



UNIVERSIDAD AUTONOMA DE CHIAPAS

LICENCIATURA EN INGENIERIA EN DESARROLLO DE
TECNOLOGIAS DE SOFTWARE

CONCEPTOS DE **VULNERABILIDAD**

MATERIA: ANALISIS DE VULNERABILIDADES
ALUMNO: TOMÁS ÁLVAREZ GÓMEZ

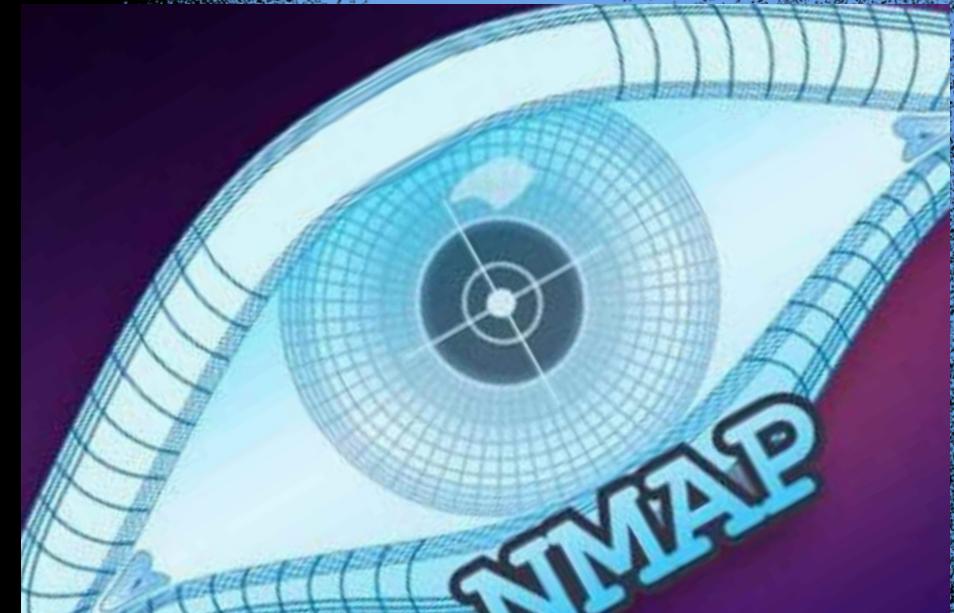
HERRAMIENTAS DE VULNERABILIDAD



N M A P

Es una herramienta de código abierto creada en 1998 que es muy reconocida en el mundo de informática por su funcionalidad de escaneo de redes, puertos y servicios que ha ido mejorando con el correr de los años.

Es de gran utilidad para identificar los dispositivos conectados a una red y obtener información de los mismos, como pueden ser aplicaciones instaladas, puertos y servicios abiertos y posibles vulnerabilidades de seguridad.



Mediante la ejecución de algunos scripts nos permite escanear una red en busca de vulnerabilidades. Por ejemplo:

- Auth: ejecuta todos sus scripts disponibles para autenticación
- Default: ejecuta los scripts básicos por defecto de la herramienta
- Discovery: recupera información del target o víctima
- External: script para utilizar recursos externos
- Intrusive: utiliza scripts que son considerados intrusivos para la víctima
- Indicios de la presencia de malware: revisa si hay conexiones abiertas por códigos maliciosos o backdoors
- Safe: ejecuta scripts que no son intrusivos
- Vuln: descubre las vulnerabilidades más conocidas
- All: ejecuta absolutamente todos los scripts con extensión NSE disponibles

JOOMSCAN

Escáner de seguridad Joomscan es una herramienta de auditoría de sitios web para Joomla. Está escrito en Perl y es capaz de detectar más de 550 vulnerabilidades como inclusiones de archivos, inyecciones de SQL, Defectos de RFI, BIA, Defecto XSS, inyección ciega de SQL, protección de directorios y otros.

Las principales características de Joomscan

- Detección de versiones de Joomla.
- Detección y enumeración de componentes, complementos y módulos vulnerables.
- Publicar una nota defensiva para proteger adecuadamente su sitio web.

