Herramientas Ciberseguridad

🔒 Ataques comunes en el Modelo OSI:

El modelo OSI (Open Systems Interconnection) no solo es una guía para entender cómo funciona la comunicación en redes, sino también un marco esencial para identificar y mitigar vulnerabilidades.

Cada una de sus #7 capas es susceptible a diferentes tipos de ataques cibernéticos:

1️⃣ Capa Física (Physical Layer):

- Ataque común:Sniffing Los atacantes interceptan señales físicas (cables, Wi-Fi) para capturar datos transmitidos.

- Ejemplo: Uso de herramientas como Wireshark para capturar paquetes en una red no cifrada.

- Protección:

- Usar cifrado en todas las comunicaciones (por ejemplo, WPA3 en Wi-Fi).

2️⃣ Capa de Enlace de Datos (Data Link Layer)

- Ataque común:Spoofing Los atacantes falsifican direcciones MAC para suplantar dispositivos en la red.

- Ejemplo: Ataques ARP spoofing para redirigir tráfico a un atacante.

- Protección:

- Implementar protocolos como DHCP snooping y detección de ARP spoofing.

- Usar VLANs para segmentar la red y limitar el alcance de los ataques.

3 Capa de Red (Network Layer)

- Ataque común: Man in the Middle (MITM).

- Los atacantes se interponen entre dos dispositivos para interceptar o modificar el tráfico.

- Ejemplo:Ataques en redes públicas o mal configuradas.

- Protección:

- Usar VPNs para cifrar el tráfico.

4 Capa de Transporte (Transport Layer).

- Ataque común: Reconocimiento (Reconnaissance).

- Los atacantes escanean puertos y servicios para identificar vulnerabilidades.

- Ejemplo: Uso de herramientas como Nmap para descubrir puertos abiertos.

- Protección:

- Cerrar puertos innecesarios y usar firewalls.

- Implementar sistemas de detección de intrusiones (IDS).

5 Capa de Sesión (Session Layer)

- Ataque común: Hijacking

- Los atacantes secuestran sesiones activas para tomar el control de una conexión.

- Ejemplo: Robo de cookies de sesión en aplicaciones web.

- Protección:

- Usar tokens de sesión seguros y regenerarlos frecuentemente.

- Implementar autenticación (MFA).

6 Capa de Presentación (Presentation Layer).

- Ataque común: Phishing

- Los atacantes engañan a los usuarios para obtener información confidencial.

- Ejemplo: Correos electrónicos falsos que imitan a entidades legítimas.

- Protección:

- Educar a los usuarios sobre cómo identificar intentos de phishing.

- Usar filtros de correo y soluciones antiphishing.

7️⃣ Capa de Aplicación (Application Layer).

- Ataque común: Exploit

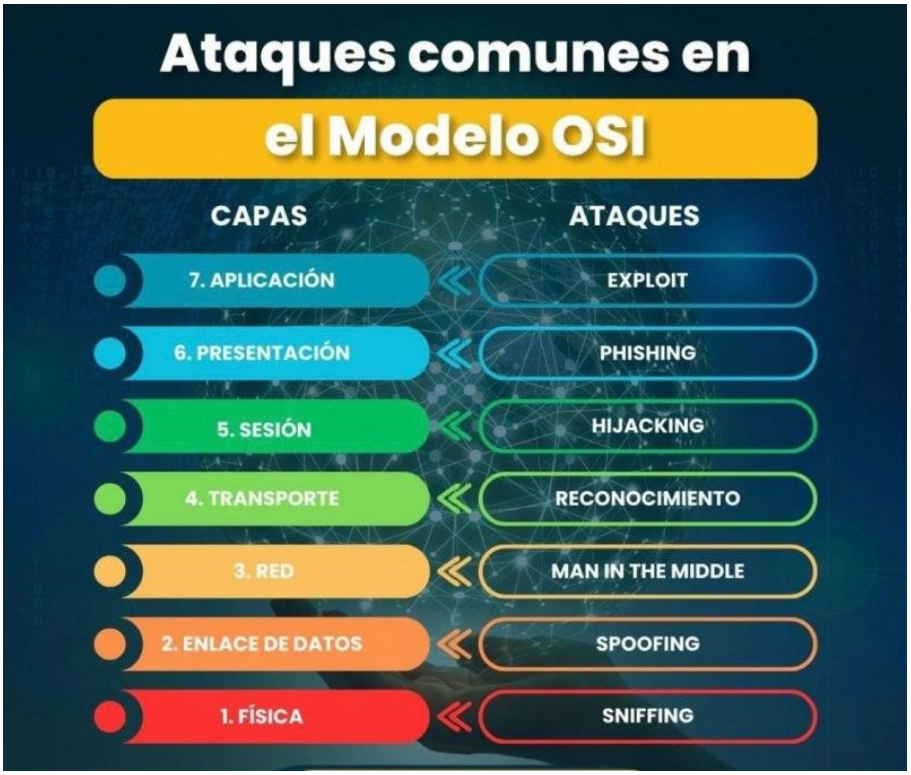
- Los atacantes aprovechan vulnerabilidades en aplicaciones para obtener acceso no autorizado.

