ESCANEO DE REDES (NMAP)

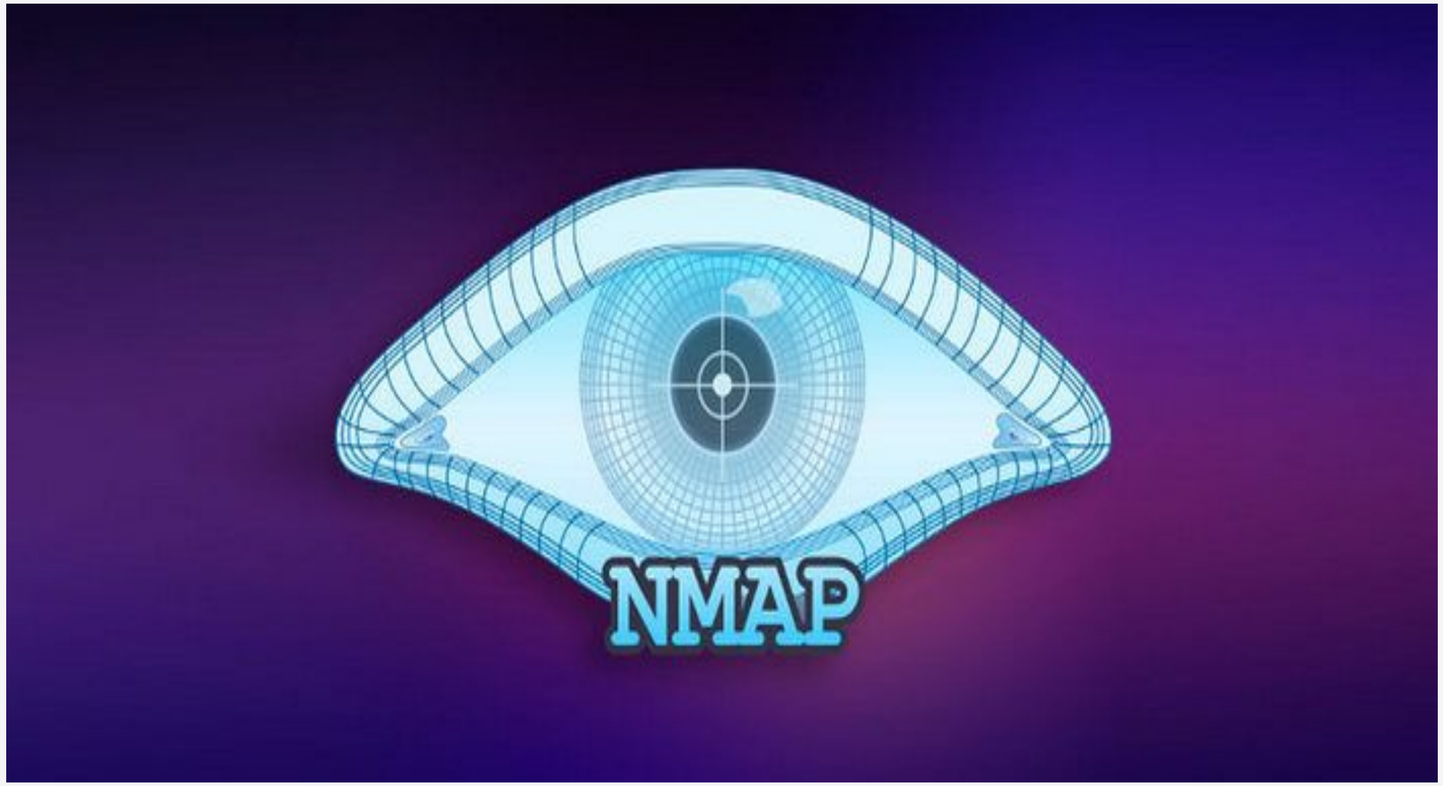
Activos y servicios

OpenWebinars

¿QUÉ ES NMAP?

- Nmap (Network Mapper) es una herramienta de código abierto para exploración de red y auditoría de seguridad
    - Utilizado para descubrir hosts y servicios en una red informática

¿QUÉ ES NMAP?



USOS NMAP

- Identificación rápida de dispositivos activos en la red
- Comandos básicos para escanear rangos de IP

```
nmap -sP 192.168.0.1/24
```

```
nmap 192.168.0.*
```

USOS NMAP II

- Detección de servicios y aplicaciones que se ejecutan en los puertos abiertos
- Escaneo de TODOS los puertos

```
nmap -sV [IP o dominio]

nmap -p80,443,8080 [IP o dominio]

nmap -p- -sV [IP o dominio]
```

USOS NMAP III

- Mediante los servicios detectados puedes hacerte una idea del sistema operativo, si este no es exfiltrado en el proceso de reconocimiento de versiones de servicios, sin embargo podemos valernos de:

```
nmap -O [IP o dominio]
```

Este comando requiere permisos administrativos

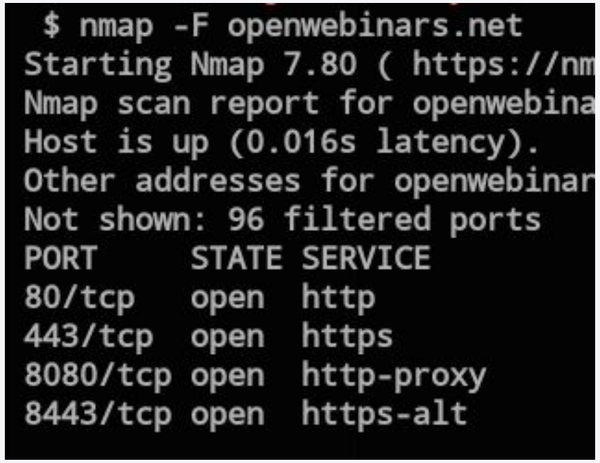
USOS NMAP IV

- Escaneo de los puertos - UDP -

  nmap -sU [IP o dominio]

- Escaneo rápido:

  nmap -F [IP o dominio]



MORE IN NMAP

- Podemos controlar la salida de nmap a ficheros distintos. Los formatos de salida de nmap son:
  - nmap
  - grep output
  - xml

OUTPUT IN NMAP

nmap <ip> -oA ouput_filename

MORE IN NMAP

- NMAP incluye script que automatizan ciertas detecciones o ataques contra servicios. Estos usan Nmap Scripting Engine (NSE) basado en el lenguaje LUA

  nmap --script vuln [IP o dominio]

  nmap --script firewall-bypass [IP o dominio]

NET CONSIDERATIONS

- **Precauciones y Consideraciones Éticas**
    - El escaneo de redes ha implicado un debate sobre su legitimidad y responsabilidad de uso.Siempre obtener permiso antes de escanear redes que no te pertenecen
    - Puede existir un impacto en la red derivado de posibles riesgos de sobrecarga en dispositivos de red durante escaneos agresivos

¡LET’S TRY IT!