



# ACT. 1.1

Bryan Andrew Castro Valencia  
Universidad Autonoma De Chiapas  
Facultad de Contaduria y Administacion I  
7M LITDS  
8/8/23

# Herramientas de vulnerabilidades:

- nmap
- Joomscan
- Wpscan
- Nessus Essentials
- Vega



# nmap

NMAP (Network Mapper) es un software de código abierto que se utiliza para escanear una red y sus puertos con el objetivo de obtener información importante sobre la misma para controlar y gestionar su seguridad. Es una aplicación que se utiliza normalmente para realizar auditorías de seguridad y monitoreo de redes. Sus funciones principales son:

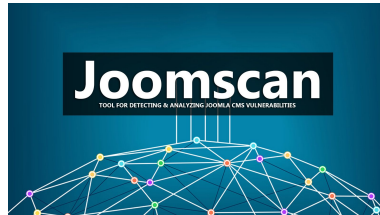
- Mapear una red
- Identificar servicios en ejecución
- Realizar una auditoría de seguridad
- Detectar sistemas operativos



# Joomscan

Joomscan es un escáner de vulnerabilidades en la red utilizado para detectar la ejecución de comandos, inyección SQL y otros ataques contra aplicaciones web. Como sugiere su nombre, Joomscan escanea sitios web creados con Joomla. Joomscan localiza las carpetas navegables, localiza cada archivo para identificar la versión de un componente instalado.

- Detectar el firewall y los archivos de registro y respaldo comunes.
- Enumerar los componentes instalados y las vulnerabilidades conocidas asociadas a ellos.



# Wpscan

WPScan es un software de código abierto para Kali Linux, diseñado para escanear vulnerabilidades y fallos en un sitio web de WordPress.

WPScan es una herramienta muy poderosa y capaz de darte información detallada sobre una página web. Con ella, puedes auditar sistemas, verificar su estado y corregir cada fallo que encuentres antes de que lo aproveche un delincuente.



**WPScan**

# Nessus Essentials

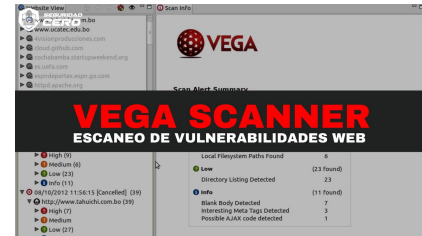
Nessus es un programa de escaneo de vulnerabilidades en diversos sistemas operativos. Consiste en un demonio o diablo, `nessusd`, que realiza el escaneo en el sistema objetivo, y `nessus`, el cliente (basado en consola o gráfico) que muestra el avance e informa sobre el estado de los escaneos. Desde consola `nessus` puede ser programado para hacer escaneos programados con `cron`.

En operación normal, `nessus` comienza escaneando los puertos con `nmap` o con su propio escáner de puertos para buscar puertos abiertos y después intentar varios exploits para atacarlo.

# Vega

Vega es un analizador de vulnerabilidades Open Source que está en su versión 1.0 que nos permite realizar las siguientes funciones:

- Análisis de vulnerabilidades
- Realización de un crawler(copia del sitio web)
- Análisis de contenido
- Modificación manual de paquete HTTP gracias a un proxy.



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

# Inteligencia Misceláneo.

- Gobuster:
- Dumpster Diving
- Ingeniería Social



# Gobuster

Gobuster es útil para pentesters, hackers éticos y expertos en forense. También se puede usar para pruebas de seguridad. Está escrito en lenguaje Go y es más rápido y eficiente que otras herramientas similares.

se usa para hacer fuerza bruta de:

- URIs (directorios y archivos) en sitios web.
- Subdominios DNS (con soporte de comodines).
- Nombres de host virtuales en servidores web objetivo.
- Buckets abiertos de Amazon S3 y Google Cloud.
- Servidores TFTP.

# Dumpster Diving

Dumpster diving es una vulnerabilidad que consiste en buscar información sensible en la basura de una víctima, ya sea física o digitalmente. Es un tipo de ataque que no requiere de habilidades o herramientas técnicas especiales, y que puede ser usado por diferentes actores, como profesionales de la ciberseguridad, agentes de la ley, periodistas o hackers. El objetivo de este ataque es obtener datos que puedan ser usados para lanzar otros ataques más sofisticados, como ingeniería social o robo de identidad.



# Ingenieria Social

La ingeniería social es una forma de ataque que se basa en la manipulación psicológica de las personas para que revelen información confidencial, descarguen malware, accedan a sitios web maliciosos o realicen otras acciones que comprometan su seguridad o la de sus organizaciones. Los ingenieros sociales se aprovechan de las vulnerabilidades humanas, como la curiosidad, el miedo, la confianza, la urgencia o la autoridad, para engañar a sus víctimas y hacerles creer que están actuando en su propio beneficio o en el de alguien más.



# Inteligencia Activa

La inteligencia activa de vulnerabilidades es un proceso que consiste en recopilar, analizar y utilizar información sobre los sistemas, redes y aplicaciones de un objetivo para identificar y explotar sus debilidades.

- Descubrir los dispositivos y servicios que se ejecutan en una red, así como sus versiones, configuraciones y dependencias.
- Detectar las vulnerabilidades existentes en los sistemas y aplicaciones del objetivo
- Realizar ataques simulados o reales contra el objetivo, utilizando las técnicas y herramientas adecuadas para cada caso.

