20 amenazas de ciberseguridad

Emilio Cabo Gomis

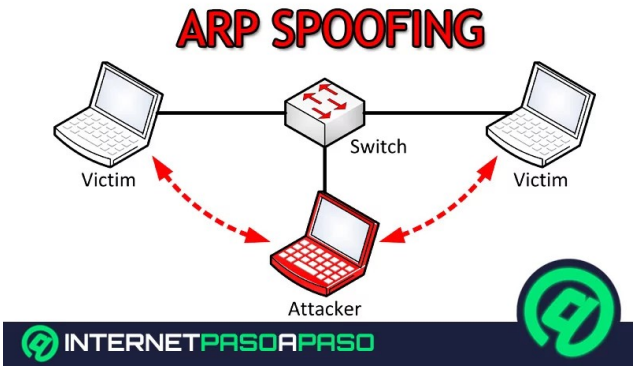
Índice

20 ataques (Descripción y prevención)

Phishing
Descripción: Engañar a los usuarios haciéndose pasar por una institución o persona para que proporcionen credenciales de acceso.
Prevención: Educación para identificar amenazas por parte de los usuarios.

Denegación de Servicio (DoS)
Descripción: Inundar servicios con peticiones para que las solicitudes legítimas no encuentren ancho de banda.
Prevención: Empleo de firewalls y sistemas de detección de intrusos (IDS).

ARP Spoofing
Descripción: Manipular el protocolo ARP para asociar la dirección MAC del atacante con la dirección IP de otro nodo.
Prevención: Usar ARP estático, activar inspección ARP en switches y herramientas de detección de intrusiones.



Keyloggers
Descripción: Registrar las pulsaciones de teclas para robar información.
Prevención: Usar software antivirus e implementar seguridad del software.

Ransomware
Descripción: Malware que cifra archivos y exige un pago para restaurar el acceso.
Prevención: Respaldos regulares, software antivirus actualizado y evitar enlaces sospechosos.

Man-in-the-Middle (MITM)
Descripción: Interceptar y alterar la comunicación entre dos partes sin que estas lo sepan. Además podemos modificar los datos que le llegan al tercero
Prevención: Uso de cifrado extremo a extremo y redes privadas virtuales (VPN).

SQL Injection
Descripción: Insertar código SQL malicioso en formularios web para manipular bases de datos.
Prevención: Validar entradas de usuarios y usar consultas preparadas.

Cross-Site Scripting (XSS)
Descripción: Inyectar scripts maliciosos en páginas web vistas por otros usuarios.
Prevención: Filtrar y validar datos de entrada, y usar políticas de seguridad de contenido (CSP).

Malware
Descripción: Software diseñado para dañar, interrumpir o acceder a sistemas de forma no autorizada. Suele inyectarse de forma inadvertida.
Prevención: Mantener software actualizado y usar herramientas de detección de malware.

Ataques de fuerza bruta
Descripción: Intentar múltiples combinaciones de contraseñas hasta encontrar la correcta.
Prevención: Uso de contraseñas fuertes y bloqueo tras varios intentos fallidos.

Spoofing de correo electrónico
Descripción: Enviar correos que parecen provenir de una fuente confiable para engañar al receptor.
Prevención: Implementar autenticación SPF, DKIM y DMARC en servidores de correo.

Ataques de día cero
Descripción: Aprovechar vulnerabilidades desconocidas antes de que sean parchadas. Estas vulnerabilidades aún no han sido descubiertas por proveedores de software o
Prevención: Usar sistemas de detección de amenazas y aplicar actualizaciones de seguridad inmediatamente.

Sniffing
Descripción: Interceptar tráfico de red para capturar información sensible.
Prevención: Usar cifrado en las comunicaciones (TLS/SSL).

Rootkits
Descripción: Malware que proporciona acceso remoto y encubre su presencia en el sistema.
Prevención: Implementar detección avanzada de malware y limitar privilegios de usuario.

Ingeniería social

Descripción: Manipular psicológicamente a las personas para que revelen información confidencial.

Prevención: Educación y entrenamiento continuo para reconocer tácticas de manipulación.

Ataques a contraseñas

Descripción: Métodos para obtener contraseñas, como diccionarios o phishing.

Prevención: Usar autenticación multifactor y contraseñas seguras.

Exploits

Descripción: Aprovechar vulnerabilidades en software o hardware para comprometer un sistema.

Prevención: Actualizaciones regulares y monitoreo constante de sistemas.

Botnets

Descripción: Red de dispositivos infectados controlados de forma remota para realizar actividades maliciosas.

Prevención: Usar firewalls, IDS y actualizar dispositivos IoT.

Criptominería no autorizada

Descripción: Uso de recursos de hardware de la víctima para minar criptomonedas sin permiso.
Prevención: Implementar herramientas de detección de minería y actualizaciones de seguridad.

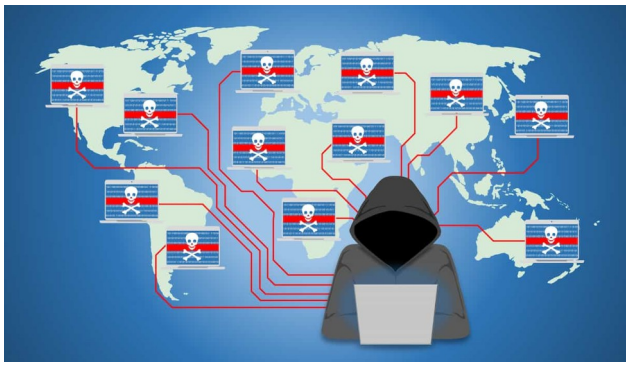
Ataques de replay

Descripción: Reutilizar datos interceptados ex acceder a sistemas o redes.
Prevención: Uso de tokens únicos y cifrado en las transmisiones de datos.

Anécdota

Mirai es un software que mediante infección de dispositivos IOT cómo impresoras o cafeteras, cámaras de seguridad.

Estos dispositivos se controlan mediante un servidor de "*command and control*" que hace que todos actúen a la vez.



En un ataque al proveedor de DNS DYN con cientos de millones de máquinas haciendo peticiones desde diferentes partes del mundo.

Este ataque dejó sin servicio a millones de usuarios de Norteamérica y Europa.