- Ejemplo :Explotación de fallos en software desactualizado.

- Protección:

- Mantener el software actualizado con los últimos parches de seguridad.

- Usar firewalls de aplicaciones web (WAF).



Herramientas

En ciberseguridad, la prevención, detección e investigación son clave para proteger nuestros sistemas y redes. Ya sea en defensa (Blue Team) o ataque controlado (Red Team – Hacking Ético), contar con las herramientas adecuadas marca la diferencia.

Aquí tienes una lista de herramientas imprescindibles en distintas categorías:

🔍 Escaneo y Evaluación de Vulnerabilidades

✅ OpenVAS – Escaneo de vulnerabilidades en redes y sistemas.

✅ Nessus – Detección de debilidades en servidores y aplicaciones.

✅ Zed Attack Proxy (ZAP) – Pentesting web automatizado y manual.

✅ Nmap – Descubrimiento de hosts y puertos abiertos en una red.

🎯 Hacking Ético y Pentesting

🚀 SQLMap – Automatiza ataques de inyección SQL.

🚀 Burp Suite – Análisis y explotación de vulnerabilidades en apps web.

🚀 Metasploit – Framework para pruebas de penetración y explotación de sistemas.

🚀 John the Ripper – Auditoría y fuerza bruta de contraseñas.

🚀 Aircrack-NG – Evaluación de seguridad en redes Wi-Fi.

🌎 Análisis de Red y OSINT

🔎 Wireshark – Captura y análisis de tráfico en red.

🔎 Maltego – Inteligencia de fuentes abiertas (OSINT) para análisis de relaciones.

🔎 OpenSSH – Conexiones seguras y administración remota.

🧿 Análisis y Detección de Malware

🛑 VirusTotal – Escaneo de archivos y URLs con múltiples motores antivirus.

🛑 Hybrid Analysis – Sandbox para análisis dinámico de malware.