(_____) (_____) (_____) (_____) / (_____) / (_____) / (_____) \ (_____)
(_____) (_____) (_____) (_____) (_____) (_____) (_____) (_____) (_____) (_____) (_____) (_____)
(_____) (_____) (_____) (_____) (_____) (_____) (_____) (_____) (_____) (_____) (_____) (_____)
1337.today

```
--=[OWASP JoomScan
+---+---+=[Version : 0.0.7
+---+---+=[Update Date : [2018/09/23]
+---+---+=[Authors : Mohammad Reza Espargham , Ali Razmjoo
--=[Code name : Self Challenge
```



WPScan

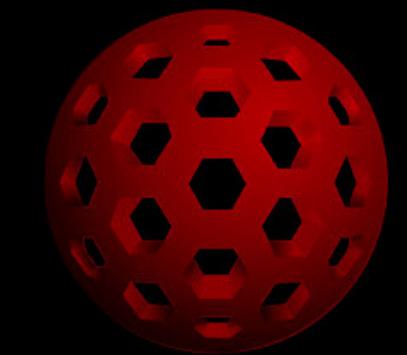
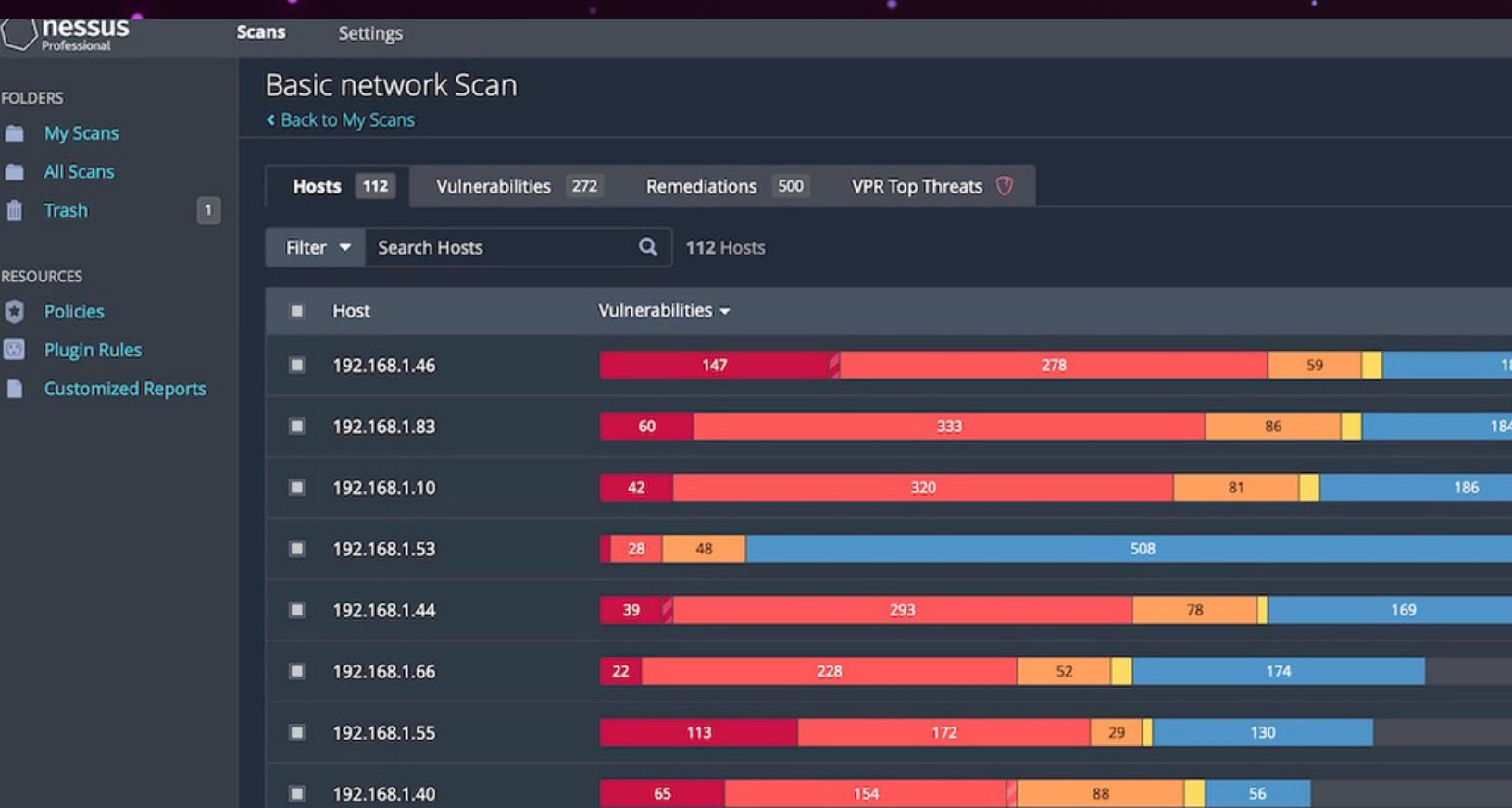
Es una herramienta muy útil para comprobar las vulnerabilidades y puntos débiles de tu sitio Wordpress. Las irregularidades y problemas en Wordpress cada vez son más comunes. Así podemos decir que es un plugin pero que no elimina los objetos sospechosos, sino que ayuda al usuario a identificarlos para eliminarlos por completo. Usa la base de datos de wpvulndb.com y va sumando nuevas vulnerabilidades a su lista.

