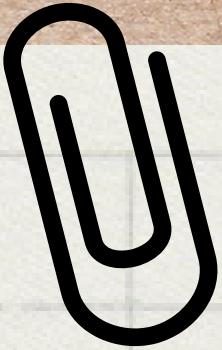


CONCEPTOS DE VULNERABILIDADES

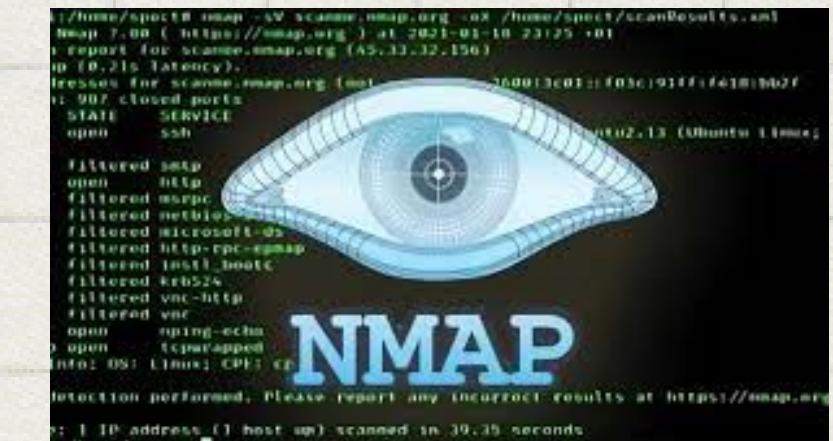
**Alumno: Jose Manuel Lopez Sanchez
7ºM**

Conceptos de Vulnerabilidades



Herramientas de vulnerabilidades:

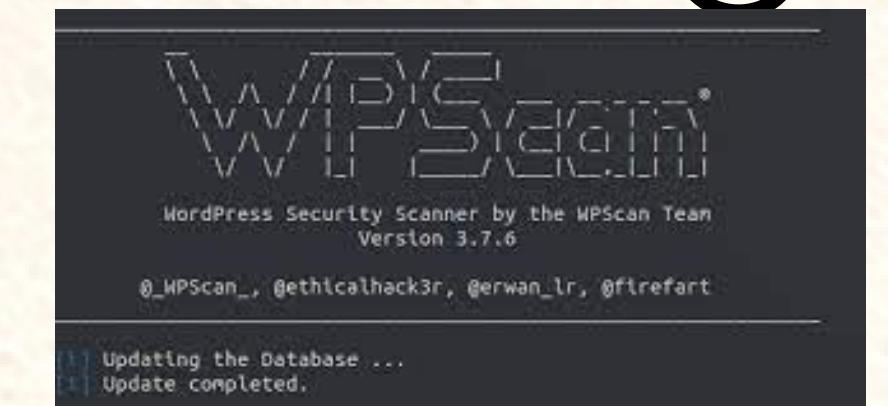
- **nmap:** Nmap es un programa de código abierto que sirve para efectuar rastreo de puertos escrito originalmente por Gordon Lyon y cuyo desarrollo se encuentra hoy a cargo de una comunidad. Fue creado originalmente para Linux aunque actualmente es multiplataforma.



