habilitan agujeros en de texto claro.
Equipos de red mal configurados	Las configuraciones incorrectas del equipo en sí pueden causar una seguridad significativa del switch. Por ejemplo, listas de acceso mal configuradas, protocolos de enrutamiento o Las cadenas de comunidad SNMP pueden crear o habilitar agujeros en la seguridad.

Vulnerabilidades de política

Vulnerabilidad	Descripción
Falta de políticas de seguridad por escrito	Una política de seguridad no se puede aplicar o hacer cumplir consistentemente si es no escrito.
Políticas	Las batallas políticas y las guerras territoriales pueden dificultar la implementación de una política de seguridad coherente.
Falta de continuidad de autenticación	Las contraseñas mal elegidas, fácilmente descifradas o predeterminadas pueden permitir acceso no autorizado a la red.
Controles de acceso lógico no aplicados	El monitoreo y la auditoría inadecuados permiten ataques y uso no autorizado para continuar, desperdiciando los recursos de la empresa. Esto podría dar lugar a acciones legales o terminación contra técnicos de TI, administración de TI, o incluso la empresa liderazgo que permite que estas condiciones inseguras persistan.
La instalación de software y hardware y los cambios no respetan la política	Cambios no autorizados a la topología de red o instalación de aplicación no aprobada crear o habilitar agujeros en la seguridad.
No existe plan de recuperación tras un desastre	La falta de un plan de recuperación ante desastres permite el caos, el pánico y la confusión. cuando se produce un desastre natural o un actor de amenaza ataca a la enterprise.

Seguridad física

Un área vulnerable igualmente importante de la red a considerar es la seguridad física de los dispositivos. Si los recursos de la red pueden verse comprometidos físicamente, un actor de amenazas puede negar el uso de los recursos de la red.

Las cuatro clases de amenazas físicas son las siguientes:

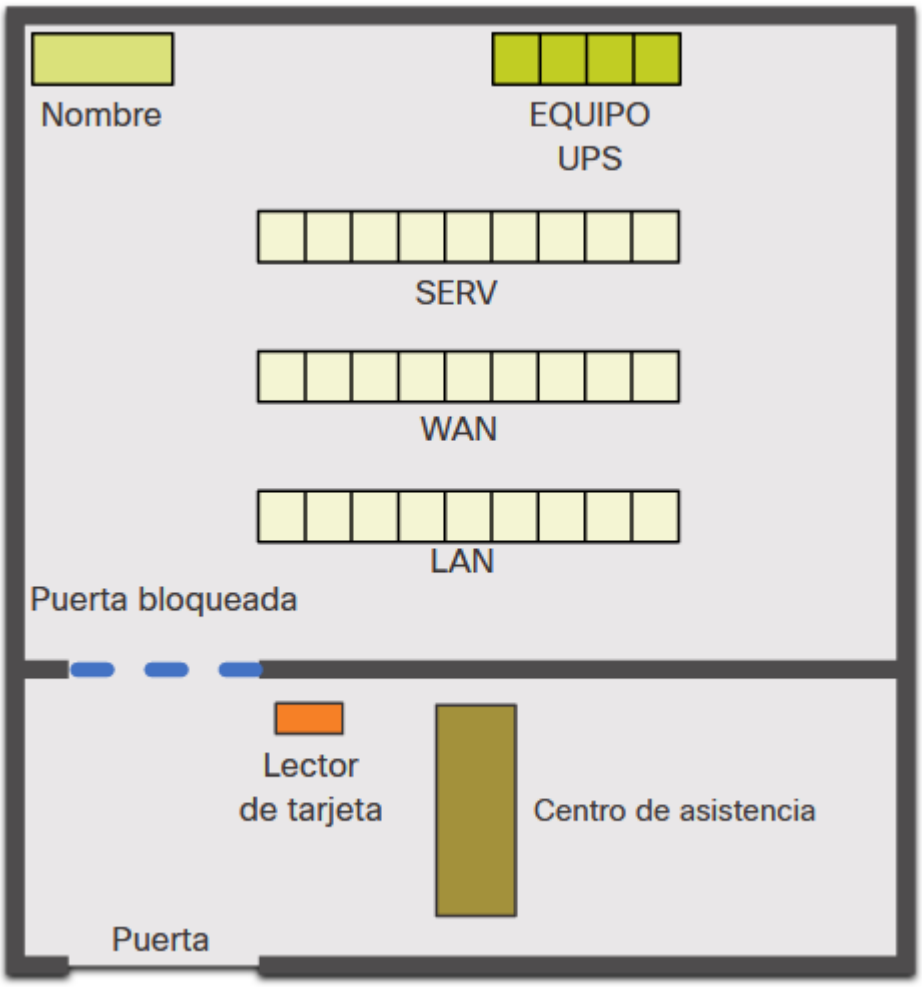
- **Amenazas de Hardware -** Esto incluye daños físicos a servidores, enrutadores, conmutadores, planta de cableado y estaciones de trabajo.

- **Amenazas del Entorno -** Esto incluye temperaturas extremas (demasiado calor o demasiado frío) o temperaturas extremas (demasiado húmedo o demasiado seco).
- **Amenazas Eléctricas -** Esto incluye picos de voltaje, voltaje de suministro insuficiente (caídas de voltaje), energía no condicionada (ruido) y pérdida total de energía.
- **Amenazas de Mantenimiento -** Esto incluye un manejo deficiente de los componentes eléctricos clave (descarga electrostática), falta de repuestos críticos, cableado deficiente y etiquetado deficiente.

Se debe crear e implementar un buen plan de seguridad física para abordar estos problemas. La figura muestra un ejemplo de plan de seguridad física.

La figura es un cuadrado que representa una sala de computadoras. Dentro de la sala de ordenadores en la esquina superior izquierda, es un pequeño rectángulo etiquetado, AC. Arriba a la derecha esquina, cuatro cuadrados están conectados y etiquetados, UPS BAY. En el centro de la hay tres filas de cuadrados, servidores etiquetados, WAN y LAN. La parte inferior de la sala de computadoras se divide para crear una habitación separada. Existe es una sección punteada del divisor etiquetada, puerta cerrada. Dentro de la es un escritorio de ayuda, un lector de tarjetas, así como otra puerta en el exterior.

Planifique la seguridad física para limitar el daño al equipo



- Sala de informática segura.
- Implemente seguridad física para limitar el daño al equipo.

Paso 1. Mantenga los equipos bajo llave y evite el acceso no autorizado por puertas, techos, pisos elevados, ventanas, canales y conductos de ventilación.

Paso 2. Controle la entrada del armario con registros electrónicos.

Paso 3. Utilice cámaras de seguridad.

Tipos de malware

En el tema anterior se explicaban los tipos de amenazas de red y las vulnerabilidades que hacen posibles las amenazas. En este tema se detalla más

detalladamente cómo los actores de amenazas obtienen acceso a la red o restringen el acceso a los usuarios autorizados.

Malware es la abreviatura de software malicioso. Es un código o software diseñado específicamente para dañar, interrumpir, robar o infligir acciones "malas" o ilegítimas en los datos, hosts o redes. Los virus, gusanos y caballos de Troya son tipos de malware.

Virus

Un virus informático es un tipo de malware que se propaga mediante la inserción de una copia de sí mismo en otro programa, del que pasa a formar parte. Se propaga de una computadora a otra, dejando infecciones a medida que viaja. La gravedad de los virus puede variar desde causar efectos ligeramente molestos hasta dañar datos o software y causar condiciones de denegación de servicio (DoS). Casi todos los virus se adjuntan a un archivo ejecutable, lo que significa que el virus puede existir en un sistema pero no estará activo ni será capaz de propagarse hasta que un usuario ejecute o abra el archivo o programa host malicioso. Cuando se ejecuta el código del host, el código viral se ejecuta también. Normalmente, el programa host sigue funcionando después de que el virus lo infecta. Sin embargo, algunos virus sobrescriben otros programas con copias de sí mismos, lo que destruye el programa host por completo. Los virus se propagan cuando el software o documento al que están adjuntos se transfiere de una computadora a otra mediante la red, un disco, el intercambio de archivos o archivos adjuntos de correo electrónico infectados.

Gusanos

Los gusanos informáticos son similares a los virus en que se replican en copias funcionales de sí mismos y pueden causar el mismo tipo de daño. A diferencia de los virus, que requieren la propagación de un archivo host infectado, los gusanos son software independiente y no requieren de un programa host ni de la ayuda humana para propagarse. Un gusano no necesita unirse a un programa para infectar un host y entrar en una computadora a través de una vulnerabilidad en el sistema. Los gusanos se aprovechan de las características del sistema para viajar a través de la red sin ayuda.

Caballos de Troya

Un caballo de Troya es otro tipo de malware que lleva el nombre del caballo de madera que los griegos utilizaron para infiltrarse en Troya. Es una pieza de software dañino que parece legítimo. Los usuarios suelen ser engañados para cargarlo y ejecutarlo en sus sistemas. Después de activarse, puede lograr cualquier número de ataques al host, desde irritar al usuario (con ventanas emergentes excesivas o cambiar el escritorio) hasta dañar el host (eliminar archivos, robar datos o activar y

difundir otro malware, como los virus). Los caballos de Troya también son conocidos por crear puertas traseras para que usuarios maliciosos puedan acceder al sistema.

A diferencia de los virus y gusanos, los caballos de Troya no se reproducen al infectar otros archivos. Se autoreplican. Los caballos de Troya deben extenderse a través de la interacción del usuario, como abrir un archivo adjunto de correo electrónico o descargar y ejecutar un archivo de Internet.