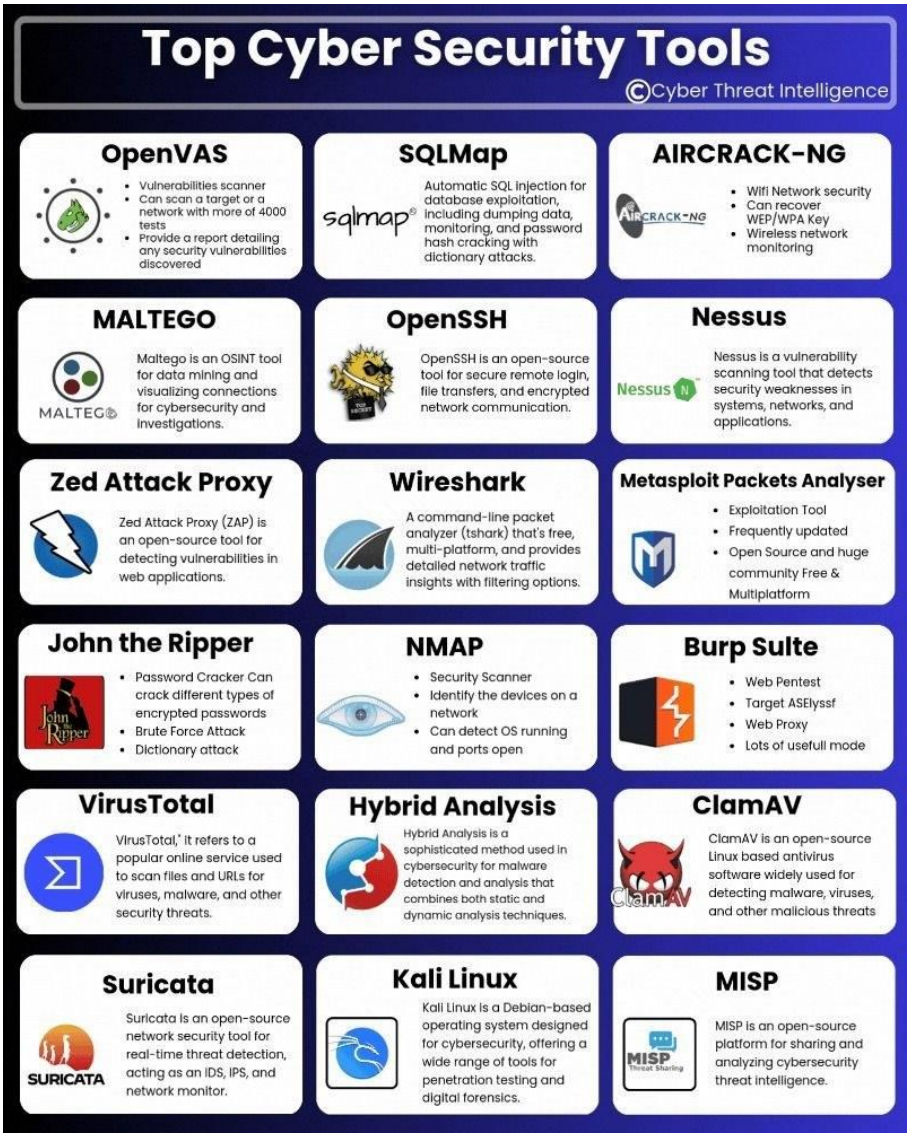
🛑 ClamAV – Antivirus de código abierto para entornos Linux.

🔐 Seguridad en Red y Sistemas Operativos

🔷 Suricata – Sistema de detección y prevención de intrusiones (IDS/IPS).

🔷 Kali Linux – Distribución especializada en ciberseguridad y pentesting.

🔷 MISP – Plataforma de compartición de inteligencia de amenazas.



HERRAMIENTAS Y TRUCOS PARA DETECTAR AMENAZAS

🔥ANALIZA CORREOS SOSPECHOSOS

🛠️ Herramientas clave:

- MxToolBox → https://mxtoolbox.com/ : Analiza cabeceras

- Google Message Header → https://toolbox.googleapps.com/apps/messageheader/: Descifra cabeceras

- Microsoft Azure Header Analyzer→ https://mha.azurewebsites.net/ : Herramienta oficial de Microsoft

- Gaijin Email Tester→ https://email.gaijin.at/ : Detecta suplantación de identidad

💡Truco: Verifica los campos "Received-SPF" y "Reply-To". Si algo no cuadra es una señal de alarma

🌐 **DESENMASCARA ENLACES MALICIOSOS E IPs**

🔎 Verificadores de reputación:

- VirusTotal → https://www.virustotal.com/gui/ : Escanea URLs/IPs

- AbuseIPDB → https://www.abuseipdb.com/ : Reporta IPs maliciosas

- urlscan.io → https://urlscan.io/ : Previsualiza sitios web sin riesgo

- IBM X-Force → https://exchange.xforce.ibmcloud.com/: Base de datos de amenazas avanzadas

⚡ Usa Webcheck Security https://web-check.xyz/ → Un escaneo OSINT completo para analizar DNS, SSL e historial de redes.

📂 **ANALIZA ARCHIVOS Y MALWARE**

🔬 Herramientas de sandbox:

- ANY.RUN → https://any.run/ : Análisis interactivo de malware

- Hybrid Analysis → https://www.hybrid-analysis.com/: Detecta zero-days

- Joe Sandbox → https://www.joesandbox.com/#windows: Inspección profunda de archivos

- Triage → https://tria.ge/ : Informes automáticos de malware

⚠️ Alerta: Nunca abras adjuntos desconocidos. Primero escanea con VirusTotal

🔍 **RASTREA PROPIETARIOS DE DOMINIOS E IPs**

- CentralOps → https://centralops.net/ : Dossier completo de dominios

- ViewDNS.info → https://viewdns.info/ : Búsqueda inversa de IP

- DomainTools → https://whois.domaintools.com/ : Datos históricos de dominios

🎯 Usa IPinfo (https://ipinfo.io/) → Geolocalización de IPs para mapear infraestructura de atacantes.

