

## Resumen 16

### Vulnerabilidades y amenazas a la seguridad

• **Tipos de amenazas** → 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 de software o explotando Vulnerabilidades se denominan **actores de amenazas**. Ya con acceso a la red hay 4 tipos de amenazas:

**Robo de información** → Es cuando en tu computadora la accesan y obtienen información confidencial, la información puede ser usada con varios propósitos: robar información de una empresa.

**Manipulación y perdida de datos** → Entrar para destruir o alterar los registros de datos. Por ejemplo, un actor de amenaza envía un virus que formatea el disco duro de una computadora.

**Robo de identidad** → Forma de robo de información en la que se roba información personal para apoderarse de la identidad de alguien.

**Interrupción del servicio** → Es una "prevención" legítima a los usuarios para acceder a los servicios que acceden a esos anuncios malignos.

• **Tipos de vulnerabilidades** → La vulnerabilidad es el grado de debilidad en una red o dispositivo. Algun grado de vulnerabilidad es inherente a routers, commutadores, PC, etc. Los que sufren más ataques son las terminales, servidores y PC de escritorio. Las 3 fuentes de vulnerabilidad pueden dejar a una red o dispositivo abierto a varios ataques. Son:

#### Vulnerabilidades tecnológicas

Vulnerabilidad	Descripción
Debilidad TCP/IP	HTTP, FTP, ICMP, SNMP, SMTP.
Debilidades de los sistemas operativos	Unix, Linux, MAC OS, Windows Server 2012, Windows 7 y Windows 8.
Debilidad de los equipos de red	Equipos de red como routers, firewalls. Falta de contraseña, autenticación, protocolos de enrutamiento y agujeros de firewall.

#### Vulnerabilidades de configuración

Cuentas de usuario no seguras, cuentas del sistema con contraseñas fáciles de adivinar, servicios de internet mal configurados, Configuraciones predeterminadas no seguras dentro de productos y equipos de red mal configurados.

#### Vulnerabilidades de política

Falta de políticas de seguridad por escrito, Políticas, Falta de continuidad de autenticación, controles de acceso lógico no aplicados, instalación de software y hardware y los cambios no

no respetan la política, no existe plan de recuperación tras un desastre.

● **Seguridad física** → Las 4 amenazas físicas son:

● **Amenazas de hardware** → Incluye daños físicos a servidores, routers, conmutadores, planta de cableado y estaciones de trabajo.

● **Amenazas de entorno** → Incluye temperaturas extremas (calor o frío).

● **Amenazas eléctricas** → Incluye picos de voltaje, voltaje de suministro insuficiente, energía no condicionada y Pérdida total de energía.

● **Amenazas de mantenimiento** → Esto incluye un manejo deficiente de componentes eléctricos clave, faltante de repuestos críticos, cableado deficiente y etiquetado deficiente.

## 16.2 Ataques de red

● **Tipos de malware** → Malware es el abreviado de software malicioso. Es un código o software diseñado para dañar, interrumpir, robar o inflingir acciones "malas" o ilegítimas.

● **Virus** → Tipo de malware que se propaga mediante la inserción de una copia de sí mismo en otro programa. Se propaga de compu a compu. Puede denegar servicios.

● **Gusanos** → Son similares a los virus en que se replican en copias funcionales de sí mismos y causan el mismo tipo de daño. Los gusanos son software independiente y no requieren de un programa host ni la ayuda humana para propagarse.

● **Caballos de troya** → Pieza de software dañino que parece legítimo. Después de instalarse puede lograr cualquier número de ataques al host. Son conocidos por abrir puertas para usuarios maliciosos.

● **Ataques de reconocimiento** → Además de malware, las redes pueden ser presas de ataques, las 3 categorías son: **ataques de reconocimiento** → Descubrimiento y mapeo de sistemas, servicios o Vulnerabilidades. **Ataques de acceso** → Manipulación no autorizada de datos, acceso al sistema o privilegios de usuario. **Denegación de servicio** → Desactivación o corrupción de redes, sistemas o servicios.

En un ataque de reconocimiento, los actores pueden usar herramientas de internet como nslookup como servicios públicos, whois para determinar el espacio de IP asignado a una corporación. También puede usar Fping ó gping, hace que todas las direcciones de red hagan ping en el rango de la red. Ejemplos:

- Consultas a través de internet

- Escaneo de puertos

- Barridos de ping

• **Ataques con acceso** → Exploran las vulnerabilidades conocidas de los servicios de autenticación, servicios FTP y servicios web para obtener acceso a las cuentas web, bases de datos confidenciales y demás información. Pueden clasificarse en:

**Ataques de contraseña** → Implementan ataques de contraseña usando ataques por fuerza bruta, caballos de troja y programas detectores de paquetes.