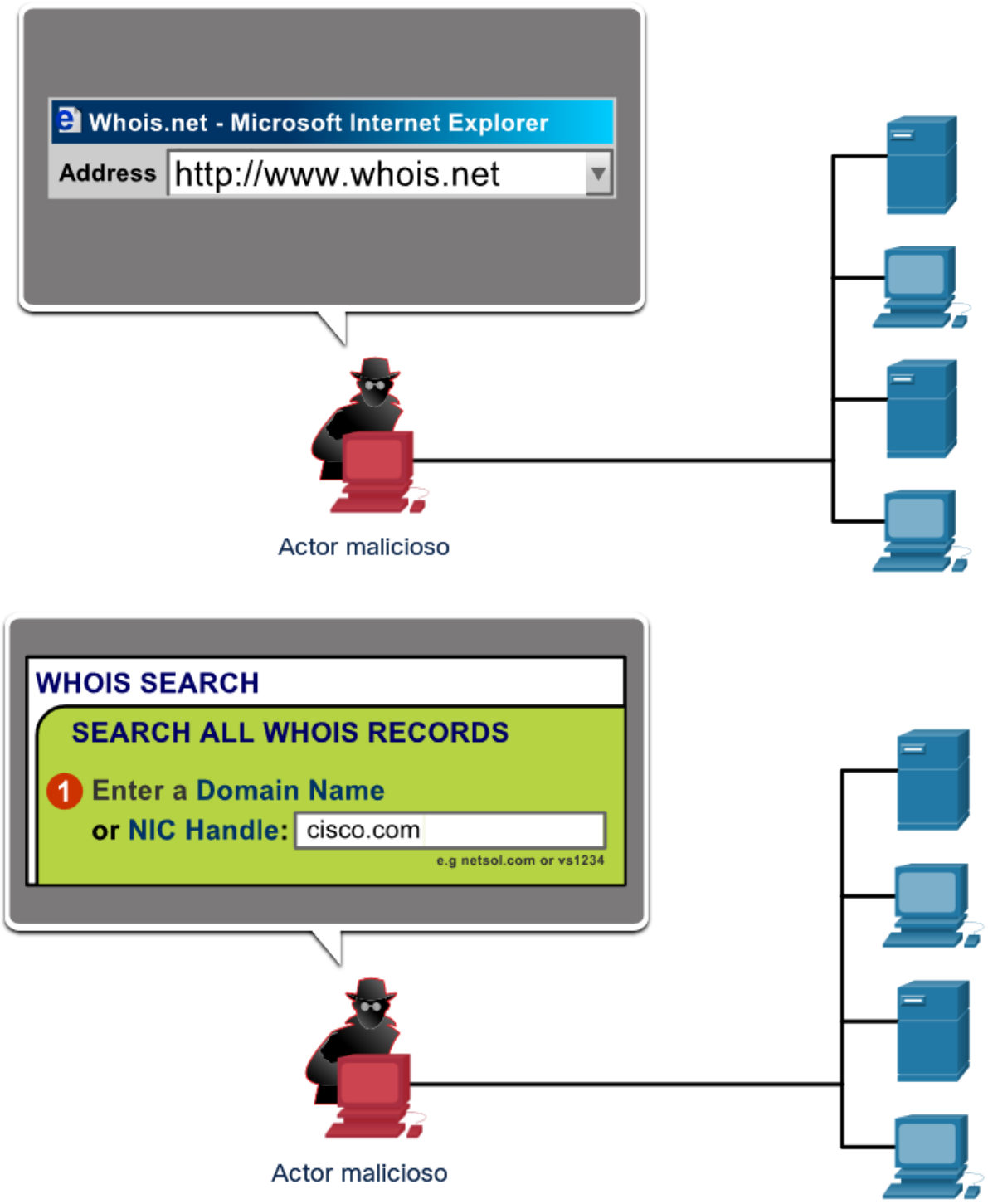
Ataques de reconocimiento

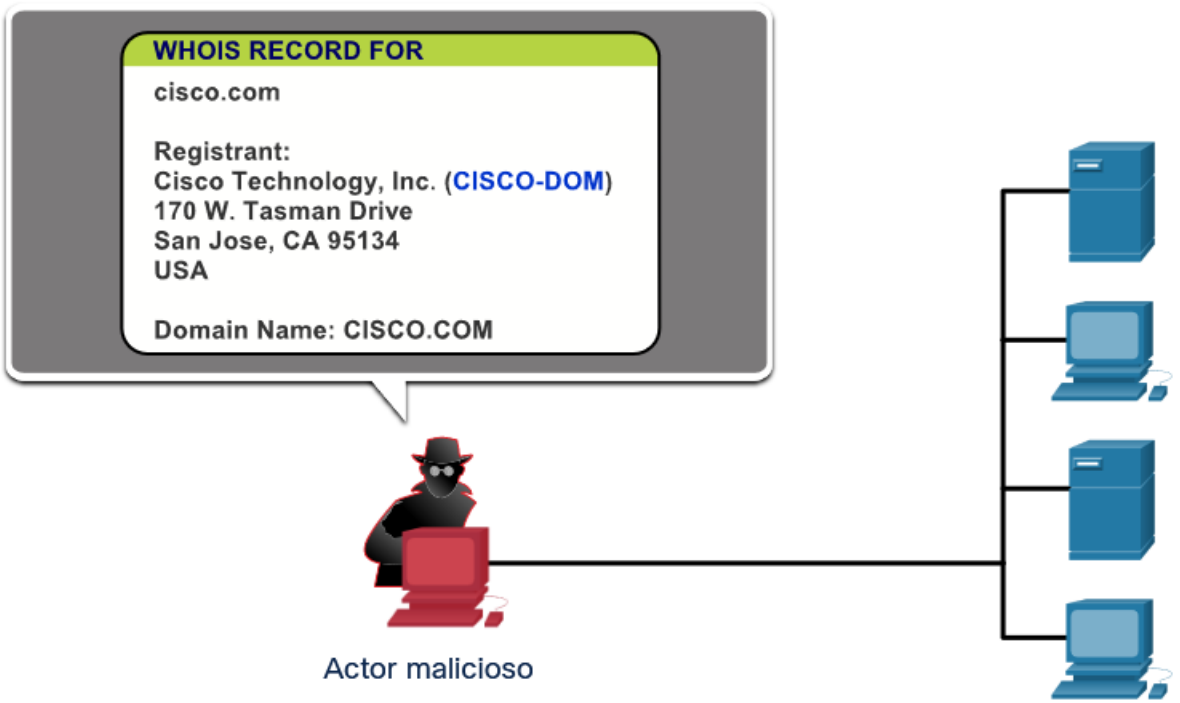
Además de los ataques de código malintencionado, es posible que las redes sean presa de diversos ataques de red. Los ataques de red pueden clasificarse en tres categorías principales:

- **Ataques de reconocimiento** - El descubrimiento y mapeo de sistemas, servicios o vulnerabilidades.
- **Ataques de acceso** - La manipulación no autorizada de datos, acceso al sistema o privilegios de usuario.
- **Denegación de servicio** - La desactivación o corrupción de redes, sistemas o servicios.

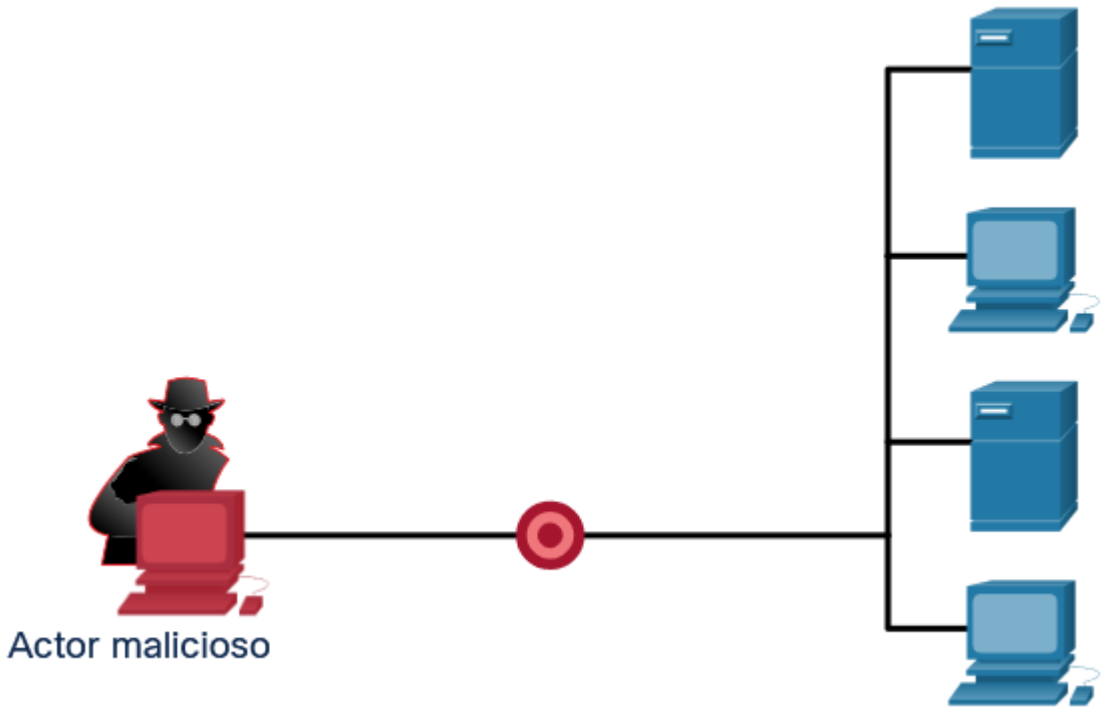
Para los ataques de reconocimiento, los actores de amenazas externas pueden usar herramientas de Internet, **nslookup** como los servicios públicos, **whois** para determinar fácilmente el espacio de direcciones IP asignado a una determinada corporación o entidad. Una vez que se determina el espacio de la dirección IP, un actor de amenazas puede hacer ping a las direcciones IP disponibles públicamente para identificar las direcciones que están activas. Para ayudar a automatizar este paso, un actor de amenazas puede usar una herramienta de barrido de ping, como **fping** o **gping**. Esto hace ping sistemáticamente a todas las direcciones de red en un rango o subred dado. Esto es similar a revisar una sección de una guía telefónica y llamar a cada número para ver quién atiende.