WPSCAN

NESSUS ESSENTIALS

Es una herramienta utilizada principalmente para escanear vulnerabilidades, es desarrollada y mantenida por Tenable.

Tiene un motor para escanear los objetivos que se basa en plugins; los plugins son pequeños programas escritos en un lenguaje de scripting denominado Nessus Attack Scripting Language (NASL) que le indican al motor que es lo que debe evaluar en el objetivo, con el fin de determinar las fallas del mismo.



VEGA

Vega es una herramienta gráfica de auditoría web gratuita y de código abierto. Esta herramienta realiza diversas funciones tales como:

- Análisis de Vulnerabilidades
- Crawler (copia del sitio web)
- Análisis de contenido
- Modificación manual de paquete HTTP (proxy)

La herramienta tiene módulos para realizar ataques típicos del OWASP como XSS, SQL Injection, Directorio transversal, URL Injection, detección de errores, etc.

VEGA

INTELIGENCIA MISCELÁNEO



G O B U S T E R

Gobuster es una herramienta utilizada para realizar fuerza bruta a: URLs (directorios y archivos) en sitios web, subdominios DNS (con soporte de comodines), y nombres de hosts virtuales en los servidores web.

Gobuster tiene tres modos disponibles. "dir", el modo clásico de fuerza bruta contra directorios, "dns", el modo de fuerza bruta contra subdominios DNS, y "vhost", el modo de fuerza bruta contra hosts virtuales (no es lo mismo a "DNS").



DUMPSTER DIVING

```
root@kali:~# gobuster help
Usage:
gobuster [command]

Available Commands:
dir      Uses directory/file bruteforcing mode
dns      Uses DNS subdomain bruteforcing mode
help     Help about any command
vhost    Uses VHOST bruteforcing mode

Flags:
-h, --help          help for gobuster
-z, --noprogress   Don't display progress
-o, --output string Output file to write results to (defaults to stdout)
-q, --quiet         Don't print the banner and other noise
-t, --threads int  Number of concurrent threads (default 10)
-v, --verbose       Verbose output (errors)
-w, --wordlist string Path to the wordlist

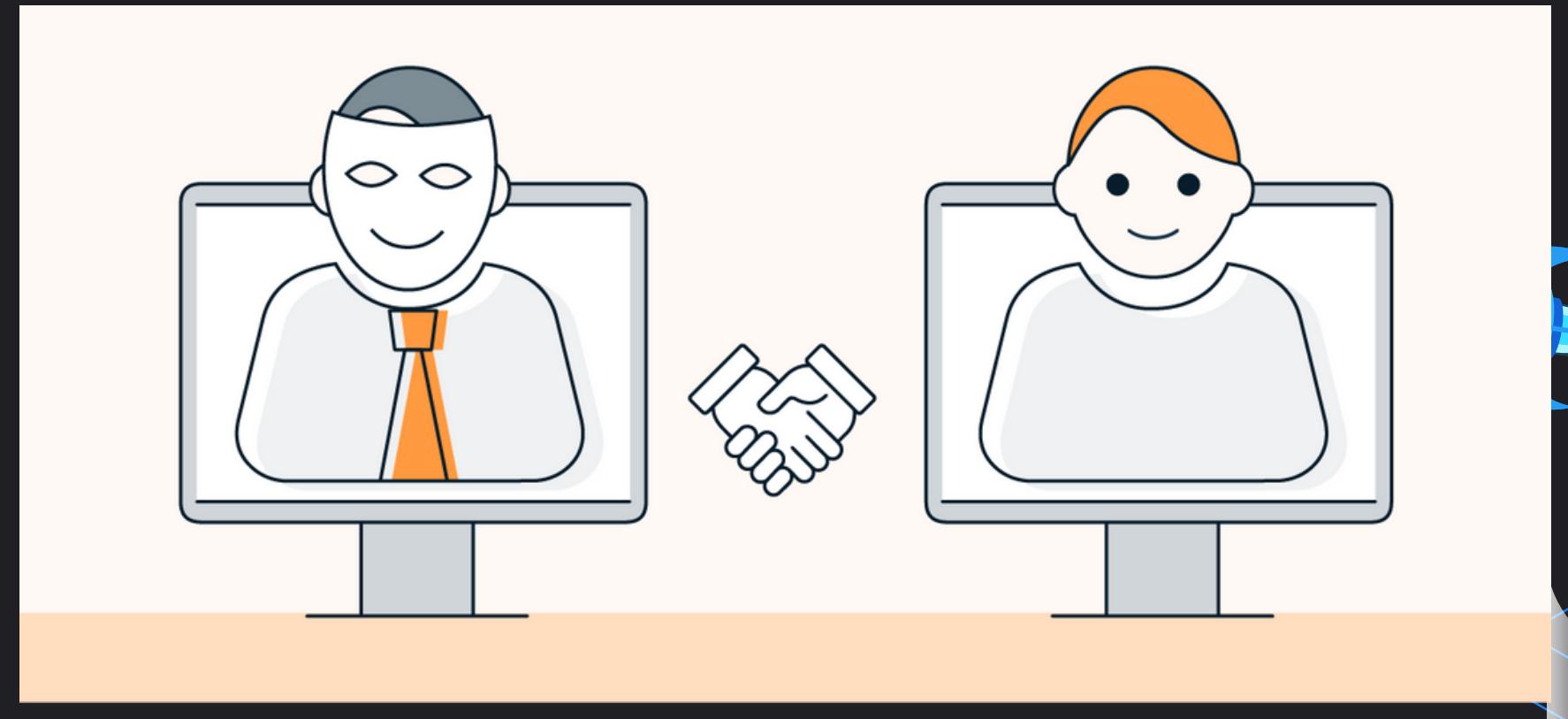
Use "gobuster [command] --help" for more information about a command.
root@kali:~#
```

