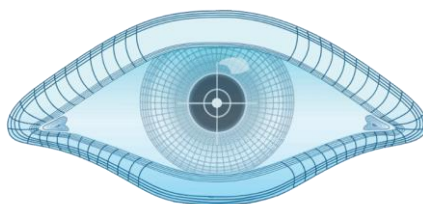


Guía Práctica: Escaneo de Redes con Nmap en Ubuntu

AUTOR: <https://github.com/Alexandeeer-0>

1. ¿De qué trata este proyecto?

En este proyecto aprenderás a usar **Nmap**, una de las herramientas más poderosas en el mundo del análisis de redes y la ciberseguridad. Vamos a escanear redes para identificar dispositivos, puertos abiertos, servicios en ejecución y algunas vulnerabilidades básicas. Esta guía te acompañará en cada paso, para que te sientas cómodo con lo que estás haciendo.



2. ¿Qué necesitas para empezar?

Antes de comenzar, asegúrate de tener lo siguiente listo:

- **Ubuntu.** Si usas otra distro Linux, no hay problema, pero los comandos pueden variar un poquito.
- **Nmap** instalado en tu sistema. (Lo haremos).
- Conocimientos básicos de la terminal (aunque te explicaré todo).
- Una red local activa a la que estés conectado para hacer los escaneos.



3. Primer paso: Instalando Nmap

No podemos escanear sin Nmap, así que lo instalamos en Ubuntu. Abre tu terminal preferida y ejecuta los siguientes comandos:

1. Actualiza los repositorios:

```
ap@ap-Nitro-AN515-55:~/VSCoDe/EscaneoBasicoDeRedesConNmap$ sudo apt update && sudo apt upgrade
```

sudo apt update && sudo apt upgrade

2. Instala Nmap:

```
ap@ap-Nitro-AN515-55:~$ sudo apt install nmap
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
```

sudo apt install nmap

3. Verifica que Nmap se haya instalado bien:

```
ap@ap-Nitro-AN515-55:~/VSCoDe/EscaneoBasicoDeRedesConNmap$ nmap --version
Nmap version 7.94SVN ( https://nmap.org )
```

nmap --version

¡Listo! Ya tienes Nmap instalado y funcionando :)

4. ¡Vamos a crear un script de escaneo automático!

Ahora viene la parte emocionante!! Vamos a crear un pequeño **script en bash** que haga varios escaneos útiles automáticamente. Esto nos ayudará a explorar nuestra red sin tener que escribir cada comando a mano.

Paso 1: Crear el archivo del script

1. En tu terminal, crea un nuevo archivo de script con el editor de texto `nano` para que después copies el código que está dentro del repositorio:

`nano escaneo_red.sh`

```
GNU nano 7.2                                escaneo_red_1.sh *
#!/bin/bash
echo "Iniciando escaneo de red..."
NETWORK="***.***.*/24"
FILE="resultadosNMAP"
mkdir -p $FILE

echo "Escaneando dispositivos activos..."
sudo nmap -sn $NETWORK -oN $FILE/activos_$(date '+%Y-%m-%d_%H-%M-%S').txt
echo "Escaneando puertos TCP abiertos..."
sudo nmap -sT $NETWORK -oN $FILE/tcp_$(date '+%Y-%m-%d_%H-%M-%S').txt
echo "Realizando escaneo SYN..."
sudo nmap -sS $NETWORK -oN $FILE/syn_$(date '+%Y-%m-%d_%H-%M-%S').txt
echo "Detectando versiones de servicios..."
sudo nmap -sV $NETWORK -oN $FILE/versiones_$(date '+%Y-%m-%d_%H-%M-%S').txt
echo "Intentando detectar sistemas operativos..."
sudo nmap -O $NETWORK -oN $FILE/sistemas_$(date '+%Y-%m-%d_%H-%M-%S').txt
echo "Ejecutando scripts NSE para detección de vulnerabilidades..."
sudo nmap --script vuln $NETWORK -oN $FILE/vulnerabilidades_$(date '+%Y-%m-%d_%H-%M-%S').txt
echo "Escaneo completado. Los resultados están en la carpeta $FILE."
```