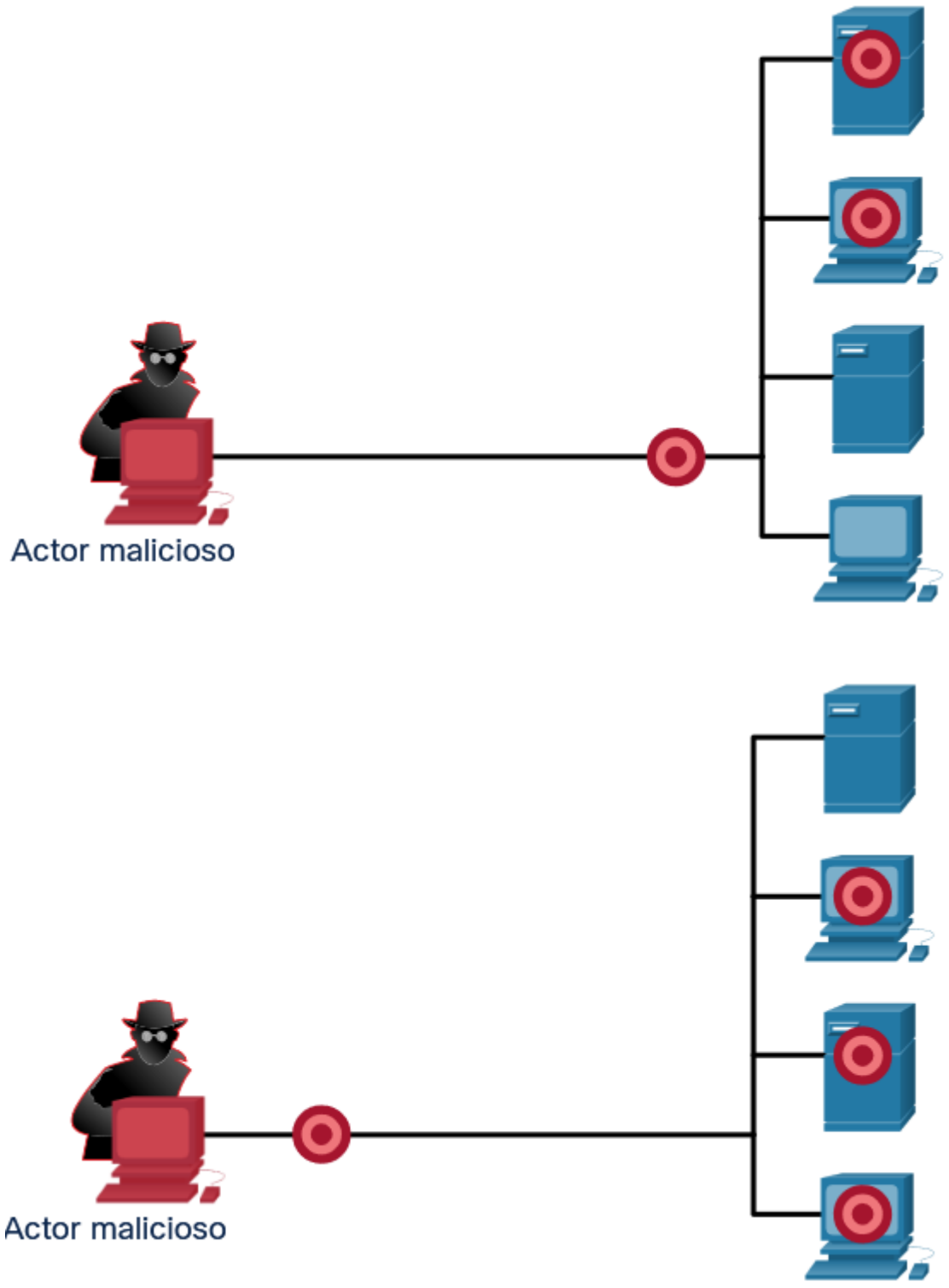
Consultas a través de Internet

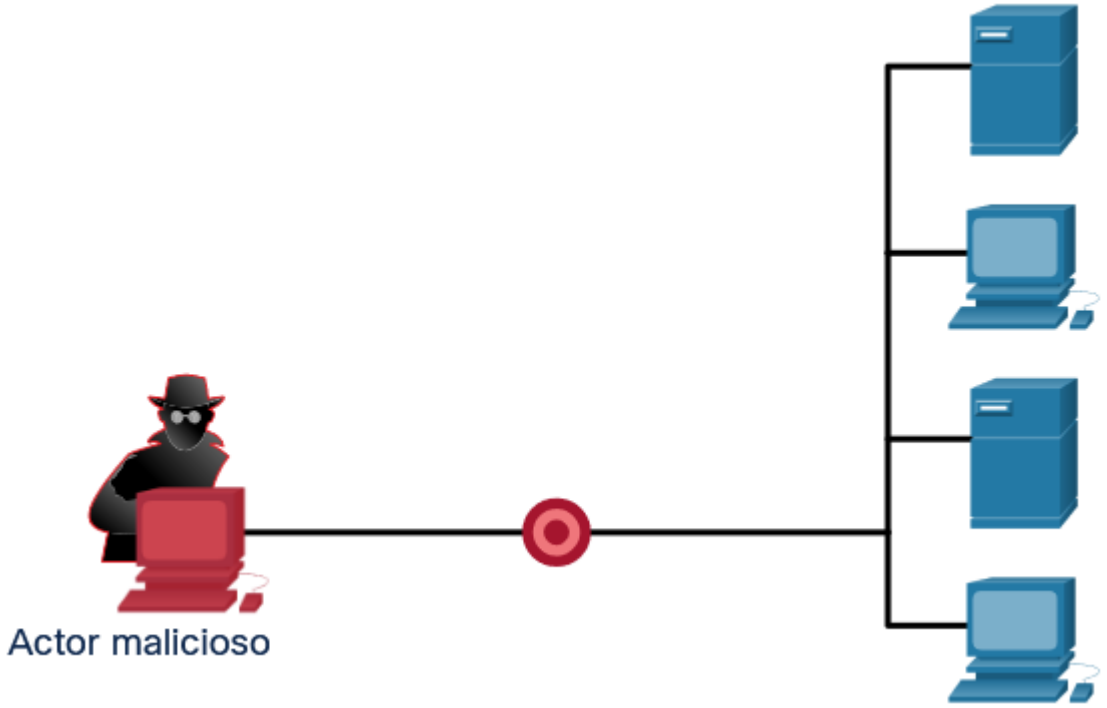




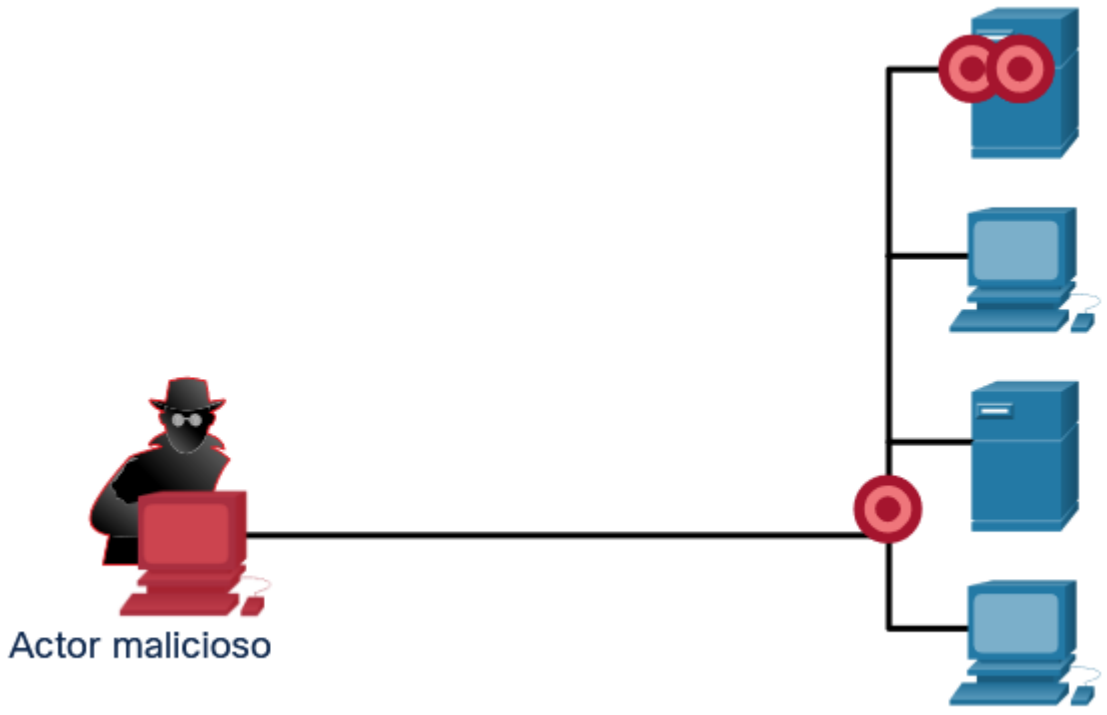
Barridos de Ping

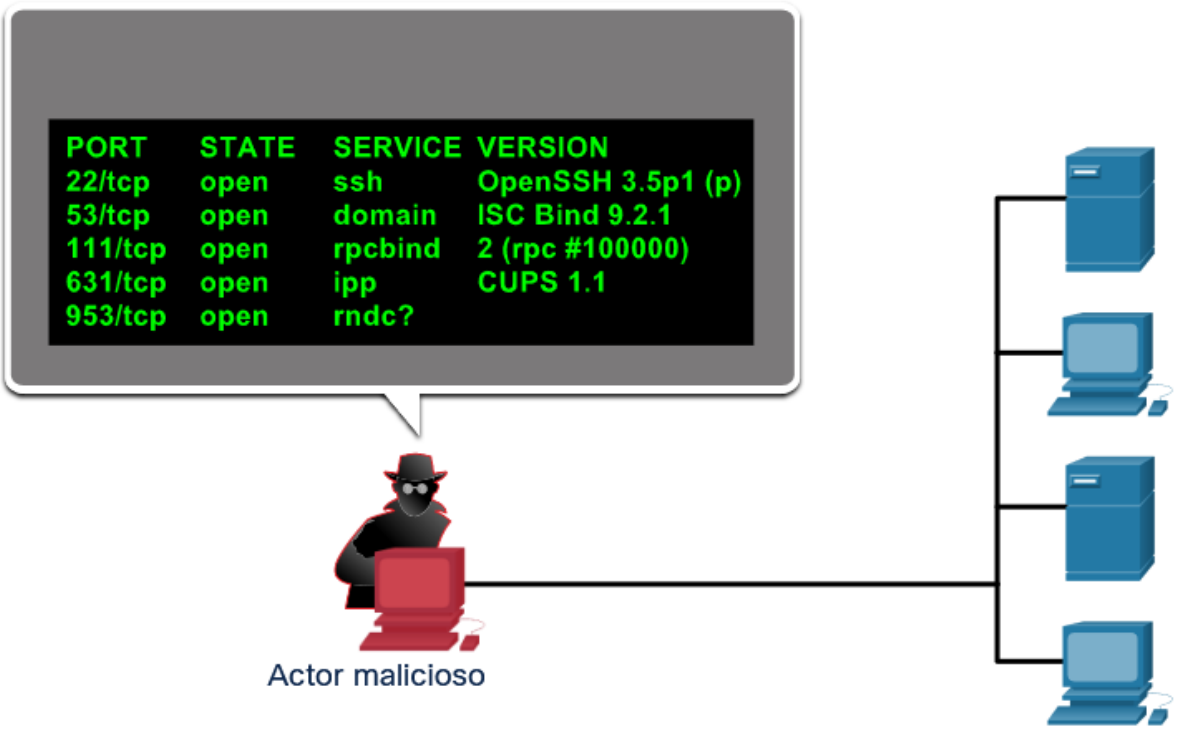



Actor malicioso
Actor malicioso



Escaneos de puertos





Ataques con acceso

Los ataques de acceso explotan las vulnerabilidades conocidas de los servicios de autenticación, los servicios FTP y los servicios Web para obtener acceso a las cuentas Web, a las bases de datos confidenciales y demás información confidencial. Un ataque de acceso permite a las personas obtener acceso no autorizado a información que no tienen derecho a ver. Los