Dumpster Diving es el acto de acceder sin autorización a determinada información que pasa por la basura de una empresa, ya sea dentro o fuera del edificio. El atacante generalmente busca algún tipo de información confidencial que se arrojó a la basura. La información de secreto comercial debe eliminarse adecuadamente.

DUMPSTER
DIVING

INGENIERIA SOCIAL

La ingeniería social es un conjunto de técnicas que usan los cibercriminales para engañar a los usuarios incautos para que les envíen datos confidenciales, infecten sus computadoras con malware o abran enlaces a sitios infectados. Además, los hackers pueden tratar de aprovecharse de la falta de conocimiento de un usuario; debido a la velocidad a la que avanza la tecnología, numerosos consumidores y trabajadores no son conscientes del valor real de los datos personales y no saben con certeza cuál es la mejor manera de proteger esta información.



INTELIGENCIA ACTIVA



ANÁLISIS DE DISPOSITIVOS Y PUERTOS CON NMAP

Este tipo de ataque también se conoce como port scan. Básicamente lo que hace un atacante es analizar de forma automática todos los puertos de un equipo, como por ejemplo un ordenador, que esté conectado a la red. Lo que buscan es detectar posibles puertos abiertos y cuáles podrían tener protocolos de seguridad deficientes. Una vez logran toda la información posible podrían detectar posibles agujeros de seguridad y llevar a cabo así sus ataques.

PARÁMETROS Opciones DE ESCANEO DE NMAP

1. -sS o -sT: Escaneo TCP SYN o TCP Connect. El primero envía paquetes SYN para detectar puertos abiertos, mientras que el segundo realiza una conexión completa.
2. -sU: Escaneo UDP. Permite detectar servicios que utilizan UDP en lugar de TCP.
3. -p: Especifica los puertos a escanear. Puedes utilizar rangos (por ejemplo, -p 1-100) o una lista separada por comas (por ejemplo, -p 80,443).
4. -A: Habilita detección de versión, script de detección de servicios y escaneo de sistemas operativos.
5. -O: Intenta adivinar el sistema operativo de los dispositivos en la red.
6. --script: Permite especificar scripts de NSE (Nmap Scripting Engine) para realizar tareas como detección de vulnerabilidades.
7. -v, -vv, -vvv: Controla el nivel de verbosidad de la salida. -v es para nivel bajo, -vv es para nivel medio y -vvv es para nivel alto.
8. -oN, -oX, -oG: Estos parámetros permiten especificar el formato de salida del escaneo. -oN genera una salida normal en texto plano, -oX genera una salida en formato XML y -oG genera una salida en formato "grepable".
9. -iL: Permite especificar un archivo con una lista de objetivos en lugar de pasarlos en línea de comandos.
10. --exclude: Excluye hosts o rangos de hosts específicos de ser escaneados.
11. --scan-delay y --max-retries: Controla el retardo entre escaneos y el número máximo de reintentos.

