

Presentacion

ACT. 1.1 INVESTIGAR LOS CONCEPTOS DE

VULNERABILIDADES:

Steven de Dios Montoya Hernández

7*M

HERRAMIENTAS DE VULNERABILIDADES:

- nmap
- Joomscan
- Wpscan
- Nessus Essentials
- Vega



Herramientas de vulnerabilidades:

NMAP:

Descripción: Nmap es una herramienta de código abierto que se utiliza para descubrir hosts y servicios en una red, así como para crear un mapa de la red.

Funciones: Escaneo de puertos, detección de servicios, detección de sistemas operativos, entre otros.

Uso típico: Identificar dispositivos en una red, encontrar puertos abiertos, evaluar la seguridad de una red.

JoomScan:

Descripción: JoomScan es una herramienta diseñada para escanear y enumerar vulnerabilidades en sitios web que utilizan el sistema de gestión de contenidos Joomla.

Funciones: Identificación de versiones de Joomla, escaneo de vulnerabilidades específicas de Joomla.

Uso típico: Evaluación de la seguridad de sitios web basados en Joomla.

WPScan:

Descripción: WPScan es una herramienta de escaneo de seguridad diseñada para buscar vulnerabilidades en sitios web que utilizan WordPress.

Funciones: Identificación de versiones de WordPress, escaneo de plugins y temas, búsqueda de vulnerabilidades conocidas.

Uso típico: Evaluación de la seguridad de sitios web basados en WordPress.

Nessus Essentials:

Descripción: Nessus es una herramienta de escaneo de vulnerabilidades que identifica y evalúa posibles amenazas en sistemas y redes.

Funciones: Escaneo de vulnerabilidades, evaluación de políticas de seguridad, generación de informes detallados.

Uso típico: Auditar la seguridad de sistemas y redes, identificar y corregir vulnerabilidades.

Vega:

Descripción: Vega es una herramienta de prueba de seguridad de aplicaciones web que realiza escaneos automáticos en busca de vulnerabilidades.

Funciones: Escaneo de aplicaciones web en busca de vulnerabilidades, análisis de seguridad, generación de informes.

Uso típico: Evaluación de la seguridad de aplicaciones web, identificación de posibles problemas de seguridad.

INTELIGENCIA MISCELÁNEO.

- Gobuster:
- Dumpster Diving
- Ingeniería Social



INTELIGENCIA MISCELÁNEO.

GOBUSTER:

- **Descripción:** Gobuster es una herramienta de línea de comandos utilizada para realizar ataques de fuerza bruta o diccionario contra varios puntos finales, como URLs o rutas de directorios.
 - **Funciones:** Descubrimiento de directorios y archivos ocultos, enumeración de recursos disponibles en un servidor web.
 - **Uso típico:** Identificación de posibles puntos de entrada o vulnerabilidades en una aplicación web mediante la búsqueda de directorios o archivos no autorizados.

DUMPSTER DIVING:

- Descripción: Dumpster Diving se refiere a la práctica de buscar información sensible o valiosa en la basura o en desechos de una organización. En el contexto de seguridad, esto implica buscar documentos impresos, discos duros, o cualquier otro material desecharido que pueda contener información confidencial.
 - Funciones: Recopilación de información confidencial, como contraseñas, documentos internos, o cualquier otra información valiosa que haya sido desecharida.
 - Uso típico: Puede ser parte de una estrategia de ingeniería social, donde un atacante busca información física o digital en la basura de una organización con el objetivo de obtener acceso no autorizado o realizar actividades maliciosas.



INGENIERÍA SOCIAL:

Consectetur

adipiscing

elit,

sed

do eiusmod tempor

incididunt ut labore

et dolore magna

aliqua.

Ut enim ad

minim veniam,

quis

nostrud exercitation

ullamco laboris nisi

ut aliquip ex ea

commodo

consequat.

INTELIGENCIA ACTIVA:



Inteligencia Activa

- Análisis de dispositivos y puertos con Nmap
- Parámetros y opciones de escaneo de nmap
- Full TCP scan
- Stelth Scan
- Fingerprinting
- Zenmap
- Análisis traceroute

INTELIGENCIA ACTIVA:

Análisis de dispositivos y puertos con Nmap

Descripción: Nmap puede utilizarse para identificar qué puertos están abiertos en un dispositivo o servidor remoto.

Funciones: Descubrimiento de servicios en ejecución y evaluación de la superficie de ataque.

Uso Típico: Identificación de servicios en un servidor para evaluar la seguridad y posibles vulnerabilidades.

Parametros opciones de escaneo de nmap

- Descripción: Especifica los puertos a escanear.
- Funciones: Limita el escaneo a puertos específicos, reduciendo el tiempo y la carga de red.
- Uso Típico: nmap -p 80,443 ejemplo.com escanea solo los puertos 80 y 443 en el host ejemplo.com.

Stelth Scan

Descripción:

Un Escaneo Stealth, también conocido como escaneo silencioso, es una técnica de exploración de puertos que busca minimizar la detección al no completar completamente la conexión con el objetivo. El escaneo stealth es comúnmente asociado con el escaneo SYN (paquetes SYN).