ataques de acceso se pueden clasificar en cuatro tipos: ataques de contraseña, explotación de confianza, redirección de puertos y man-in-the middle.

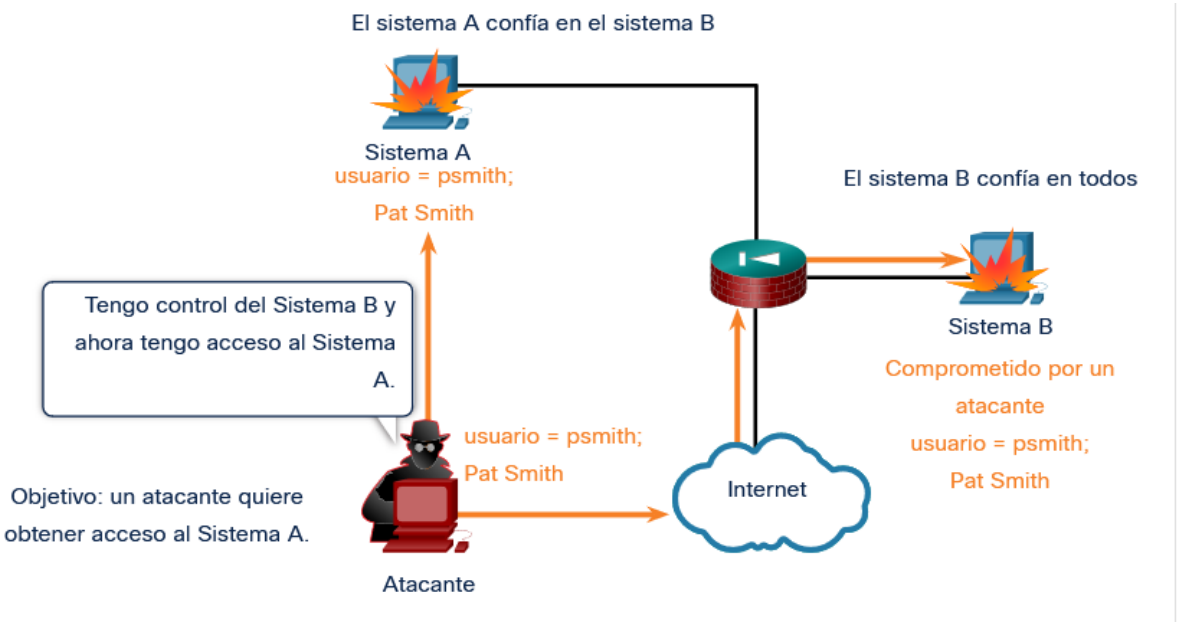
Ataques de contraseña

Los actores de amenazas pueden implementar ataques de contraseña utilizando varios métodos diferentesds:

- Ataques por fuerza bruta
- Ataques de caballos de Troya
- Programas detectores de paquetes

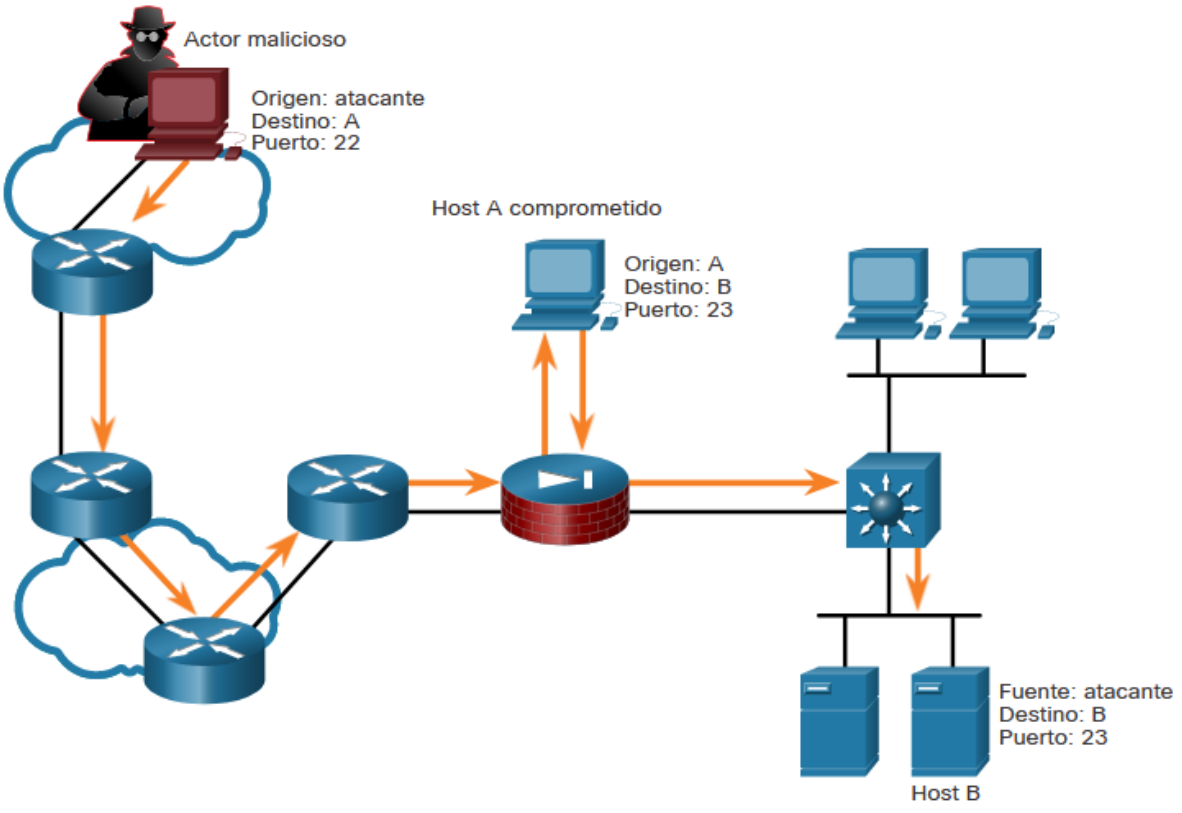
Explotación de confianza

En un ataque de explotación de confianza, un actor de amenazas utiliza privilegios no autorizados para obtener acceso a un sistema, posiblemente comprometiendo el objetivo.