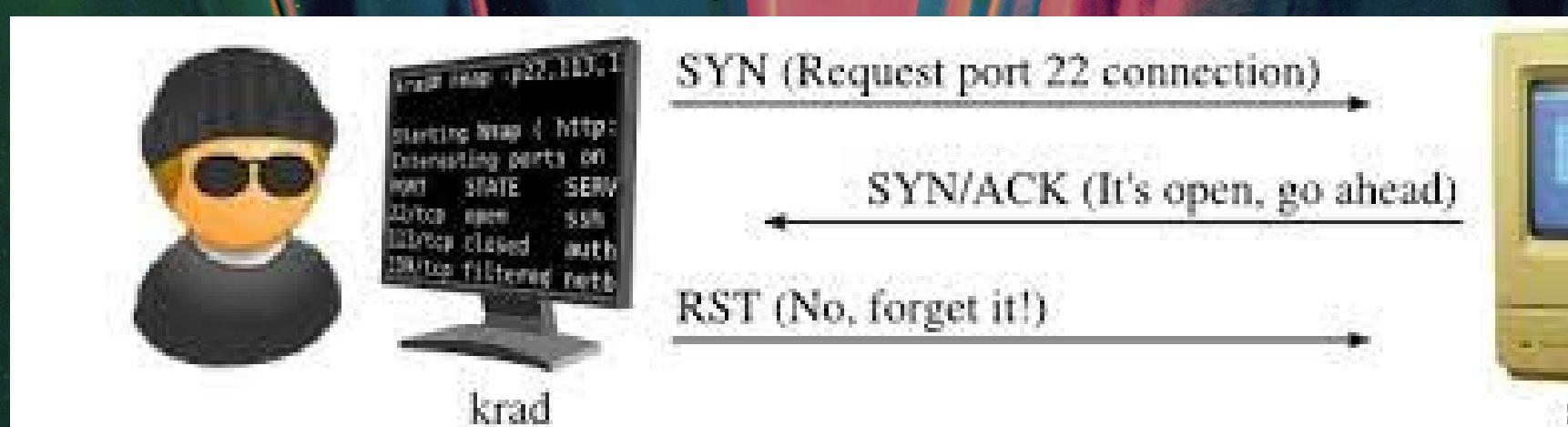
FULL TCP SCAN

Un "Full TCP Scan" es un término no oficial que a menudo se usa para referirse a un escaneo exhaustivo de todos los puertos TCP en un objetivo. En el contexto de Nmap, puedes lograr esto utilizando el parámetro `-p-`, que escaneará todos los 65535 puertos TCP posibles en el rango.

Ejemplo

```
nmap -p- <objetivo>
```

Reemplaza `<objetivo>` con la dirección IP o el nombre de host del objetivo que deseas escanear. Ten en cuenta que un escaneo de todos los puertos puede ser intensivo en recursos y tiempo, y también podría ser considerado inapropiado en algunas redes sin permiso adecuado.



STEALTH SCAN

El término "Stealth Scan" se refiere a un tipo específico de escaneo de puertos en el que el escáner intenta ser lo más discreto posible, evitando que el objetivo detecte el escaneo. El objetivo principal de un "Stealth Scan" es recopilar información sobre los puertos abiertos y servicios en una red sin alertar a los sistemas de seguridad o a los registros de actividad.

En Nmap, uno de los métodos comunes para realizar un "Stealth Scan" es utilizando el escaneo TCP SYN (síncrono). En este escaneo, el escáner envía paquetes SYN al objetivo y analiza las respuestas para determinar qué puertos están abiertos. El objetivo no establece una conexión completa, lo que puede dificultar la detección del escaneo.

FINGERPRINTING

El "fingerprinting" (identificación de huellas o perfiles) se refiere al proceso de recopilar información detallada sobre un sistema o servicio específico en una red para determinar su versión, configuración y otros detalles relevantes. Esto se hace a menudo con el objetivo de identificar las vulnerabilidades y posibles puntos débiles en un sistema para fines de análisis de seguridad.

