**Guía de uso Scanner de Nmap, Red Team.**

Este script es un wrapper de Nmap que permite realizar escaneos de red de forma interactiva mediante línea de comandos.

**Características principales:**

La clase NetworkScanner gestiona la ejecución de Nmap con diferentes perfiles predefinidos. Cada escaneo genera tres archivos de salida: XML, TXT y JSON con metadatos del escaneo.

Los perfiles disponibles son:

- stealth: Escaneo sigiloso TCP SYN
- version: Detección de versiones de servicios
- aggressive: Escaneo completo con detección de OS
- quick: Escaneo rápido de puertos comunes
- comprehensive: Escaneo exhaustivo con scripts NSE

**Uso del argparse:**

El argumento target permite especificar una IP o hostname individual. Como alternativa, target_file permite cargar múltiples objetivos desde un archivo de texto.

El parámetro scan_type define el perfil de escaneo a utilizar. Por defecto usa el modo stealth.

El argumento ports permite especificar puertos específicos en formato individual (22,80,443) o rango (1-1000).

El parámetro output_dir define dónde se guardarán los resultados.

**Ejemplos:**

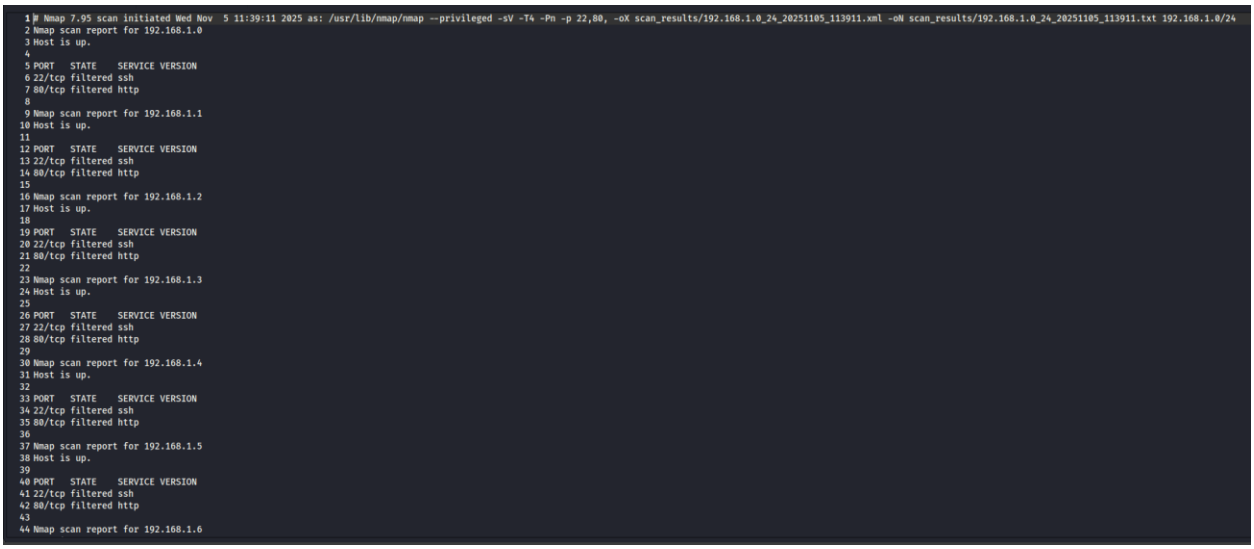
Escaneo básico: `python scanner.py -t 192.168.1.1`

Escaneo con detección de versiones en puertos específicos: `python scanner.py -t 192.168.1.1 -s version -p 22,80,443`

Escaneo de múltiples objetivos: `python scanner.py -T targets.txt -s quick`

El script incluye manejo de errores para timeouts, Nmap no instalado, y archivos no encontrados. Los resultados se organizan con timestamps para mantener un historial de escaneos.

```
┌──(jander㉿Lolo)-[~/Documentos]
└─$ python scanner.py -t 192.168.1.0/24 -s version -p 22,80,
[*] Ejecutando: nmap -sV -T4 -Pn -p 22,80, 192.168.1.0/24 -oX scan_results/192.168.1.0_24_20251105_113911.xml -oN scan_results/192.168.1.0_24_20251105_113911.txt
[*] Target: 192.168.1.0/24
[*] Tipo de scan: version
[*] Guardando resultados en: scan_results
[+] Scan completado exitosamente
[+] Resultados guardados:
    - XML: scan_results/192.168.1.0_24_20251105_113911.xml
    - TXT: scan_results/192.168.1.0_24_20251105_113911.txt
    - JSON: scan_results/192.168.1.0_24_20251105_113911.json
```



```
# Nmap 7.95 scan initiated Wed Nov  5 11:39:11 2025 as: /usr/lib/nmap/nmap --privileged -sV -T4 -Pn -p 22,80, -oX scan_results/192.168.1.0_24_20251105_113911.xml -oN scan_results/192.168.1.0_24_20251105_113911.txt 192.168.1.0/24
Nmap scan report for 192.168.1.0
Host is up.

PORT   STATE    SERVICE VERSION
22/tcp filtered ssh
80/tcp filtered http

Nmap scan report for 192.168.1.1
Host is up.

PORT   STATE    SERVICE VERSION
22/tcp filtered ssh
80/tcp filtered http

Nmap scan report for 192.168.1.2
Host is up.

PORT   STATE    SERVICE VERSION
22/tcp filtered ssh
80/tcp filtered http

Nmap scan report for 192.168.1.3
Host is up.

PORT   STATE    SERVICE VERSION
22/tcp filtered ssh
80/tcp filtered http

Nmap scan report for 192.168.1.4
Host is up.

PORT   STATE    SERVICE VERSION
22/tcp filtered ssh
80/tcp filtered http

Nmap scan report for 192.168.1.5
Host is up.

PORT   STATE    SERVICE VERSION
22/tcp filtered ssh
80/tcp filtered http

Nmap scan report for 192.168.1.6
```