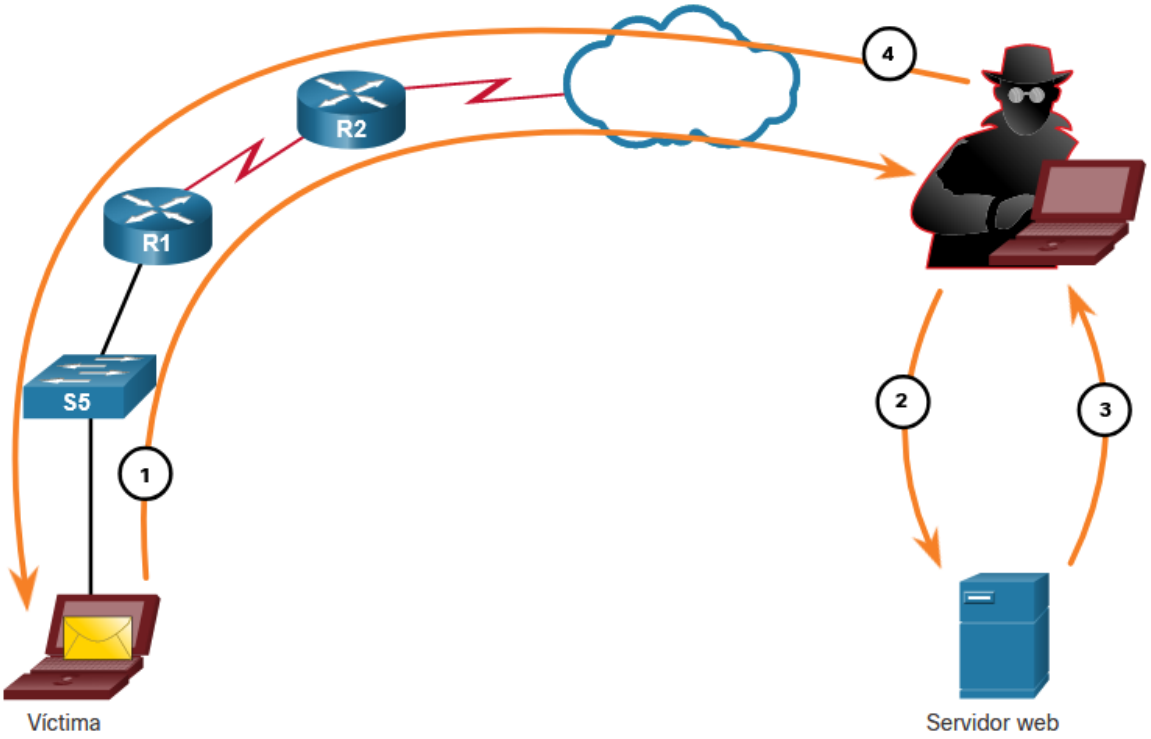
Redireccionamiento de puertos

Redireccionamiento de puertos: esto ocurre cuando un agente de amenaza utiliza un sistema en atacado como base para ataques contra otros objetivos. El ejemplo de la figura muestra un actor de amenaza que usa SSH (puerto 22) para conectarse a un host A comprometido. El host B confía en el host A y, por lo tanto, el actor de amenaza puede usar Telnet (puerto 23) para acceder a él.



Ataque Man-in-the-Middle

Ataque Man-in-the-Middle: el agente de amenaza se coloca entre dos entidades legítimas para leer, modificar o redirigir los datos que se transmiten entre las dos partes. En la figura 3, se ve un ejemplo de un ataque Man-in-the-Middle.



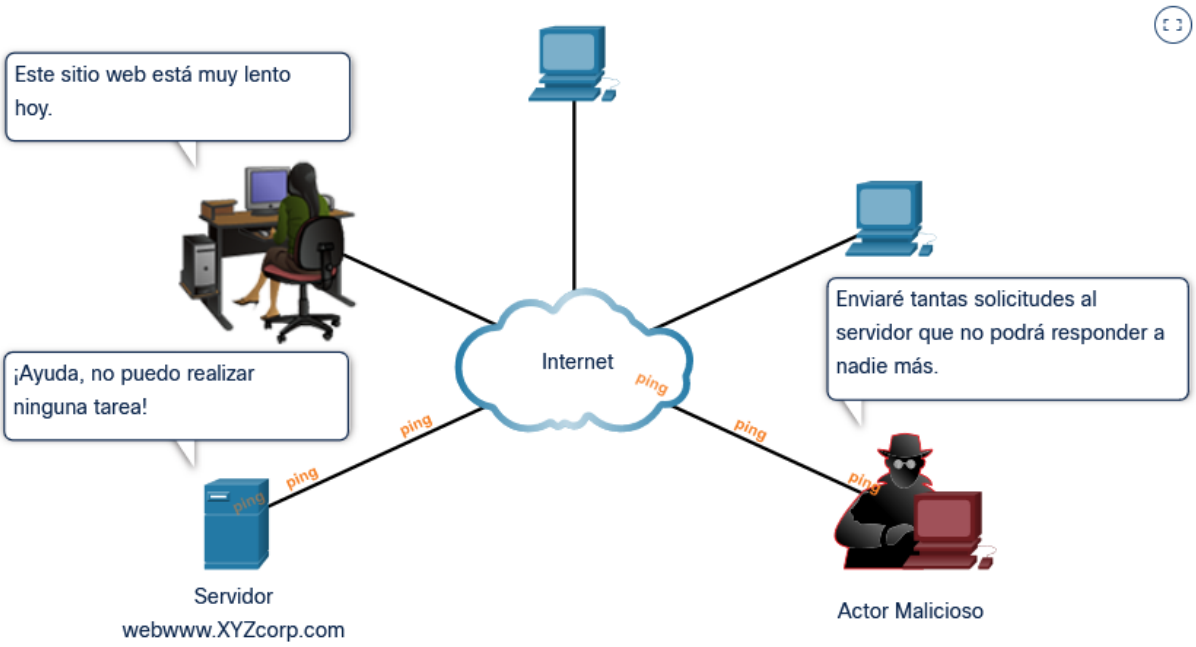
Ataques de denegación de servicio

Los ataques de denegación de servicio (DoS) son la forma de ataque más publicitada y una de las más difíciles de eliminar. Sin embargo, debido a su facilidad de implementación y daño potencialmente significativo, los ataques DoS merecen una atención especial por parte de los administradores de seguridad.

Los ataques DoS tienen muchas formas. Fundamentalmente, evitan que las personas autorizadas utilicen un servicio mediante el consumo de recursos del sistema. Para prevenir los ataques de DoS es importante estar al día con las actualizaciones de seguridad más recientes de los sistemas operativos y las aplicaciones.

