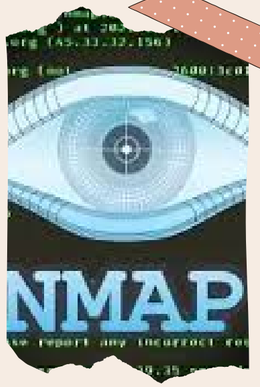
Conceptos de Vulnerabilidades

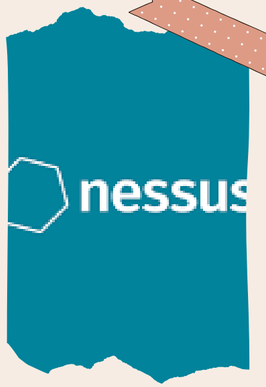
Edgar Daniel López Carbajal 7M LIDTS

Herramientas de Vulnerabilidades

Software para identificar debilidades en redes y sistemas.

Herramientas de vulnerabilidades





- **Nmap:** Escáner de red para descubrir dispositivos, puertos y evaluar la seguridad de sistemas.
- **Joomscan:** Analiza vulnerabilidades en sitios web basados en Joomla, ayudando a fortalecer su seguridad.
- **Wpscan:** Detecta debilidades en sitios web de WordPress, mejorando la protección contra posibles ataques.
- **Nessus Essentials:** Escáner de vulnerabilidades para identificar fallos de seguridad en sistemas y redes.
- **Vega:** Herramienta de prueba de seguridad web para encontrar vulnerabilidades en aplicaciones y sitios.


Inteligencia
Miscelaneo

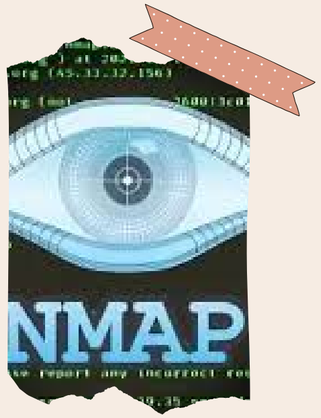
Inteligencia Misceláneo

- **Gobuster:** Herramienta de pruebas de seguridad que busca rutas ocultas en aplicaciones web mediante ataques de fuerza bruta.
- **Dumpster Diving:** Táctica de ingeniería social que busca información valiosa en desechos físicos para ataques.
- **Ingeniería Social:** Manipulación psicológica para obtener información confidencial o acceso no autorizado a sistemas.

Inteligencia Activa

Recopilación proactiva de información mediante acciones directas, como escaneo y búsqueda de vulnerabilidades.

Inteligencia Activa



Seleccionar objetivos

Direcciones o rangos IP, nombres de sistemas, redes, etc.

- Ejemplo: scanme.nmap.org, microsoft.com/24, 192.168.0.1, 10.0.0-255.1-254
- -iL fichero lista en fichero -iR n elegir objetivos aleatoriamente, 0 nunca acaba
- –exclude –excludefile fichero excluir sistemas desde fichero

- **Análisis de dispositivos y puertos con Nmap:** Uso de Nmap para descubrir y evaluar dispositivos y servicios en una red.
- **Parámetros y opciones de escaneo de Nmap:** Configuraciones personalizadas para adaptar el escaneo de Nmap a necesidades específicas.
- **Full TCP scan:** Escaneo exhaustivo de todos los puertos TCP de un dispositivo o red con Nmap.
- **Stealth Scan:** Escaneo sigiloso que busca minimizar detección al reducir actividad de red, realizado por Nmap.
- **Fingerprinting:** Técnica para identificar sistemas y aplicaciones mediante análisis de respuestas de red.
- **Zenmap:** Interfaz gráfica para Nmap que facilita visualización y análisis de resultados de escaneos.
- **Análisis traceroute:** Rastreo de ruta de paquetes para identificar nodos y demoras en comunicaciones de red.

Bibliografía

Molina Marin, Y y Orozco Nott, L. (2020). Vulnerabilidades de los Sistemas de Información: una revisión. Tecnológico de Antioquia, Institución Universitaria.

Choi, K., & Toro – Álvarez, M. Cibercriminología: Guía para la Investigación del Cibercrimen y Mejores Prácticas en Seguridad Digital1

KA, M. Aprendizaje análisis de malware2.

Toro, G. (n.d.). Guía de referencia de Nmap.