UNACH

FCA C1

Act. 1.1 Investigar los conceptos de vulnerabilidades

7 “M”

LIDTS

OPT 2. Análisis De Vulnerabilidades

Sub. 1

Alumno:

Marco Antonio Zúñiga Morales - A211121

Docente:

Dr. Luis Gutiérrez Alfaro

Tuxtla GTZ, Chiapas

26/Enero/2024

#1

HERRAMIENTAS DE VULNERABILIDADES

Nmap

Definición

Nmap (Network Mapper) es una herramienta de exploración de redes que identifica dispositivos y servicios, evaluando la seguridad de una red.

Usos

- Descubrimiento de hosts y servicios en una red.
- Auditoría de seguridad: identificación de vulnerabilidades y configuración de firewall.

Joomscan

Definición

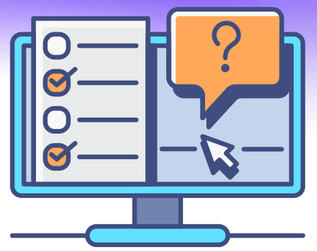
Joomscan es una herramienta especializada en escanear la seguridad de sitios web construidos con Joomla, un sistema de gestión de contenidos (CMS).

Usos

- Detección y evaluación de vulnerabilidades específicas de Joomla.
- Pruebas de penetración en sitios Joomla.

HERRAMIENTAS DE VULNERABILIDADES

Wpscan



Definición

Wpscan es una herramienta de seguridad enfocada en evaluar la seguridad de sitios web basados en WordPress.

Usos

- Escaneo de vulnerabilidades en sitios WordPress.
- Auditoría de seguridad y detección de configuraciones inseguras.

Nessus Essentials

Definición

Nessus Essentials es una herramienta de evaluación de vulnerabilidades que analiza sistemas y redes en busca de debilidades de seguridad.

Usos

- Identificación y evaluación de vulnerabilidades en sistemas y redes.
- Ayuda en el cumplimiento de políticas de seguridad.

HERRAMIENTAS DE VULNERABILIDADES

Vega

Definición

Vega es una herramienta de análisis de seguridad para aplicaciones web, detectando vulnerabilidades durante el desarrollo y pruebas de seguridad.

Usos

- Escaneo de aplicaciones web en busca de vulnerabilidades como inyecciones SQL o cross-site scripting (XSS).
- Pruebas de penetración y generación de informes detallados.

Herramientas de Vulnerabilidades

Definición

Las herramientas de vulnerabilidades son aplicaciones informáticas diseñadas para identificar debilidades y posibles riesgos en sistemas, redes y aplicaciones. Estas herramientas son esenciales en el análisis de seguridad, permitiendo a los profesionales evaluar y mejorar la postura de seguridad de un entorno informático.

INTELIGENCIA MISCELÁNEO

Gobuster

Definición

Gobuster es una herramienta de línea de comandos para buscar directorios y ficheros en aplicaciones web mediante fuerza bruta.

Usos

- Descubrimiento de directorios y archivos ocultos en servidores web.
- Identificación de puntos de acceso y vulnerabilidades en aplicaciones web.
- Evaluación de la superficie de ataque de una aplicación.

Dumpster Diving

Definición

Dumpster Diving es una técnica de ingeniería social que implica buscar información sensible en documentos impresos o desechos electrónicos.

Usos

- Recopilación de información confidencial descartada imprudentemente.
- Evaluación de la seguridad física de una organización.
- Concienciación sobre la gestión adecuada de información impresa y electrónica.

INTELIGENCIA MISCELÁNEO

Ingeniería Social

Definición

Ingeniería Social es manipular a personas para obtener información confidencial o inducir acciones que comprometan la seguridad.

Usos

- Obtención de credenciales de acceso mediante engaño.
- Pruebas de concienciación para evaluar la susceptibilidad de empleados.
- Complemento a evaluaciones de seguridad técnica al considerar el factor humano.

Inteligencia Misceláneo

Definición

Inteligencia Misceláneo se refiere a la recopilación y análisis de información diversa para obtener conocimientos en seguridad informática.

Usos

- Identificación de amenazas mediante análisis de datos dispersos.
- Obtención de información relevante para evaluar vulnerabilidades.
- Complemento a la inteligencia de amenazas convencional para comprender el panorama de riesgos.