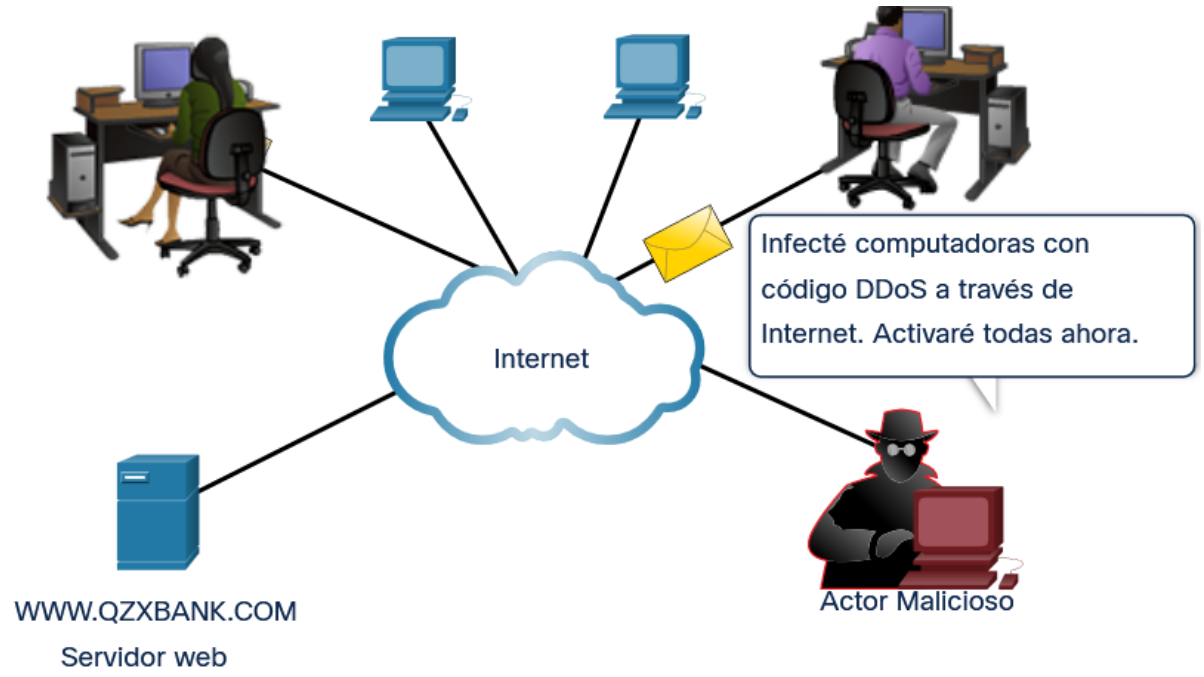
Ataque DoS

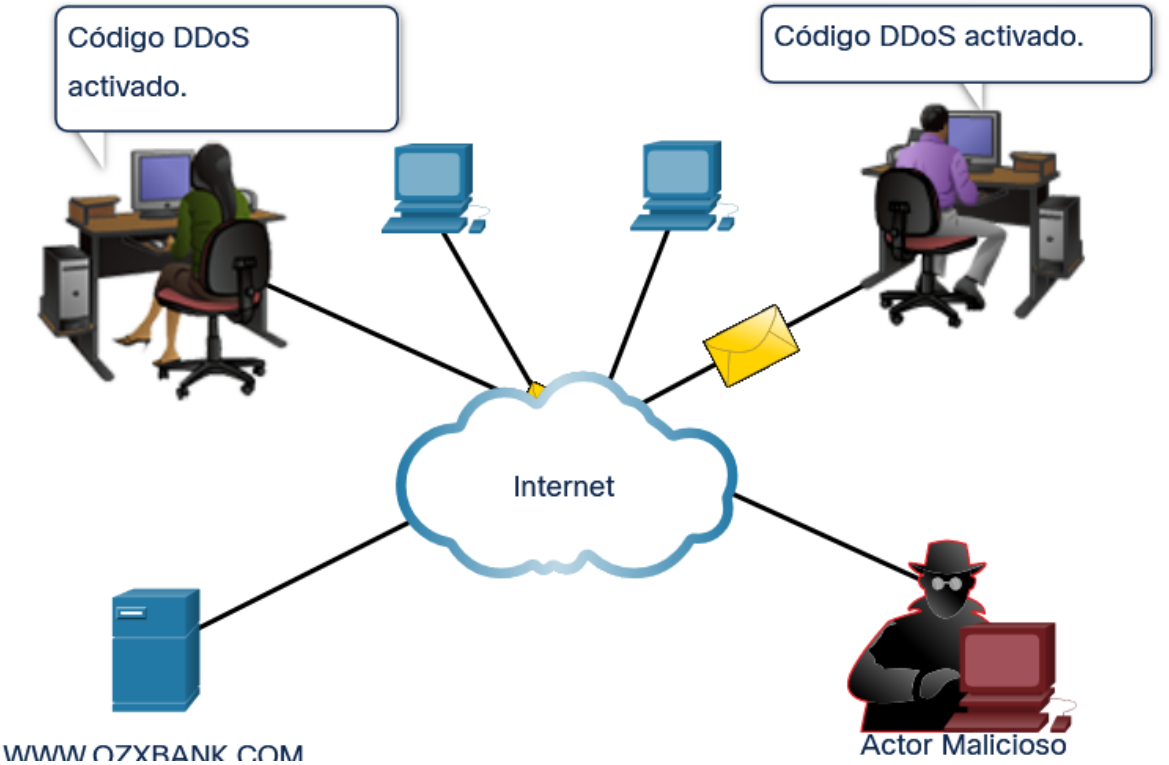
Los ataques de DoS son un riesgo importante porque pueden interrumpir fácilmente la comunicación y causar una pérdida significativa de tiempo y dinero. Estos ataques son relativamente simples de ejecutar, incluso si lo hace un agente de amenaza inexperto.

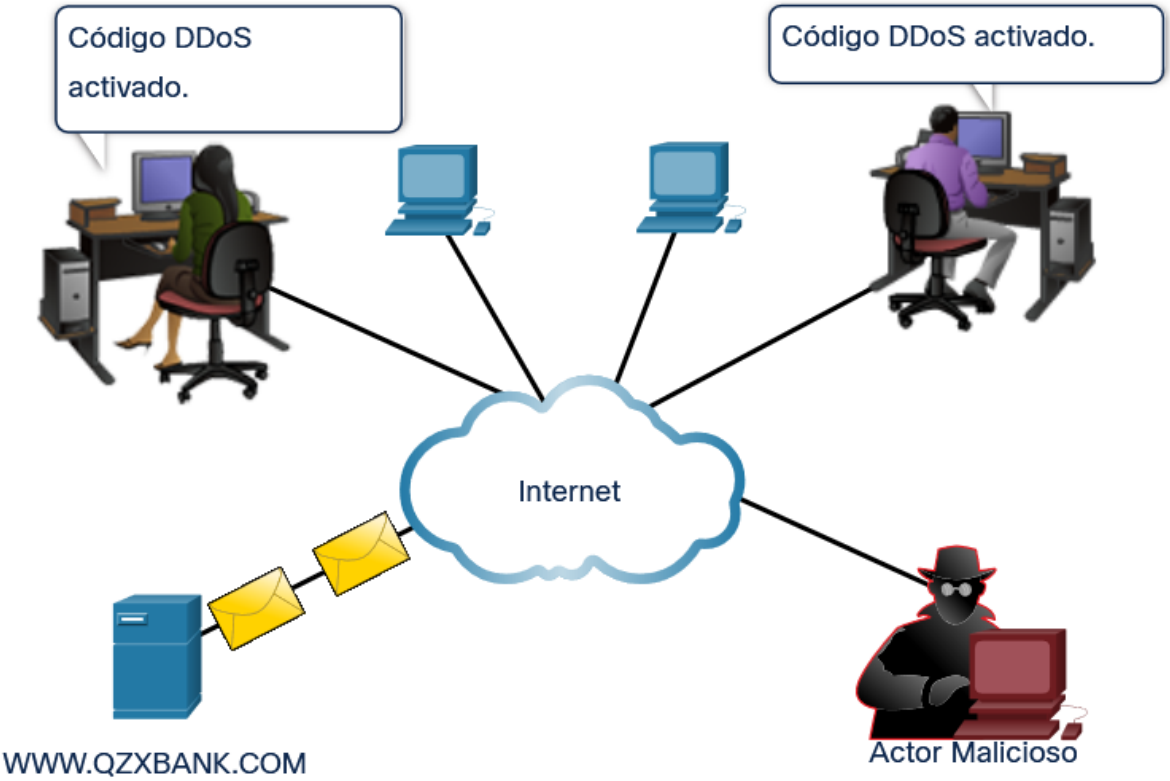


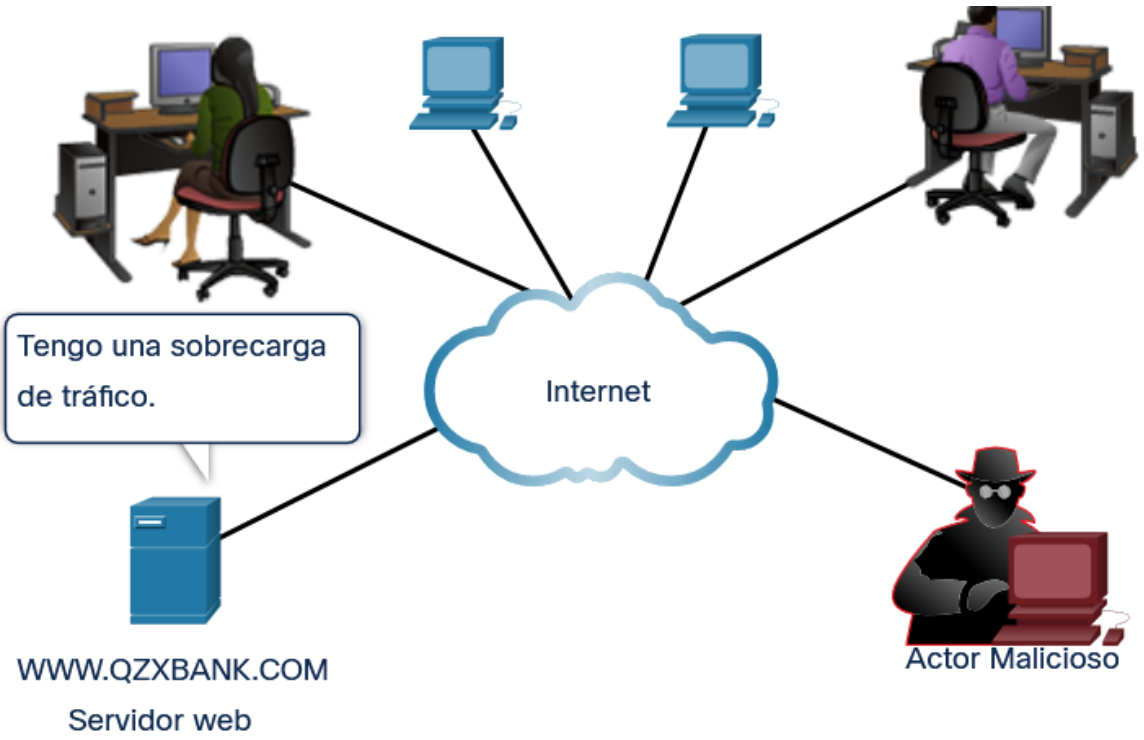
Ataque DDoS

A DDoS is similar to a Ataque DoS, but it originates from multiple, coordinated sources. Por ejemplo, un actor de amenazas construye una red de hosts infectados, conocidos como zombies. Una red de zombies se llama botnet. El actor de amenazas utiliza un programa de comando y control (CNC) para instruir a la botnet de zombies para llevar a cabo un ataque DDoS.




Código DDoS activado.
Código DDoS activado.
Internet
WWW.QZXBANK.COM
Actor Malicioso


Código DDoS activado.
Código DDoS activado.
Internet
WWW.QZXBANK.COM
Actor Malicioso



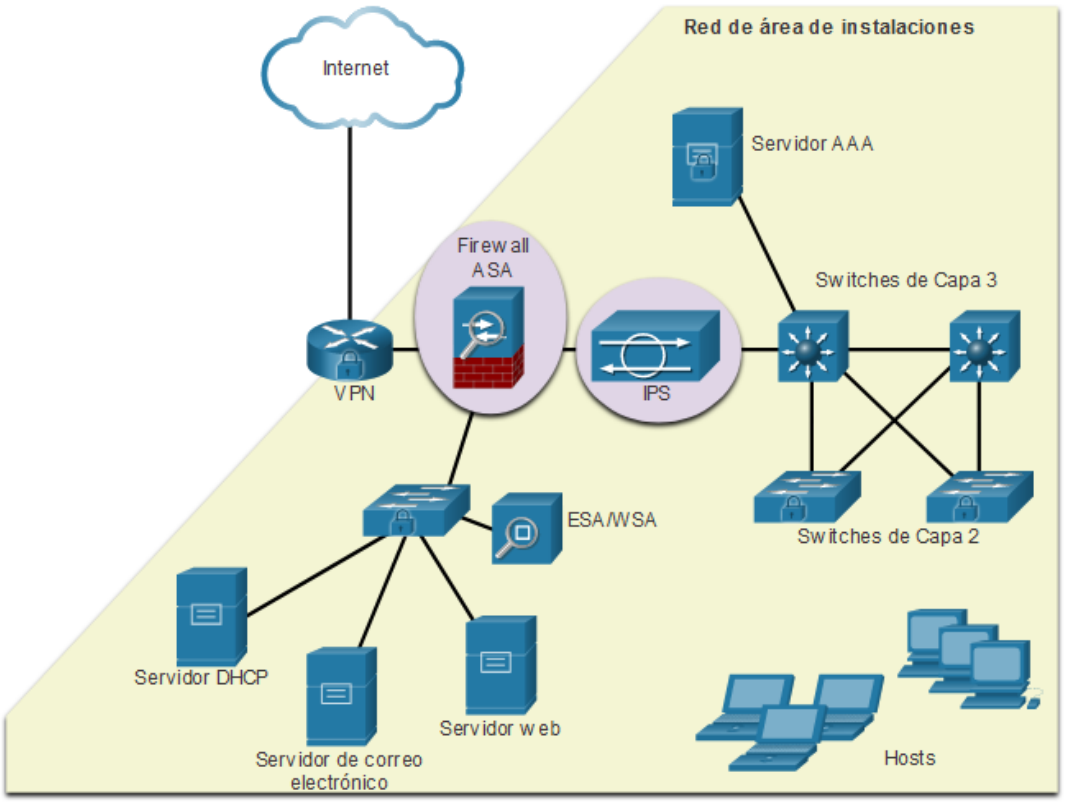
Enfoque de Defensa en Profundidad

Ahora que sabe más acerca de cómo los actores de amenazas pueden entrar en las redes, debe comprender qué hacer para evitar este acceso no autorizado. En este tema se detallan varias acciones que puede realizar para que su red sea más segura.

