

# Conceptos de Vulnerabilidades

José Gilberto Guzmán Gutiérrez

# Tabla de Contenido

01

## Herramientas de Vulnerabilidades

Nmap, JoomScan, WPScan,  
Nessus Essentials, Vega

02

## Inteligencia Misceláneo

Gobuster, Dumpster Diving,  
Ingeniería Social

03

## Inteligencia Activa


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





# 01

## Herramientas de Vulnerabilidades



# Herramientas de Vulnerabilidades

- **Nmap:** Es una herramienta que puede detectar o diagnosticar los servicios que se ejecutan en un sistema conectado a Internet por parte de un administrador de red en su sistema en red que se utiliza para identificar posibles fallas de seguridad.
- **JoomScan:** Es un escáner de vulnerabilidades de código abierto basado en perl que se utiliza para detectar errores de configuración y vulnerabilidades de seguridad de Joomla CMS.
- **WPScan:** Es un escáner de seguridad de WordPress que se utiliza para probar las instalaciones de WordPress y los sitios web con tecnología de WordPress.
- **Nessus Essentials:** Permite escanear su entorno (hasta 16 direcciones IP por escáner) con las mismas evaluaciones detalladas y de alta velocidad y la comodidad de escaneo sin agente que disfrutaron los suscriptores de Nessus
- **Vega:** Es un escáner de seguridad web gratuito y de código abierto y una plataforma de prueba de seguridad web para probar la seguridad de las aplicaciones web. Sirve para encontrar y validar SQL Injection, Cross-Site Scripting (XSS), información confidencial divulgada inadvertidamente y otras vulnerabilidades.





02

Inteligencia  
Misceláneo



# Inteligencia Misceláneo

- **Gobuster:** Esta herramienta se utiliza para directorios y archivos de fuerza bruta y subdominios DNS. También puede buscar nombres de host virtuales en servidores web de destino.
- **Dumpster Diving:** Es una técnica utilizada para recuperar información que podría utilizarse para llevar a cabo un ataque o acceder a una red informática a partir de elementos desechados.
- **Ingeniería Social:** Es el acto de explotar las debilidades humanas para obtener acceso a información personal y sistemas protegidos. La ingeniería social se basa en manipular a las personas en lugar de piratear los sistemas informáticos para penetrar en la cuenta de un objetivo





03

Inteligencia  
Activa



# Inteligencia Activa



- **Análisis de dispositivos y puertos con Nmap:** Se utiliza para realizar análisis activos de dispositivos y puertos en una red. Puede identificar qué dispositivos están activos en una red y qué puertos están abiertos en esos dispositivos.
- **Parámetros opciones de escaneo de nmap:** Ofrece una variedad de opciones y parámetros de escaneo que permiten ajustar la profundidad y el alcance del análisis. Esto incluye escaneos rápidos, detección de sistemas operativos, detección de servicios, entre otros.
- **Full TCP scan:** Es un tipo de escaneo exhaustivo en el que Nmap intenta conectarse a todos los 65,535 puertos TCP posibles en un dispositivo. Puede ser intensivo y llevar tiempo, pero proporciona un panorama completo de la exposición de puertos.





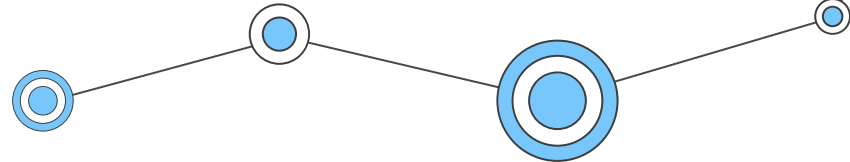
# Inteligencia Activa

- **Stelth Scan:** Aquí, el escáner de puertos crea paquetes IP sin procesar y los envía al host para monitorear las respuestas. Este tipo de escaneo también se conoce como escaneo semiabierto o escaneo SYN, ya que nunca abre una conexión TCP completa... Este tipo de escáner crea un paquete SYN y lo envía al host. Si el puerto de destino está abierto, el host responderá con un paquete SYN-ACK. Luego, el cliente responderá con un paquete RST para cerrar la conexión antes de completar el protocolo de enlace. Si el puerto está cerrado pero sin filtrar, el objetivo responderá instantáneamente con un paquete RST.
- **Fingerprinting:** Es el proceso en el que un sitio o servicio remoto recopila pequeños fragmentos de información sobre la máquina de un usuario y los une para formar una imagen única, o "huella digital", del dispositivo del usuario. Las dos formas principales son la toma de huellas dactilares del navegador, donde esta información se entrega a través del navegador cuando un usuario visita sitios remotos, y la toma de huellas digitales del dispositivo, cuando la información se entrega a través de aplicaciones que un usuario ha instalado en su dispositivo.