🎧 **AUTOMATIZA EL ANÁLISIS DE PHISHING**

🤖 Herramientas contra phishing:

- PhishTool → https://phishtool.org/ : Kit gratuito para análisis

- CyberChef → https://gchq.github.io/CyberChef/ : Descifra URLs ofuscadas

- PhishCheck → https://phishcheck.me/ : Detecta clones de sitios legítimos

🧩 **HERRAMIENTAS EXTRA Y HACKS**

- Browserling→ https://www.browserling.com/: Navegación segura en sandbox

- HaveIBeenPwned→ https://haveibeenpwned.com/ : Verifica si tus datos han sido filtrados

- PhishingArmy→ https://phishing.army/ : Lista de bloqueo de phishing

Herramientas preinstaladas en el SO

En Windows:

✅ • Power Automate Desktop: automatiza tareas repetitivas como un mini-robot.

✅ • Windows Sandbox: prueba archivos dudosos sin ensuciar el sistema.

✅ • Sysinternals Suite: herramientas brutales para diagnosticar, monitorear y optimizar.

✅ • Robocopy: copias automáticas con verificación avanzada.

✅ • BitLocker: cifrado completo de disco incluido.

En Linux:

✳️ • rsync + cron: copias de seguridad automáticas y sincronización sin abrir un solo programa.

✳️ • fail2ban: protección inteligente contra ataques sin pagar antivirus.

✳️ • systemd timers: mejor que cron, más flexible, más pro.

✳️ • tmux + htop: controla sesiones y monitoriza todo como un hacker (pero legal).

✳️ • Cockpit: interfaz web brutal para gestionar servidores con clics.

Motores de búsqueda especializados

I. Descubrimiento de Activos y Superficie de Ataque 🌐

Estos motores te permiten mapear la infraestructura de internet y descubrir dispositivos y servicios conectados.

1. 🛡️ **Shodan.io (Server):** El motor de búsqueda más conocido para encontrar dispositivos conectados a internet. Ideal para descubrir servidores, cámaras web, routers y mucho más.

2. 🌐 **Onyphy.io (Server):** Similar a Shodan, ofrece una interfaz intuitiva para descubrir dispositivos y su información asociada.
3. ⚙️ **Censys.io (Server):** Otro potente motor que indexa dispositivos conectados, proporcionando datos detallados sobre sus configuraciones y certificados.
4. 🎯 **App.netlas.io (Attack Surface):** Te ayuda a mapear la superficie de ataque de una organización, identificando posibles puntos débiles.
5. 🎯 **Binaryedge.io (Attack Surface):** Ofrece capacidades de escaneo y análisis de la superficie de ataque, identificando vulnerabilidades y exposiciones.
6. 🛠️ **Ivre.rocks (Server):** Una interfaz web para interactuar con los resultados de escaneos de red realizados con herramientas como Nmap.
7. 🕵️ **Spyse.com:** Un motor de búsqueda integral para activos de internet, incluyendo información de DNS, WHOIS y mucho más.
8. 🔍 **Fullhunt.io (Attack Surface):** Especializado en el descubrimiento de subdominios, una parte crucial de la evaluación de la superficie de ataque.

II. Inteligencia de Amenazas y Análisis de Riesgos 🚨

Mantente un paso adelante de los atacantes con estos motores que te brindan información crucial sobre amenazas y actividades maliciosas.

1. 🚨 **App.binaryedge.io (Threat Intelligence):** Ofrece información sobre amenazas activas, malware y vulnerabilidades explotadas.
2. 🚦 **Viz.greynoise.io (Threat Intelligence):** Ayuda a filtrar el "ruido" de internet, permitiéndote enfocarte en la actividad maliciosa real.
3. CN **Fofa.info (Threat Intelligence):** Un motor de búsqueda de inteligencia de amenazas con un enfoque en la infraestructura china.
4. 👀 **Zoomeye.org (Threat Intelligence):** Similar a Shodan y Censys, con capacidades adicionales para analizar dispositivos y sus posibles vulnerabilidades.
5. 🔓 **Leakix.net (Threat Intelligence):** Indexa información que ha sido expuesta en filtraciones de datos, útil para identificar posibles brechas.
6. 🌐 **Urlscan.io (Threat Intelligence):** Analiza sitios web en tiempo real, identificando comportamientos sospechosos y posibles amenazas.
7. 🚨 **Socradar.io (Threat Intelligence):** Monitorea la dark web y filtraciones de datos en busca de información relevante para tu organización.