Para mitigar los ataques de red, primero debe proteger los dispositivos, incluidos enrutadores, conmutadores, servidores y hosts. La mayoría de las organizaciones emplean un enfoque de defensa en profundidad (también conocido como enfoque en capas) para la seguridad. Esto requiere una combinación de dispositivos y servicios de red que funcionen en conjunto.

Mire la red de la figura. Se han implementado varios dispositivos y servicios de seguridad para proteger a sus usuarios y activos contra las amenazas de TCP / IP.

Todos los dispositivos de red, incluidos el router y los switches, también están protegidos, como indican los candados de combinación de sus respectivos iconos. Esto indica que se han protegido para evitar que los actores de amenazas obtengan acceso y manipulen los dispositivos.



Se han implementado varios dispositivos y servicios de seguridad para proteger a los usuarios y activos de las amenazas de TCP/IP.

- **VPN** - Un router se utiliza para proporcionar servicios de VPN seguros con sitios corporativos y soporte de acceso remoto para usuarios remotos que utilizan túneles cifrados seguros.
- **ASA Firewall** - Este dispositivo dedicado proporciona servicios de firewall con control de estado. Garantiza que el tráfico interno pueda salir y regresar, pero el tráfico externo no puede iniciar conexiones a hosts internos.
- **IPS** - Un Sistema de Prevención de Intrusiones (Intrusion Prevention System IPS) monitorea el tráfico entrante y saliente en busca de malware, firmas de ataques a la red y más. Si el sistema reconoce una amenaza, puede detenerla inmediatamente.
- **ESA/WSA** - El Dispositivo de Seguridad de Correo electrónico (Email Security Appliance ESA) filtra el spam y los correos electrónicos sospechosos. El Dispositivo de Seguridad Web (Web Security Appliance WSA) filtra sitios de malware de Internet conocidos y sospechosos.
- **Servidor AAA** - Este servidor contiene una base de datos segura de quien está autorizado para acceder y administrar dispositivos de red. Los dispositivos de red autentican a los usuarios administrativos mediante esta base de datos.

Mantener copias de seguridad

Hacer una copia de seguridad de las configuraciones y los datos del dispositivo es una de las formas más efectivas de protección contra la pérdida de datos. Una copia de seguridad

de datos almacena una copia de la información de una PC en medios de copia de seguridad extraíbles que pueden conservarse en lugares seguros. Los dispositivos de infraestructura deben tener copias de seguridad de archivos de configuración e imágenes de IOS en un servidor FTP o de archivos similar. Si falla el equipo o el hardware del router, los datos o la configuración se pueden restaurar mediante la copia de seguridad.

Las copias de seguridad se deben realizar de forma regular tal como se identifica en la política de seguridad. Las copias de respaldo de datos suelen almacenarse externamente para proteger los medios de copia de respaldo en caso de que ocurra algo en la instalación principal. Los hosts de Windows tienen una utilidad de copia de respaldo y restauración. Es importante que los usuarios realicen una copia de seguridad de sus datos en otra unidad o en un proveedor de almacenamiento basado en la nube.

La tabla muestra las consideraciones de copia de seguridad y sus descripciones.

Consideración	Descripción
Frecuencia	● Realice copias de seguridad de forma regular como se identifica en la seguridad de TI de la empresa. ● Los backups completos pueden llevar mucho tiempo, por lo tanto, realizar mensualmente o copias de seguridad semanales con copias de seguridad parciales frecuentes de archivos modificados.
Almacenamiento	● Valide siempre las copias de seguridad para garantizar la integridad de los datos y validar los procedimientos de restauración de archivos.
Seguridad	● Las copias de seguridad deben transportarse a un almacenamiento fuera del sitio aprobado en una rotación diaria, semanal o mensual, según lo requiera la politica de seguridad.
Validación	● Las copias deben protegerse con contraseñas seguras. La contraseña es requerido para restaurar los datos.

Actualización, actualización y revisión

Mantenerse al día con los últimos desarrollos puede conducir a una defensa más efectiva contra los ataques a la red. A medida que se publica nuevo malware, las empresas deben mantenerse al día con las versiones más recientes del software antivirus.

La manera más eficaz de mitigar un ataque de gusanos consiste en descargar las actualizaciones de seguridad del proveedor del sistema operativo y aplicar parches a todos los sistemas vulnerables. La administración de numerosos sistemas implica la creación de

una imagen de software estándar (sistema operativo y aplicaciones acreditadas cuyo uso esté autorizado en los sistemas cliente) que se implementa en los sistemas nuevos o actualizados. Sin embargo, los requisitos de seguridad cambian y los sistemas ya implementados pueden necesitar tener parches de seguridad actualizados instalados.

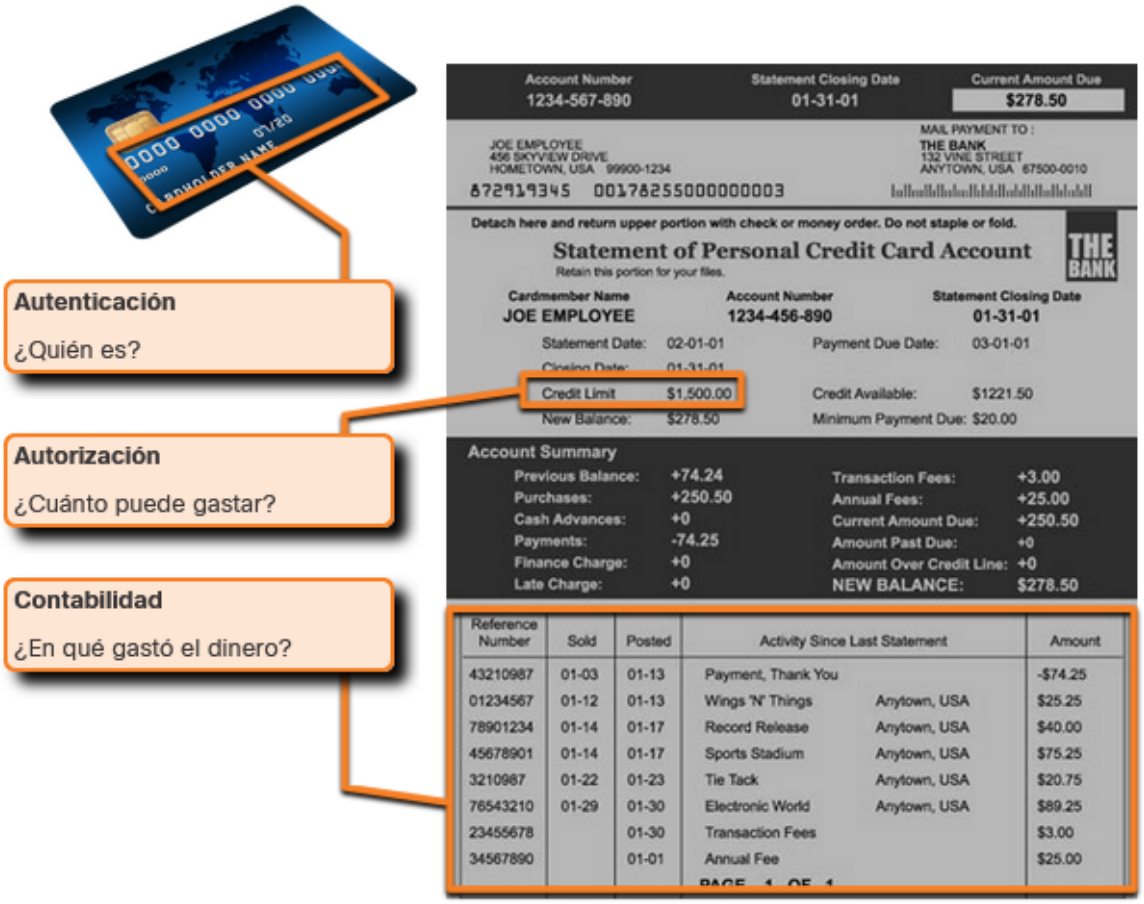
Una solución para la administración de parches de seguridad críticos es asegurarse de que todos los sistemas finales descarguen automáticamente actualizaciones, como se muestra para Windows 10 en la figura. Los parches de seguridad se descargan e instalan automáticamente sin la intervención del usuario.

Autenticación, autorización y contabilidad AAA

Todos los dispositivos de red deben estar configurados de forma segura para proporcionar acceso solo a personas autorizadas. Los servicios de seguridad de red de autenticación, autorización y contabilidad (AAA o "triple A") proporcionan el marco principal para configurar el control de acceso en dispositivos de red.

