



Automatización del Escaneo y Enumeración de Servicios en Redes Análisis Estratégico con Python y Nmap



# Introducción al Reconocimiento Activo



#### Introducción al Reconocimiento Activo

- El reconocimiento activo permite detectar servicios expuestos, configuraciones erróneas y vulnerabilidades.
- Escanear y enumerar servicios es el primer paso en auditorías y pentesting.
- Python permite automatizar esta tarea de forma escalable y eficiente.





# ¿Qué es Nmap y por qué usarlo?



#### ¿Qué es Nmap y por qué usarlo?

- Nmap (Network Mapper) es una herramienta de escaneo robusta y precisa.
- Detecta: puertos abiertos, servicios activos, versiones, sistemas operativos, políticas de firewall, etc.
- Modos comunes:
  - -sS: escaneo SYN (sigiloso)
  - -sV: detección de versiones
  - -A: escaneo avanzado (SO, rutas, scripts NSE)
  - -p: rango de puertos





# Automatización con Python



#### Automatización con Python

- Python puede controlar Nmap mediante la biblioteca python-nmap.
- Permite escaneos automatizados, programables y con salidas reutilizables.
- Ideal para CI/CD, escaneos recurrentes y análisis en lote.





## Escaneo Automatizado



#### **Escaneo Automatizado**

- Escaneo sobre red 192.168.1.0/24 y puertos 1-1024.
- Detección de hosts, puertos abiertos, servicios, versiones y estado.
- Estructura de salida organizada y legible para informes.
- Posibilidad de generar alertas ante cambios en versiones detectadas.





## Interpretación de Resultados



#### Interpretación de Resultados

#### Datos clave que Nmap ofrece:

- Puertos abiertos o filtrados
- Servicios identificados
- Producto y versión del software
- Estado del host y sistema operativo

#### Con estos datos se pueden:

- Identificar servicios vulnerables
- Priorizar parches
- Detectar configuraciones inseguras
- Comparar contra bases como CVE o Exploit-DB





# Buenas Prácticas Profesionales



#### **Buenas Prácticas Profesionales**

- Escanear solo con autorización formal.
- Documentar el alcance, fecha, objetivos y herramientas.
- Limitar la velocidad del escaneo para evitar disrupciones.
- Filtrar resultados útiles y automatizar su análisis.
- Integrar en procesos de mantenimiento y monitoreo continuo.





# Casos Reales por Falta de Enumeración



#### Casos Reales por Falta de Enumeración

Equifax (2017): Apache Struts vulnerable sin detectar (CVE-2017-5638).

Panama Papers (2016): servidor Drupal expuesto, sin auditar.

Capital One (2019): metadata filtrada por headers mal configurados.

Todos estos casos pudieron prevenirse con un escaneo automatizado y estratégico.





# Consideraciones Éticas



#### Consideraciones Éticas

- Escaneo automatizado ≠ permiso para explorar sin límites.
- Toda acción debe realizarse en entornos autorizados.
- Capturar información sin consentimiento es una violación ética.
- La ciberseguridad profesional se basa en integridad, no en intrusión.



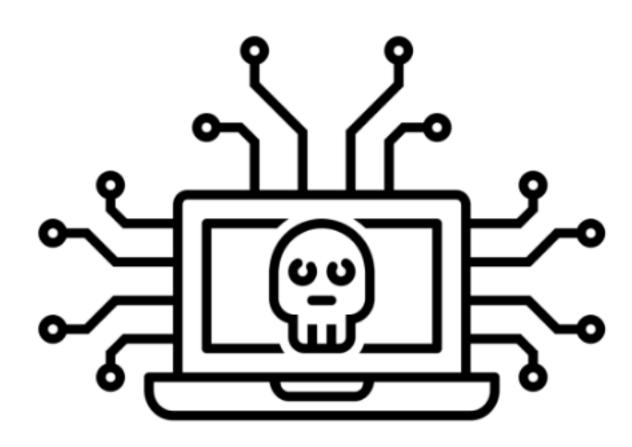


### Conclusión



#### Conclusión

- Automatizar el escaneo y la enumeración es clave para prevenir ataques.
- Python y Nmap permiten transformar un proceso técnico en una capacidad estratégica.
- La enumeración moderna no es ofensiva: es una línea de defensa automatizada.



Energiza!