# Parametros opciones de escaneo de nmap

- sT: Realiza un escaneo TCP conectado, que establece una conexión completa con cada puerto objetivo y determina su estado
- sS: Realiza un escaneo TCP SYN, que envía un paquete SYN a cada puerto objetivo y espera una respuesta. Si recibe un paquete SYN/ACK, el puerto está abierto. Si recibe un paquete RST, el puerto está cerrado.
- sU: Realiza un escaneo UDP, que envía un paquete UDP a cada puerto objetivo y espera una respuesta. Si recibe un paquete ICMP de tipo 3 y código 3, el puerto está cerrado.
- sV: Realiza una detección de servicios y versiones, que intenta identificar el nombre y la versión del servicio que se ejecuta en cada puerto abierto.

# Full TCP Scan

Un Full TCP scan es un tipo de escaneo de puertos que consiste en establecer una conexión TCP completa con cada puerto objetivo y determinar su estado (abierto, cerrado o filtrado). Es el tipo de escaneo más fiable, pero también el más fácil de detectar por los sistemas de defensa.

- Envía un paquete SYN y espera una respuesta. Si recibe un SYN/ACK, el puerto está abierto. Si recibe un RST, el puerto está cerrado. Si no recibe nada, el puerto está filtrado.
- Se puede hacer con Nmap usando la opción -sT o sin ninguna opción.

# Stealth Scan

Un Stealth Scan es un tipo de escaneo de puertos que consiste en enviar un paquete SYN (solicitud de conexión) a cada puerto objetivo y esperar una respuesta, sin completar la conexión TCP. Algunos de sus puntos importantes son:

- Es un método rápido y sigiloso para detectar los puertos abiertos, cerrados o filtrados de un objetivo.
- Es menos detectable que un escaneo TCP normal, ya que no genera tantos registros ni alertas en el sistema objetivo.

# Fingerprinting

El fingerprinting es un tipo de rastreo en línea que es más invasivo que el rastreo basado en cookies. Consiste en crear un perfil único de un usuario basado en las características de su hardware, software, complementos y preferencias

- Permite identificar y seguir a un usuario sin su consentimiento ni conocimiento, violando su privacidad y seguridad.
- Puede usarse para fines maliciosos, como robar información personal, mostrar publicidad personalizada o realizar ataques dirigidos.
- Es difícil de evitar o bloquear, ya que no depende de elementos externos como las cookies, sino de los propios datos del dispositivo o navegador del usuario.



# Zenmap

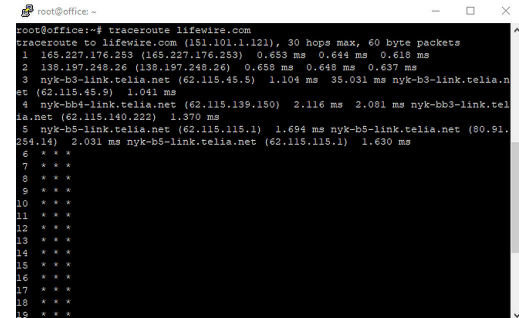
Zenmap es una interfaz gráfica de usuario (GUI) para el escáner de seguridad Nmap, que es una herramienta de código abierto para explorar, auditar y visualizar redes.

- Permite realizar escaneos de red con diferentes opciones y perfiles, usando una interfaz sencilla e intuitiva.
- Muestra los resultados de los escaneos en diferentes formatos, como tablas, listas, mapas o gráficos.
- Permite guardar y comparar los resultados de los escaneos, así como buscar y filtrar la información obtenida.

# Traceroute

Un análisis traceroute es un proceso que consiste en rastrear la ruta que siguen los paquetes de datos desde un origen hasta un destino en Internet, mostrando los saltos o nodos intermedios y el tiempo que tardan en llegar a cada uno.

- Diagnosticar problemas de conexión o rendimiento en la red, identificando posibles puntos de falla, congestión o retraso.
- Obtener información sobre la estructura y la topología de la red, como el número y el tipo de dispositivos, servicios y protocolos involucrados.
- Evaluar la seguridad y la vulnerabilidad de la red, detectando posibles ataques, filtrados o suplantaciones.



```
root@office:~# traceroute lifewire.com
traceroute to lifewire.com (151.101.1.121), 30 hops max, 60 byte packets
 1  163.227.176.253 (163.227.176.253)  0.453 ms  0.644 ms  0.638 ms
 2  138.197.248.26 (138.197.248.26)  0.658 ms  0.648 ms  0.637 ms
 3  nyk-b3-link.telnet.net (62.115.45.5)  1.104 ms  35.031 ms  nyk-b3-link.telnet.net (62.115.45.5)  1.041 ms
 4  nyk-bb4-link.telnet.net (62.115.139.150)  2.116 ms  2.081 ms  nyk-bb3-link.telnet.net (62.115.140.222)  1.370 ms
 5  nyk-b5-link.telnet.net (62.115.115.1)  1.694 ms  nyk-b5-link.telnet.net (80.91.254.14)  2.031 ms  nyk-b5-link.telnet.net (62.115.115.1)  1.630 ms
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
```