# Inteligencia Activa



- **Zenmap:** Es una GUI gratuita y de código abierto para Nmap. Está disponible en muchos sistemas operativos (Linux, Windows, Mac OS X, BSD, etc.) y hace que Nmap sea más fácil de usar para principiantes.
- **Análisis traceroute:** Proporciona un mapa de cómo viajan los datos en Internet desde su origen hasta su destino. Cuando te conectas a un sitio web, los datos que obtienes deben viajar a través de múltiples dispositivos y redes en el camino, particularmente enrutadores.

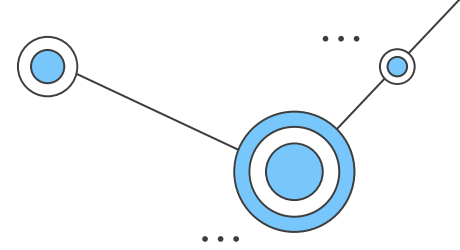


# Bibliografías.

## Herramientas de Vulnerabilidades.

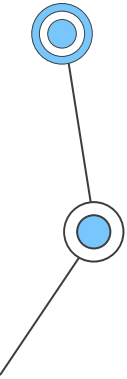
- Nmap. (s/f). Www.javatpoint.com. Recuperado el 12 de agosto de 2023, de <https://www.javatpoint.com/what-is-nmap>
- (N.d.). Alertlogic.com. Retrieved August 12, 2023, from <https://support.alertlogic.com/hc/en-us/articles/360004766571-Joomla-Tooling-O-WASP-JoomScan-Vulnerability-Scanner-Information-Disclosure>
- Follow, S. (2022, September 23). How to Use wpscan tool in Kali Linux. GeeksforGeeks. <https://www.geeksforgeeks.org/how-to-use-wpscan-tool-in-kali-linux/>
- Tenable Nessus Essentials vulnerability scanner. (n.d.). Tenable®. Retrieved August 12, 2023, from <https://www.tenable.com/products/nessus/nessus-essentials>

# Bibliografías.

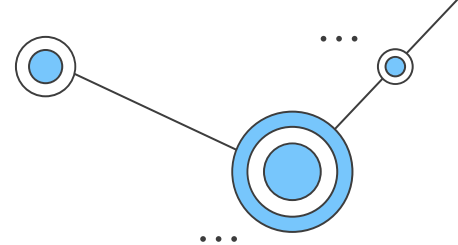


## Inteligencia Misceláneo.

- Linux, K. (2019, October 13). Gobuster -- Faster Directory Scanner. Best Kali Linux Tutorials. <https://www.kalilinux.in/2019/10/gobuster-kali-linux.html>
- Wright, G. (2021, April 6). Dumpster diving. Security; TechTarget. <https://www.techtarget.com/searchsecurity/definition/dumpster-diving>
- Kenton, W. (2017, January 24). Social Engineering: Types, Tactics, and FAQ. Investopedia. <https://www.investopedia.com/terms/s/social-engineering.asp>

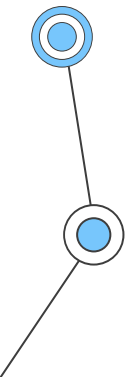


# Bibliografías.



## Inteligencia Activa.

- Toole, M. (2022, December 23). How to use Nmap to scan for open ports. Blumira. <https://www.blumira.com/using-nmap/>
- Options Summary. (n.d.). Nmap.org. Retrieved August 12, 2023, from <https://nmap.org/book/man-briefoptions.html>
- Cybersecurity. (n.d.). Codecademy. Retrieved August 12, 2023, from <https://www.codecademy.com/resources/docs/cybersecurity/nmap/tcp-connect-scan>
- Singh, M., & Mohit. (2016). Python Penetration Testing Cookbook. Packt Publishing.
- What is fingerprinting? (n.d.). Eff.org. Retrieved August 12, 2023, from <https://ssd.eff.org/module/what-fingerprinting>
- Peyo, T. (2016, March 13). What is Zenmap? Geek University. <https://geek-university.com/what-is-zenmap/>
- What is Traceroute: What Does it Do & How Does It Work? (n.d.). Fortinet. Retrieved August 12, 2023, from <https://www.fortinet.com/resources/cyberglossary/traceroutes>





# Muchas Gracias!

¿Tienes Alguna Pregunta?

josegilbertoguzmangutierrez@gmail.com

+52 221 529 2048

<https://gilberto-guzman.github.io/>

...