**Explotación de confianza** → Utilizan privilegios no autorizados para obtener acceso a un sistema, posiblemente comprometiendo el objetivo.

**Redireccionamiento de puertos** → Un agente de amenaza utiliza un sistema en atacado como base para ataques contra otros objetivos.

**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 2 partes.

• **Ataques de denegación de Servicio** → Forma más publicitada y difícil de eliminar. Tienen muchas formas, evitan que las personas autorizadas utilicen un servicio mediante el consumo de recursos del sistema.

**Ataque Dos** → Interrumpen fácilmente la comunicación y causa pérdida de tiempo y dinero. Envía solicitudes al servidor para que no pueda responder.

**Ataque DDoS** → Es similar a Dos pero puede ser múltiple. Un actor de amenaza construye una red de host infectados llamados zombies. La red se llama botnet.

### 16.3 Mitigaciones de ataque a la red

• **Enfoque de defensa en profundidad** → Para mitigar los ataques, primero debe proteger los dispositivos, routers, commutadores, host, switches. Las empresas enfocan la defensa en profundidad (**enfoque en capas**) para la seguridad.

**VPN** → Router que proporciona servicios VPN seguros con sitios corporativos y soporte de acceso remoto para usuarios remotos que usan túneles cifrados seguros.

**ASA Firewall** → Proporciona servicios firewall con control de estado. Garantiza el tráfico correcto para salir y regresar pero el tráfico externo no puede iniciar conexiones a hosts internos.

**IPS** → Monitorea el tráfico entrante y saliente en busca de malware, firmas de ataques a la red y más.

**ES/A/WSA** → Dispositivo de seguridad de correo filtra spam y correos sospechosos.

**Servidor AAA** → Contiene bases de datos de quién está autorizado a acceder y administrar dispositivos de red.

● **Mantener Copias de seguridad** → Forma más efectiva de protección contra 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 en lugares seguros.

Copia de seguridad y descripciones:

**Frecuencia** → Forma regular, backups completos se realizan mensualmente o semanalmente con copias de seguridad parciales frecuentes de archivos modificados.

**Almacenamiento** → Validar las copias de seguridad para integridad de datos y validar procedimientos de restauración de archivos.

**Seguridad** → Copias de Seguridad se transporta a un almacenamiento fuera del sitio aprobado en una rotación diaria, semanal o mensual.

**Validación** → Las copias deben protegerse con contraseñas seguras. Requerida para restaurar datos.

● **Actualización, actualización y revisión** → A medida que se publica nuevo malware, las empresas deben mantenerse al día con 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, parches**.

Una solución para la administración de parches de seguridad críticos se asegurarse de que todos los sistemas finales descarguen automáticamente actualizaciones.

● **Autenticación, autorización y contabilidad AAA** → Los servicios de seguridad de red de autenticación, autorización y contabilidad (AAA) 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**).

● **Firewalls** → Un firewall protege las computadoras y redes evitando que el tráfico no deseado ingrese a redes internas. Residen entre 2 o más redes, controlan el tráfico entre ellas y evitan el acceso no autorizado. El firewall permite el tráfico de usuarios de la red interna salga y regrese y el firewall deniega el acceso al tráfico externo a la red interna. Puede brindar a usuarios externos acceso controlado a servicios específicos. Los servidores se encuentran en una red especial **zona desmilitarizada (DMZ)**. Permite a un administrador aplicar políticas específicas.

● Tipos de firewalls → **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 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.

● Seguridad de terminales → Una terminal, host es un sistema de computación o un dispositivo individual que actúa como cliente de red. Los terminales comunes son PC, servidores, Smartphones y tablets. Las empresas deben aplicar políticas bien documentadas, y los empleados deben estar al tanto de estas reglas.

#### 16.4 Seguridad de los dispositivos

● Cisco AutoSecure → La configuración de seguridad se establece en los valores predeterminados cuando se instala un nuevo sistema operativo de un dispositivo. Esto es insuficiente. AutoSecure puede ayudar a asegurar el sistema. Hay pasos simples que se deben seguir y se aplican a la mayoría de S.O. - Se deben cambiar los nombres de usuario y contraseña predeterminada. - Restringir el acceso a los recursos del sistema. - Desactivar y desinstalar todos los servicios y aplicaciones innecesarios.

● Contraseñas → las pautas estándar para una contraseña:

- Contraseña de al menos 8 caracteres.

- Contraseñas complejas, combinando mayúsculas y minúsculas. - Cambie la contraseña con frecuencia.

- Evitar las contraseñas basadas en repetición.

- Escriba una contraseña con errores de ortografía. - No anote las contraseñas.

Un método para crear una contraseña segura es utilizar barra espaciadora y crear una frase compuesta de muchas palabras. Se conoce como **frase de contraseña**.

● Seguridad adicional de contraseñas →