AAA es una forma de controlar quién tiene permiso para acceder a una red (autenticar), qué acciones realizan mientras acceden a la red (autorizar) y hacer un registro de lo que se hizo mientras están allí (contabilidad).

El concepto de AAA es similar al uso de una tarjeta de crédito. La tarjeta de crédito identifica quién la puede utilizar y cuánto puede gastar ese usuario, y lleva un registro de los elementos en los que el usuario gastó dinero, como se muestra en la ilustración.



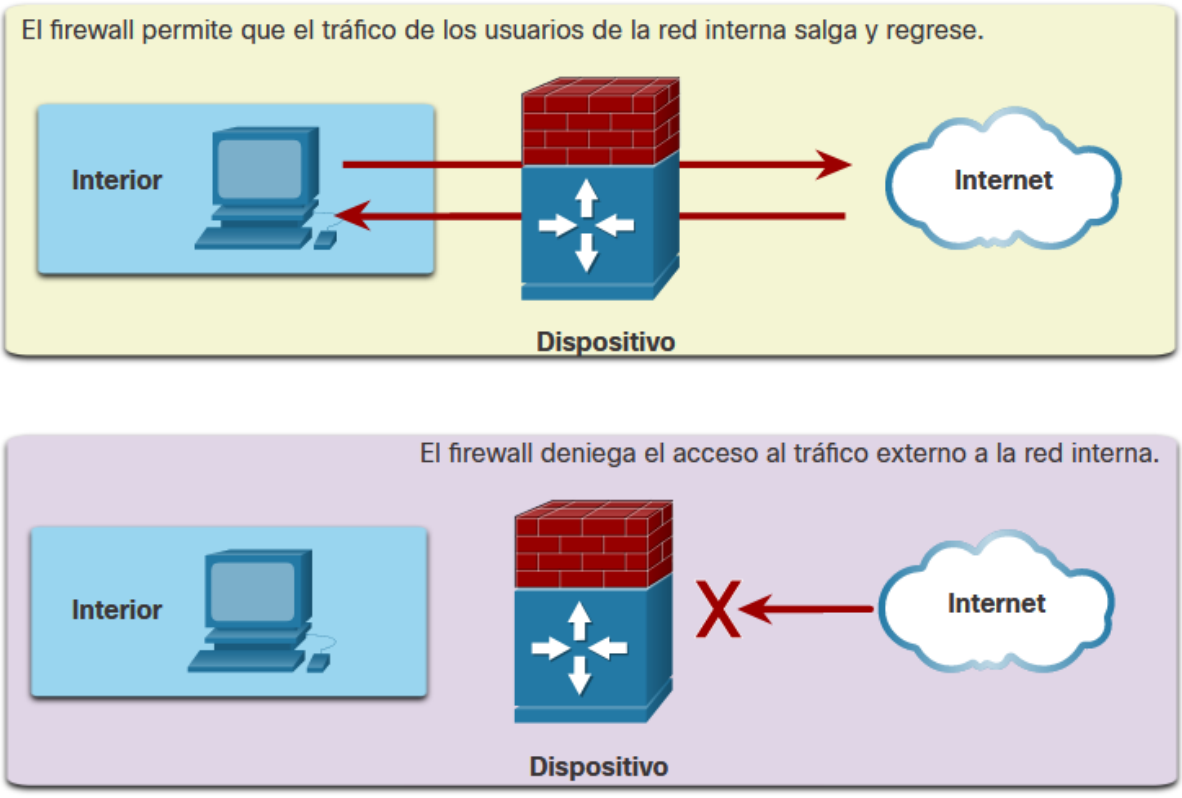
Firewalls

El firewall es una de las herramientas de seguridad más eficaces disponibles para la protección de los usuarios contra amenazas externas. Un firewall protege las computadoras y las redes evitando que el tráfico no deseado ingrese a las redes internas.

Los firewalls de red residen entre dos o más redes, controlan el tráfico entre ellas y evitan el acceso no autorizado. Por ejemplo, la topología superior en la figura ilustra cómo el firewall permite que el tráfico de un host de red interno salga de la red y regrese a la red interna. La topología inferior muestra cómo se niega el acceso a la red interna al tráfico iniciado por la red externa (es decir, Internet).

La figura muestra un rectángulo, etiquetado Inside. Dentro del rectángulo hay un 1 unidad. Fuera y a la derecha del rectángulo, hay un firewall. del derecha del firewall, hay una nube etiquetada, Internet. Hay dos flechas, uno que significa tráfico dejando el PC pasando por el firewall y fuera a la Internet. La segunda flecha indica el firewall que permite el tráfico desde el Internet a la PC. La figura muestra otro rectángulo, etiquetado Dentro. Dentro del rectángulo hay un 1 unidad. Fuera y a la derecha del rectángulo, hay un firewall. del derecha del firewall, hay una nube etiquetada, Internet. Hay una flecha apuntando desde Internet al firewall con una X que indica que el tráfico es siendo denegado desde Internet a la red interna.

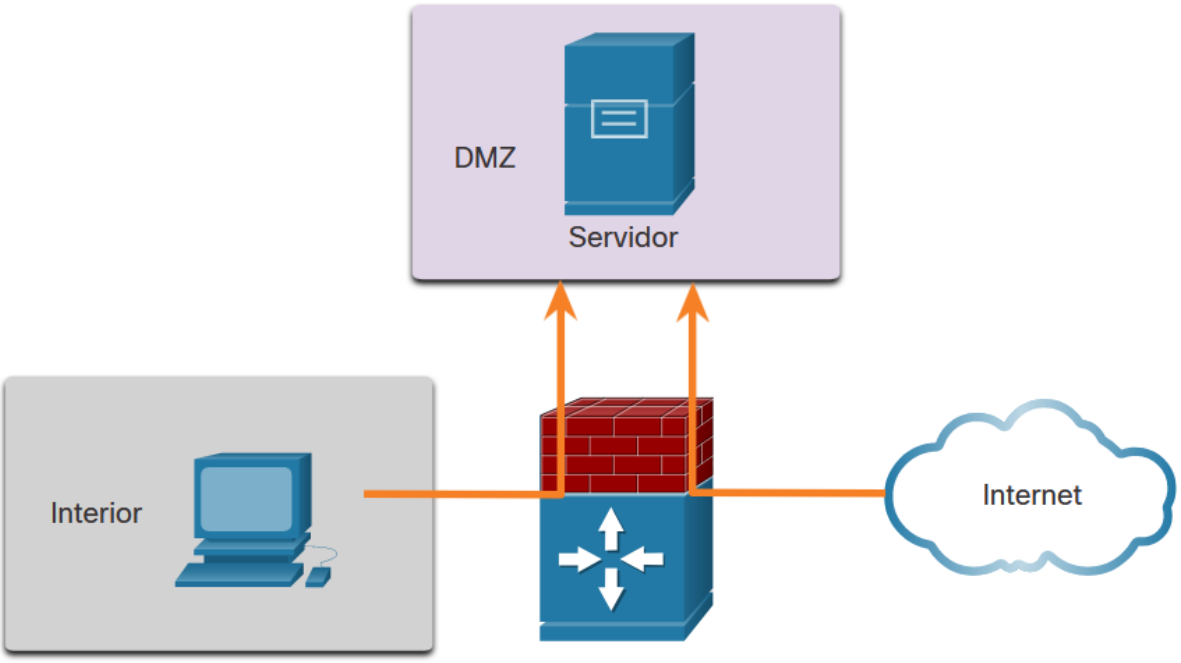
Funcionamiento del firewall



Un firewall podría brindar a usuarios externos acceso controlado a servicios específicos. Por ejemplo, los servidores accesibles para usuarios externos generalmente se encuentran en una red especial denominada zona desmilitarizada (DMZ), como se muestra en la figura. La DMZ permite a un administrador de red aplicar políticas específicas para los hosts conectados a esa red.

La figura muestra un rectángulo, etiquetado Inside. Dentro del rectángulo hay un 1 unidad. Fuera y a la derecha del rectángulo, hay un firewall. del derecha del firewall, hay una nube etiquetada Internet. Por encima del cortafuegos. hay un servidor DMZ dentro de un rectángulo. Hay dos flechas, una va desde el PC a través del firewall al servidor DMZ y otro que va desde el Internet a través del firewall al servidor DMZ.

Topología de firewall con DMZ



Tipos de firewalls

Los productos de firewall vienen empaquetados en varias formas. Estos productos utilizan diferentes técnicas para determinar qué se permitirá o negará el acceso a una red. Entre otros, se incluyen:

- **Filtrado de paquetes**: evita o permite el acceso en función de direcciones IP o MAC
- **Filtrado de aplicaciones**: evita o permite el acceso a tipos de aplicaciones específicos en función de los números de puerto
- **Filtrado de URL**: evita o permite el acceso a sitios web basados en URL o palabras clave específicas
- **Stateful packet inspection (SPI)**: los paquetes entrantes deben ser respuestas legítimas a las solicitudes de los hosts internos. Los paquetes no solicitados son bloqueados, a menos que se permitan específicamente. La SPI también puede incluir la capacidad de reconocer y filtrar tipos específicos de ataques, como los ataques por denegación de servicio (DoS).

Seguridad de terminales

Una terminal, o un host, es un sistema de computación o un dispositivo individual que actúa como cliente de red. Las terminales comunes son PC portátiles, computadoras de escritorio, servidores, teléfono inteligentes y tabletas. La seguridad de los dispositivos terminales es uno de los trabajos más desafiantes para un administrador de red, ya que incluye a la naturaleza humana. Las empresas deben aplicar políticas bien documentadas, y los empleados deben estar al tanto de estas reglas. Se debe capacitar a los empleados sobre el uso correcto de la red. En general, estas políticas incluyen el uso de software antivirus y

la prevención de intrusión de hosts. Las soluciones más integrales de seguridad de terminales dependen del control de acceso a la red.