Full TCP scan

Descripción:

Un Escaneo TCP Completo, también conocido como escaneo completo de puertos TCP, es una técnica exhaustiva que implica sondear los 65,535 puertos TCP en un sistema objetivo. Este tipo de escaneo tiene como objetivo identificar los servicios en ejecución en cada puerto, proporcionando una evaluación completa de la superficie de ataque del objetivo.

Funciones:

Identificación Exhaustiva de Puertos: El Escaneo TCP Completo intenta identificar todos los puertos TCP abiertos en el sistema objetivo.

Enumeración de Servicios: Ayuda a enumerar los servicios asociados con cada puerto abierto.

Mapeo de la Superficie de Ataque: Proporciona un mapa detallado de la superficie de ataque del objetivo al revelar todos los puertos TCP accesibles.

INTELIGENCIA ACTIVA:

Fingerprinting

Descripción:

El Fingerprinting (identificación de huellas) con Nmap se refiere al proceso de intentar determinar el sistema operativo y, en algunos casos, la versión del software que se ejecuta en un objetivo mediante el análisis de las respuestas a paquetes de red.

Funciones:

Detección de Sistema Operativo: Nmap utiliza patrones específicos de respuestas a paquetes para inferir el sistema operativo del objetivo.

Identificación de Versiones: En algunos casos, Nmap puede intentar identificar la versión del software específico que está en ejecución en un puerto abierto.

Ajuste de Políticas de Seguridad: Proporciona información valiosa para ajustar las estrategias de seguridad y configuraciones de red.

Zenmap

Descripción:

Zenmap es la interfaz gráfica de usuario (GUI) para Nmap, una poderosa herramienta de escaneo de red y evaluación de seguridad. Zenmap facilita la configuración y ejecución de escaneos de red, así como la visualización de los resultados en un formato gráfico e intuitivo.

Funciones:

Interfaz Gráfica Intuitiva: Proporciona una interfaz gráfica fácil de usar, lo que facilita la realización de escaneos incluso para usuarios menos familiarizados con la línea de comandos.

Configuración de Escaneos: Permite la configuración de parámetros de escaneo a través de menús desplegables y opciones gráficas.

Visualización de Resultados: Muestra los resultados del escaneo en un formato visual, con gráficos y tablas que resumen la información de manera accesible.

Comparación de Escaneos: Facilita la comparación de resultados de escaneos anteriores para evaluar cambios en la red.

Análisis traceroute

Descripción:

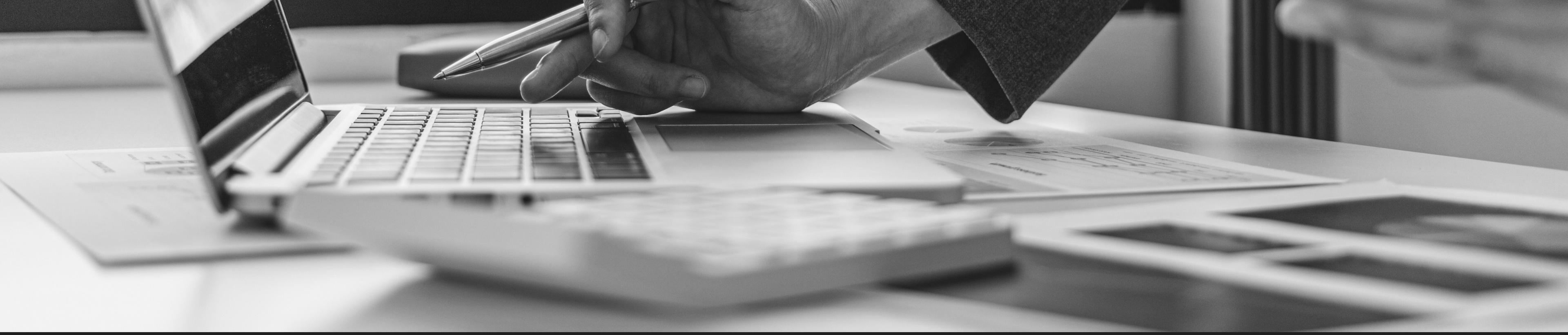
Nmap puede realizar análisis de traceroute como parte de sus funciones de escaneo de red. El análisis de traceroute implica rastrear la ruta que los paquetes toman desde el punto de origen hasta el destino, mostrando los saltos entre routers en la red.

Funciones:

Visualización de Ruta de Paquetes: Muestra los nodos (routers) a través de los cuales los paquetes pasan para llegar al destino.

Identificación de Saltos: Permite identificar el número de saltos y la dirección IP de cada router en la ruta.

Diagnóstico de Latencia: Proporciona información sobre el tiempo de respuesta de cada salto, lo que puede ayudar en la identificación de posibles cuellos de botella o problemas de latencia en la red.



BIBLIOGRAFIA

"Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning"

Autor: Gordon Fyodor Lyon

Año: 2009

"Hacking: The Art of Exploitation"

Autor: Jon Erickson

Año: 2008

"Network Warrior: Everything you need to know that wasn't on the CCNA exam"

Autor: Gary A. Donahue

Año: 2011

"The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws"

Autores: Dafydd Stuttard, Marcus Pinto

Año: 2011

"Metasploit: The Penetration Tester's Guide"

Autores: David Kennedy, Jim O'Gorman, Devon Kearns, Mati Aharoni

Año: 2011