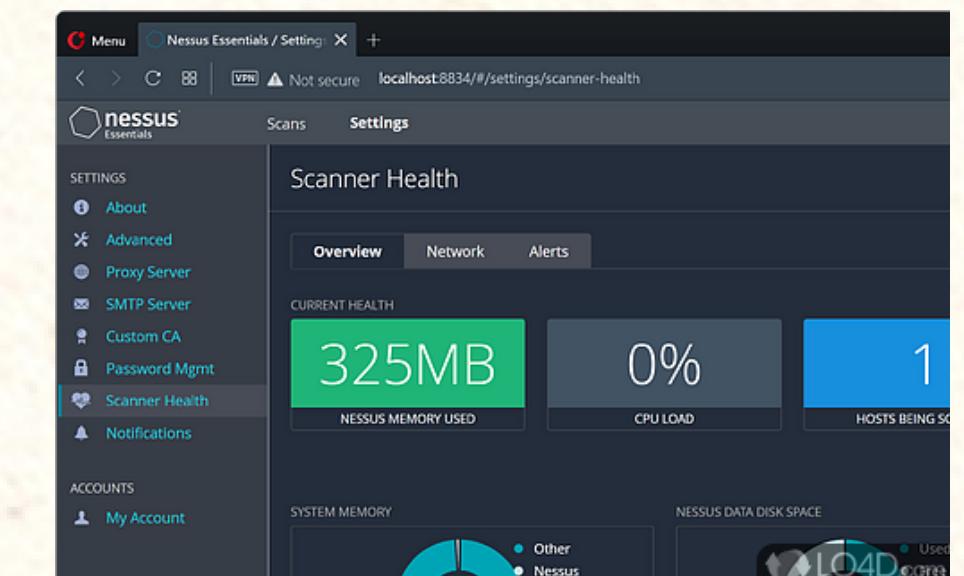
- **Joomscan:** Es una de las herramientas de código abierto más populares para ayudarlo a encontrar vulnerabilidades conocidas de Joomla Core, Componentes e Inyección SQL, ejecución de comandos.



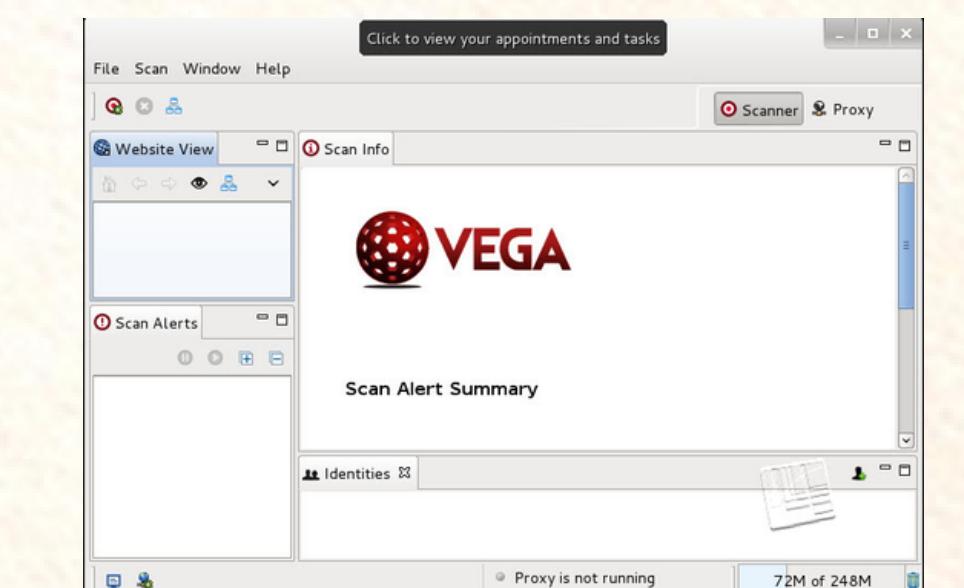
- **Wpscan:** Es un software de código abierto para Kali Linux, diseñado para escanear vulnerabilidades y fallos en un sitio web de WordPress. WPScan es una herramienta muy poderosa y capaz de darte información detallada sobre una página web.



- **Nessus Essentials:** Permite escanear la red doméstica personal con la misma alta velocidad, evaluaciones a profundidad o buscar vulnerabilidades de forma automatizada.



- **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)



Inteligencia Misceláneo.