En el contexto de la seguridad informática y las pruebas de penetración, el "fingerprinting" puede implicar el uso de diversas técnicas para obtener información sobre el sistema objetivo:



1. Fingerprinting de sistemas operativos: Se intenta determinar el sistema operativo que se ejecuta en el objetivo. Esto se puede hacer mediante el análisis de las respuestas de los paquetes de red, los tiempos de respuesta y otros comportamientos.
2. Fingerprinting de servicios: Se busca determinar las versiones y configuraciones de los servicios que se ejecutan en el objetivo, como servidores web, bases de datos y otros servicios de red. Esto puede ayudar a identificar vulnerabilidades específicas asociadas con versiones conocidas.
3. Fingerprinting de aplicaciones: Se enfoca en identificar las aplicaciones y servicios específicos que se ejecutan en el objetivo, incluyendo versiones y características específicas.
4. Fingerprinting de protocolos: Implica analizar el comportamiento de los protocolos de red utilizados en el objetivo para identificar detalles específicos sobre cómo se implementan.
5. Fingerprinting pasivo: Implica observar y analizar el tráfico de red sin interactuar directamente con el objetivo. Esto puede incluir análisis de paquetes capturados para identificar los sistemas y servicios en uso.

ZENMAP

Zenmap es una interfaz gráfica de usuario (GUI) para Nmap (Network Mapper), que es una herramienta de código abierto utilizada para el escaneo de redes y la detección de dispositivos y servicios en una red. Zenmap proporciona una manera más visual y amigable de utilizar Nmap, lo que hace que la configuración y ejecución de escaneos sea más accesible para usuarios menos familiarizados con la línea de comandos.

Algunas características clave de Zenmap incluyen:

1. Interfaz gráfica: Zenmap ofrece una interfaz gráfica fácil de usar con una variedad de opciones y configuraciones que se pueden ajustar con clics de ratón.
2. Visualización de resultados: Los resultados del escaneo se presentan de manera gráfica en forma de tablas y gráficos, lo que facilita la interpretación de la información.
3. Escaneos preconfigurados: Zenmap proporciona perfiles preconfigurados para escaneos comunes, como el escaneo rápido y el escaneo completo de TCP.
4. Personalización de escaneos: Aunque Zenmap está diseñado para ser más accesible, aún permite personalizar y ajustar las opciones de escaneo según las necesidades del usuario.
5. Guardar y cargar configuraciones: Puedes guardar configuraciones de escaneo frecuentes para usarlas nuevamente en el futuro y cargar configuraciones anteriores.
6. Comparación de escaneos: Zenmap permite comparar los resultados de diferentes escaneos para identificar cambios en la red con el tiempo.
7. Visualización de topologías: Puede representar gráficamente la topología de la red, mostrando relaciones entre dispositivos y cómo están conectados.

ANÁLISIS TRACEROUTE

El análisis de "traceroute" es una técnica utilizada para rastrear la ruta que sigue un paquete de datos a través de una red, desde el origen hasta el destino. Esta técnica es útil para entender cómo se enrutan los datos a través de diferentes dispositivos y nodos en Internet y para identificar posibles problemas de latencia o congestión en la red.

En un análisis "traceroute", se envían una serie de paquetes de datos (por lo general, paquetes ICMP o UDP) con incrementos en el campo de tiempo de vida (TTL) en los encabezados IP. Cada vez que un paquete alcanza un enrutador o nodo en la ruta, el TTL disminuye en uno. Cuando el TTL llega a cero, el dispositivo descarta el paquete y envía un mensaje de error de "Time Exceeded" al origen. De esta manera, el origen puede construir una lista de todos los nodos que ha atravesado el paquete hasta llegar al destino.

```
C:\Users\Bhishu>tracert 8.8.8.8
```

```
Tracing route to dns.google [8.8.8.8]  
over a maximum of 30 hops:
```

1	3 ms	1 ms	1 ms	192.168.101.1
2	4 ms	2 ms	3 ms	103.41.174.145
3	5 ms	2 ms	2 ms	103.41.174.140
4	5 ms	2 ms	3 ms	103.10.28.34
5	3 ms	3 ms	3 ms	ae0-bg2.vianet.com.np
6	8 ms	6 ms	7 ms	125.19.67.33
7	48 ms	39 ms	44 ms	116.119.106.142
8	47 ms	46 ms	45 ms	142.250.169.206
9	270 ms	70 ms	70 ms	142.250.209.73
10	54 ms	54 ms	53 ms	142.251.55.75
11	53 ms	53 ms	54 ms	dns.google [8.8.8.8]