8. 🚦 **GreyNoise.io:** Similar a Viz.greynoise.io, enfocado en analizar y comprender el ruido de internet.
9. 🧬 **VirusTotal.com:** Una plataforma esencial para analizar archivos, URLs, dominios y direcciones IP en busca de malware.
10. 👾 **Maltiverse.com:** Proporciona inteligencia detallada sobre malware, incluyendo su comportamiento y posibles impactos.
11. 🤝 **ThreatCrowd.org:** Una plataforma colaborativa donde los usuarios comparten información sobre amenazas, creando una base de datos de inteligencia colectiva.
12. 💡 **Pulsedive.com (Threat Intelligence):** Permite investigar Indicadores de Compromiso (IOCs) y comprender su contexto y relaciones.

III. Búsqueda de Código Fuente 💻

Para aquellos que necesitan analizar código en busca de vulnerabilidades o comprender la lógica de ciertas aplicaciones.

1. 💻 **Grep.app (Codes Search):** Un motor de búsqueda rápido y eficiente para encontrar código fuente en repositorios públicos.
2. 📜 **Searchcode.com (Codes Search):** Indexa código fuente de varias plataformas, permitiendo búsquedas detalladas.
3. **<0xF0><0x9F><0x93><0x80> Publicwww.com (Codes Search):** Busca menciones específicas de código fuente directamente en sitios web.

IV. Investigación de Vulnerabilidades y Exploits 💥

Mantente al tanto de las últimas vulnerabilidades y exploits disponibles.

1. 💥 **Vulners.com (Vulnerabilities):** Una base de datos completa de vulnerabilidades, con información detallada y referencias.
2. 💣 **Exploit-db.com:** El repositorio de exploits más conocido y utilizado por pentesters y profesionales de la seguridad.

V. Obtención de Información de Contacto 📧

Útil para investigaciones de OSINT y para contactar a responsables de seguridad.

1. 📧 **Hunter.io (Email Addresses):** Encuentra direcciones de correo electrónico asociadas a un dominio específico.

VI. Investigación en la Deep y Dark Web 🕵️

Para investigaciones más profundas que requieren explorar fuentes de información menos accesibles.

1. **Intelx.io (OSINT):** Un potente motor de búsqueda que indexa datos de fuentes públicas, incluyendo la deep y dark web.

VII. Análisis de Certificados SSL

Importante para comprender la infraestructura de seguridad de un sitio web.

1. **Crt.sh (Certificate Search):** Un proyecto de Sectigo que permite buscar certificados SSL emitidos para un dominio específico.

VIII. Análisis de Tráfico de Red

Para analizar archivos de captura de tráfico de red (PCAP).

1. **PacketTotal.com: Analiza archivos PCAP online, identificando patrones y posibles actividades maliciosas.**

IX. Análisis de URLs

Evalúa la seguridad y reputación de una URL.

1. **URLVoid.com: Analiza una URL a través de múltiples listas negras y servicios de reputación.**
2. **Urlscan.io (Threat Intelligence - Revisit):** Aunque categorizado en inteligencia de amenazas, también es excelente para un análisis detallado de URLs.

X. Información de Infraestructura de Internet

Para obtener detalles sobre la infraestructura subyacente de sitios web y servicios.

1. **SecurityTrails.com:** Proporciona información histórica y actual sobre DNS, WHOIS, direcciones IP y más.

XI. Análisis de Binarios y Malware <0xF0><0x9F><0xAA><0x9E>

Para un análisis más profundo de archivos ejecutables y malware.

1. **<0xF0><0x9F><0xAA><0x9E> BinaryDetective.com:** Permite analizar binarios y muestras de malware en busca de comportamientos sospechosos.

System Informer

Una herramienta gratuita, potente y polivalente que le ayuda a monitorear los recursos del sistema, depurar software y detectar malware.

https://systeminformer.com/