Gobuster: Es una herramienta utilizada para realizar fuerza bruta a: URIs (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”).

```
└─ $ 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, --nopress      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

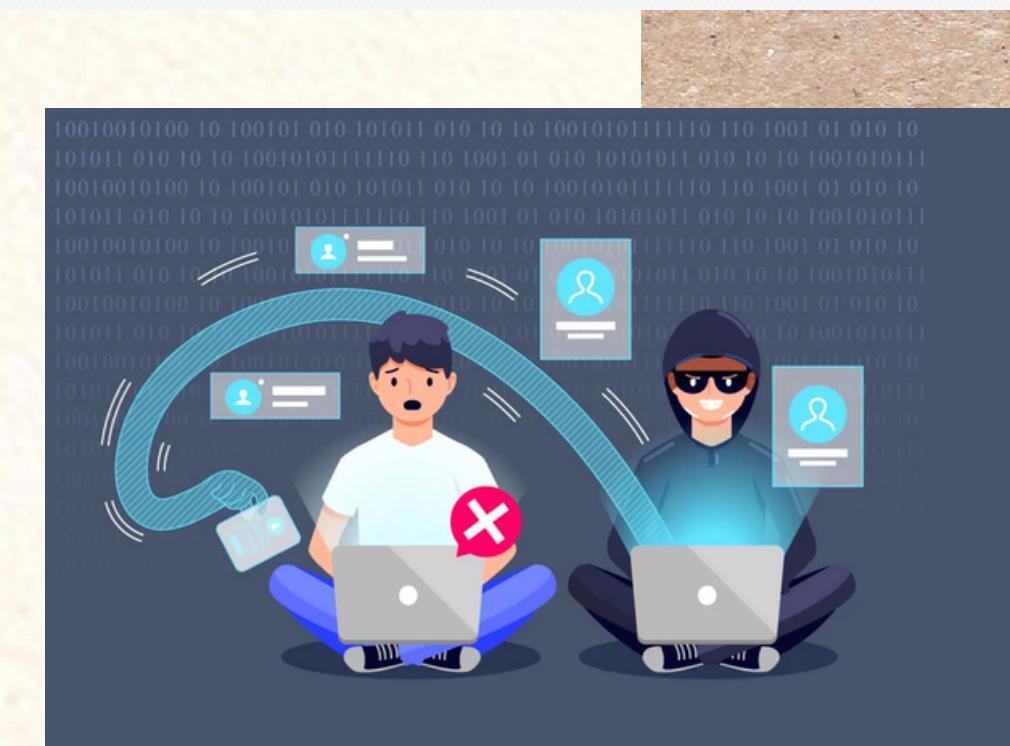
Use "gobuster [command] --help" for more information about a command.
```



Dumpster Diving: Es el proceso de buscar basura para obtener información útil sobre una persona o empresa que luego se puede utilizar con el propósito de piratear.

Este ataque está dirigido principalmente a grandes organizaciones o negocios para llevar a cabo phishing mediante el envío de correos electrónicos falsos a las víctimas que parecen provenir de una fuente legítima. La información obtenida al comprometer la confidencialidad de la víctima se utiliza para fraudes de identidad.

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.



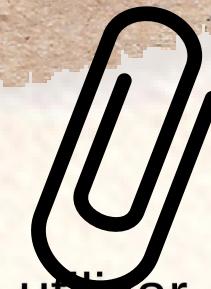


Inteligencia Activa:

Análisis de dispositivos y puertos con Nmap: proceso de utilizar la herramienta de código abierto Nmap (Network Mapper) para escanear y explorar una red informática en busca de dispositivos activos y los puertos de red que están abiertos en esos dispositivos.

Implica enviar paquetes de datos a través de la red y observar las respuestas para determinar la accesibilidad y el estado de los dispositivos y puertos.

```
ruvelnegrulero-Ubuntu:~ ruvelnegrulero-Ubuntu:~$ nmap 192.168.1.2  
Starting Nmap 6.66 ( http://nmap.org ) at 2013-03-26 12:44 CEST  
Nmap scan report for 192.168.1.2  
Host is up (0.00019s latency).  
Not shown: 995 closed ports  
PORT      STATE SERVICE  
22/tcp    open  ssh  
80/tcp    open  http  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
5001/tcp  open  amitie-xmleval  
  
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds  
ruvelnegrulero-Ubuntu:~$
```



Parametros opciones de escaneo de nmap: Parámetros y opciones más comunes que se pueden utilizar con Nmap:

- 1.-sP: Realiza un escaneo de ping para descubrir hosts activos en la red sin realizar un escaneo de puertos.
- 2.-sT (TCP connect scan): Realiza un escaneo de puertos TCP conectándose a cada puerto para determinar si está abierto o cerrado.
- 3.-sS (SYN scan): Realiza un escaneo de puertos SYN enviando paquetes SYN para determinar el estado de los puertos (abiertos, cerrados o filtrados).
- 4.-sU (UDP scan): Realiza un escaneo de puertos UDP para identificar puertos abiertos en este protocolo.
- 5.-sV: Detecta las versiones de los servicios en los puertos abiertos.
- 6.-p: Especifica los puertos a escanear. Puede ser un solo puerto, un rango de puertos (por ejemplo, 1-1024) o una lista separada por comas.
- 7.-A: Activa la detección de versión, script y escaneo de traza de ruta.
- 8.--script o -sC: Ejecuta scripts de NSE (Nmap Scripting Engine) para obtener información adicional sobre hosts y servicios.
- 9.-O: Intenta adivinar el sistema operativo de los hosts en función de las respuestas del escaneo.
- 10.--traceroute: Realiza un escaneo de ruta de traza (tracert) para mostrar la ruta que toman los paquetes a través de la red.
- 11.--max-rtt-timeout, --initial-rtt-timeout, --max-retries: Permite ajustar parámetros de tiempo de espera y reintentos para los paquetes de escaneo.



- **Full TCP scan:** Técnica de exploración de puertos que consiste en enviar un paquete FIN a un puerto determinado, con lo cual deberíamos recibir un paquete de reset (RST) si dicho puerto está cerrado. Esta técnica se aplica principalmente sobre implementaciones de pilas TCP/IP de sistemas Unix.
- **Stealth Scan:** Se diferencia del full tcp scan en que para el escaneo de un host, no permite que se complete el saludo de 3-way-handshake de una conexión normal tcp. Solo llega hasta la parte de syn-ack y envía un rst (reset) en vez de un ack para el último paso.
- **Fingerprinting:** Se utiliza para capturar y analizar tráfico de red en tiempo real, lo que permite a los usuarios ver detalles de cada paquete que viaja a través de una red.
- **Zenmap:** Es una interfaz gráfica de usuario para Nmap. Es un software gratuito y de código abierto que te ayuda a comenzar a utilizar Nmap. Además de proporcionar mapeos de red visuales, Zenmap también te permite guardar y buscar tus escaneos para uso futuro.
- **Análisis traceroute:** Es una herramienta de diagnóstico que se inicia usando una línea de comandos y le informa al usuario sobre la ruta de un paquete de datos en la red. El programa determina el router y los nudos por los que pasó antes de llegar al host de destino.



Fuentes de consulta:

<https://es.wikipedia.org/wiki/Nmap>

<https://geekflare.com/es/joomla-security-vulnerability-scanner/>

<https://platzi.com/clases/2984-inteligencia-activa/49345-nessus-essentials/#:~:text=Esc%C3%A1ner%20de%20vulnerabilidades%20Nessus%20Essentials,buscar%20vulnerabilidades%20de%20forma%20automatizada.>

[https://academy.seguridadcero.com.pe/blog/escaneo-vulnerabilidades-web-vega/#:~:text=Vega%20es%20una%20herramienta%20gr%C3%A1fica,Crawler%20\(copia%20del%20sitio%20web\)](https://academy.seguridadcero.com.pe/blog/escaneo-vulnerabilidades-web-vega/#:~:text=Vega%20es%20una%20herramienta%20gr%C3%A1fica,Crawler%20(copia%20del%20sitio%20web))

[https://www.reydes.com/d/?q=Fuerza Bruta contra Directorios utilizando Gobuster](https://www.reydes.com/d/?q=Fuerza_Bruta_contra_Directorios_utilizando_Gobuster)

<https://ciberseguridad.com/amenazas/dumpster-diving/>

<https://latam.kaspersky.com/resource-center/definitions/what-is-social-engineering>

<https://www.redeszone.net/seguridad-informatica/listado-de-parametros-de-nmap/>

https://www.seguridadyfirewall.cl/2017/12/tecnicas-de-exploracion-tcp-port_21.html#:~:text=TCP%20FIN%20Scan%3A%20Es%20una,TCP%20FIP%20de%20sistemas%20Unix.

<https://www.freecodecamp.org/espanol/news/que-es-nmap-y-como-usarlo-un-tutorial-para-la-mejor-herramienta-de-escaneo-de-todos-los-tiempos/#:~:text=Zenmap%20es%20una%20interfaz%20gr%C3%A1fica,tus%20escaneos%20para%20uso%20futuro.>