Paso 2: Dar permisos y ejecutar

1. Ahora, dale permisos de ejecución al script para que lo puedas ejecutar como un programa:

```
ap@ap-Nitro-AN515-55:~/VSCoDe/EscaneoBasicoDeRedesConNmap$ chmod +x escaneo_red_1.sh
```

`chmod +x escaneo_red.sh`

2. Ejecuta el script:

```
ap@ap-Nitro-AN515-55:~/VSCode/EscaneoBasicoDeRedesConNmap$ ./escaneo_red_1.sh
Iniciando escaneo de red...
Escaneando dispositivos activos...
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-21 19:34 -05
Nmap scan report for_gateway (192.168.1.1)
Host is up (0.00079s latency).
MAC Address: F4:C4:D6:4A:14:35 (Shenzhen Xinfu Electronic)
Nmap scan report for 192.168.1.3
Host is up (0.10s latency).
MAC Address: 38:1F:8D:3B:0F:4F (Tuya Smart)
Nmap scan report for 192.168.1.5
Host is up (0.20s latency).
MAC Address: 48:B4:23:9E:03:09 (Amazon Technologies)
Nmap scan report for 192.168.1.7
Host is up (0.24s latency).
MAC Address: 18:48:BE:B7:1F:A8 (Amazon Technologies)
Nmap scan report for 192.168.1.122
Host is up (0.00068s latency).
MAC Address: F4:A8:0D:8C:EE:FE (Wistron InfoComm(Kunshan)Co.)
Nmap scan report for 192.168.1.192
Host is up (3.1s latency).
MAC Address: 00:F3:61:1A:9B:9F (Amazon Technologies)
Nmap scan report for ap-Nitro-AN515-55 (192.168.1.193)
Host is up.
Nmap scan report for ap-Nitro-AN515-55 (192.168.1.195)
Host is up.
Nmap done: 256 IP addresses (8 hosts up) scanned in 9.95 seconds
```

./escaneo_red.sh

Esto hará que el script ejecute todos los escaneos y guarde los resultados en la carpeta `resultadosNMAP` de manera organizada.

5. ¿Qué significan los resultados?

Después de ejecutar el script, vas a ver varios archivos dentro de la carpeta `resultadosNMAP`, cada uno correspondiente a un tipo de escaneo. ¿Pero que significa?:

- **Dispositivos activos** (`activos.txt`): Este archivo muestra todos los dispositivos que respondieron al ping. Básicamente, te dice qué dispositivos están conectados a tu red.
- **Puertos TCP abiertos** (`tcp.txt`): Aquí verás una lista de los puertos abiertos en los dispositivos de la red.
- **Escaneo SYN** (`syn.txt`): Es una forma más rápida de escanear puertos abiertos sin ser muy intrusivo. Esto se usa mucho en auditorías de seguridad porque es rápido y "silencioso".

- **Versiones de servicios** (`versiones.txt`): Este archivo muestra las versiones del software que está corriendo en los puertos abiertos. Es útil para detectar software obsoleto o vulnerable.
- **Vulnerabilidades** (`vulnerabilidades.txt`): Nmap ejecuta este scripts que buscan vulnerabilidades conocidas en los servicios detectados.

▼ resultadosNMAP	
≡ activos_2024-10-21_19-34-13.txt	U
≡ sistemas_2024-10-21_19-48-16.txt	U
≡ syn_2024-10-21_19-40-39.txt	U
≡ tcp_2024-10-21_19-34-23.txt	U
≡ versiones_2024-10-21_19-42-46.txt	U
≡ vulnerabilidades_2024-10-21_19-50-07.txt	U

6. Conclusión

¡Felicidades! Has completado tu primer proyecto de escaneo de red con Nmap. Ahora ya dominas cómo identificar dispositivos en la red, explorar puertos abiertos y detectar posibles vulnerabilidades. Este proyecto es solo el primer paso hacia el vasto mundo de la ciberseguridad. ¡Espero que lo hayas disfrutado, querido usuario de GitHub! 📦

AUTOR: <https://github.com/Alexandeeer-0>