INTELIGENCIA ACTIVA

Análisis de dispositivos y puertos con Nmap

Definición

Nmap es una herramienta de exploración de redes que analiza dispositivos y servicios, identificando puertos abiertos y otros detalles para evaluar la seguridad de una red.

Usos

- Descubrimiento de hosts y servicios en una red.
- Identificación de vulnerabilidades mediante análisis de puertos y servicios.
- Evaluación de la topología de red.

Parámetros opciones de escaneo de Nmap

Definición

Son configuraciones específicas utilizadas al ejecutar Nmap, que personalizan el comportamiento del escaneo según las necesidades del análisis.

Usos

- Adaptación del escaneo a diferentes entornos y requisitos de seguridad.
- Especificación de técnicas de escaneo, como escaneos rápidos o exhaustivos.

INTELIGENCIA ACTIVA

Full TCP scan

Definición

Es un tipo de escaneo completo en Nmap que verifica la conectividad de todos los puertos TCP en un host.

Usos

- Identificación exhaustiva de servicios y puertos abiertos.
- Evaluación completa de la superficie de ataque de un sistema.

Stealth SCAN

Definición

Es un escaneo en Nmap que busca minimizar la detección al reducir al máximo la interacción con el objetivo.

Usos

- Exploración sigilosa para evitar alertar a sistemas de seguridad.
- Útil en pruebas de penetración cuando se busca pasar desapercibido.

INTELIGENCIA ACTIVA

Fingerprintig

Definición

Fingerprinting implica identificar detalles específicos de un sistema, como su sistema operativo o versión de software, mediante análisis de las respuestas a ciertos estímulos.

Usos

- Identificación precisa de sistemas para adaptar estrategias de ataque o defensa.
- Obtención de información para análisis de vulnerabilidades.

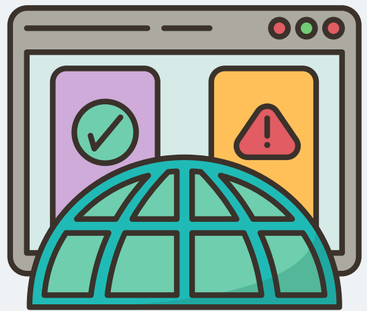
Zenmap

Definición

Zenmap es la interfaz gráfica de usuario para Nmap, proporcionando una representación visual de los resultados de los escaneos.

Usos

- Facilita la interpretación de los resultados de escaneos Nmap de manera gráfica.
- Permite análisis más intuitivos y detallados.



INTELIGENCIA ACTIVA

Análisis traceroute

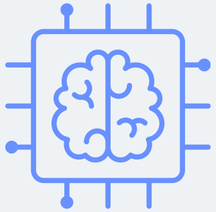
Definición

Traceroute es una herramienta que muestra la ruta que sigue un paquete de datos desde la fuente hasta el destino, revelando los nodos intermedios.

Usos

- Identificación de la ruta de la red y posibles puntos de fallo.
- Ayuda en la optimización de la red y la detección de dispositivos intermedios.

Inteligencia Activa



Definición

Se refiere a la recopilación de información mediante interacciones directas y exploratorias con sistemas o redes para comprender su estructura y detectar posibles vulnerabilidades.

Usos

- Identificación de activos y servicios en una red.
- Evaluación de la seguridad de sistemas mediante interacciones directas.
- Descubrimiento proactivo de vulnerabilidades.

REFERENCIA BIBLIOGRÁFICA

Mitnick, K. (2023). The Art of Deception: Controlling the Human Element of Security. Wiley.

Bazzell, M. (2023). The Art of Dumpster Diving. No Starch Press.

Riley, C. J. (2023). Gobuster: A Web Application Scanner. Chris John Riley.

Fedor. (2023). Nmap: The Network Mapper. Nmap Project. obtenido de https://nmap.org/

Joomscan Team. (2023). Joomscan: A Joomla Security Scanner. Joomscan Team.

Jacobson, V. (1988). Traceroute: A Tool for Finding the Route of a Packet Through a Network. University of California, Berkeley.

Qualys. (2023). Vega: A Web Application Security Scanner. Qualys.

WPScan Team. (2023). WPScan: A WordPress Security Scanner. WPScan Team.

Tenable Network Security. (2023). Nessus Essentials. Tenable Network Security.