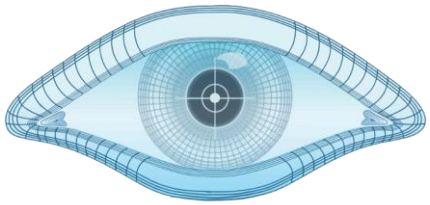
# Guía Práctica: Escaneo de Redes con Nmap en Ubuntu

---

*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?

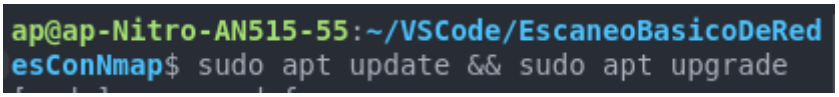
Antes de comenzar, asegúrate de tener lo siguiente listo:

- **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

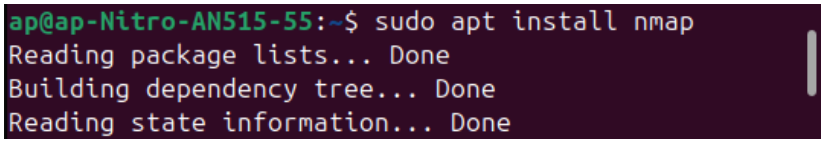
No podemos escanear sin Nmap, así que lo instalamos en Ubuntu. Abre tu terminal preferida y ejecuta los siguientes comandos:

1. **Actualiza los repositorios**:



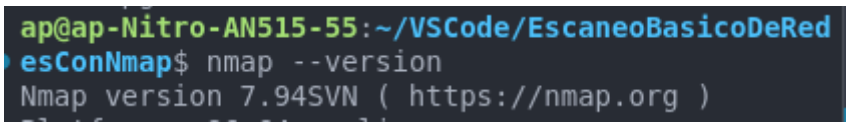

*sudo apt update && sudo apt upgrade*

2. **Instala Nmap**:




*sudo apt install nmap*

3. **Verifica que Nmap se haya instalado bien**:




*nmap --version*

¡Listo! Ya tienes Nmap instalado y funcionando :)

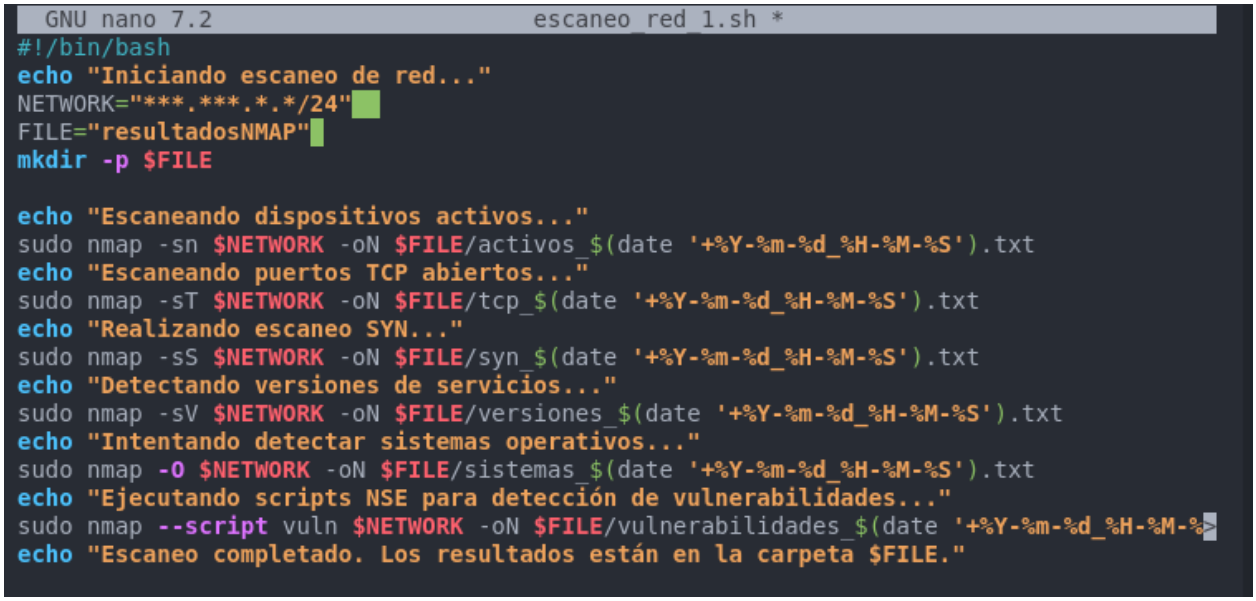
# 4. ¡Vamos a crear un script de escaneo automático!

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 despues copies el codigo que esta dentro del repositorio:

nano escaneo_red.sh

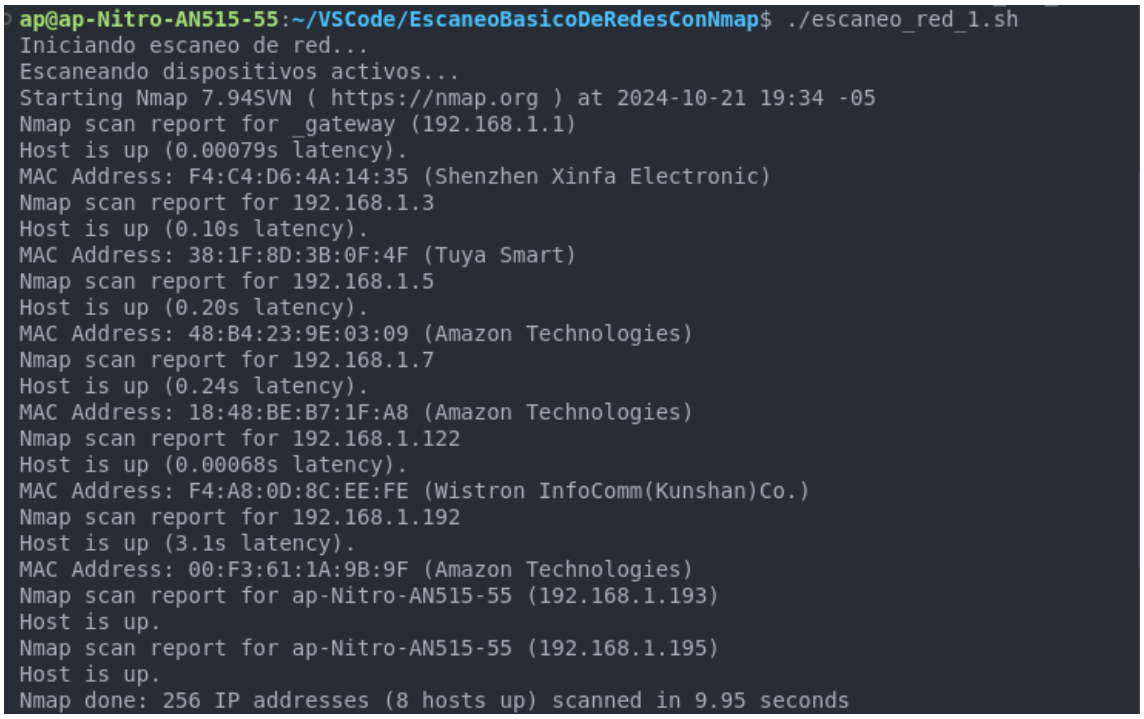



## Paso 2: Dar permisos y ejecutar

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


chmod +x escaneo_red.sh

2. Ejecuta el script:




`./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?:

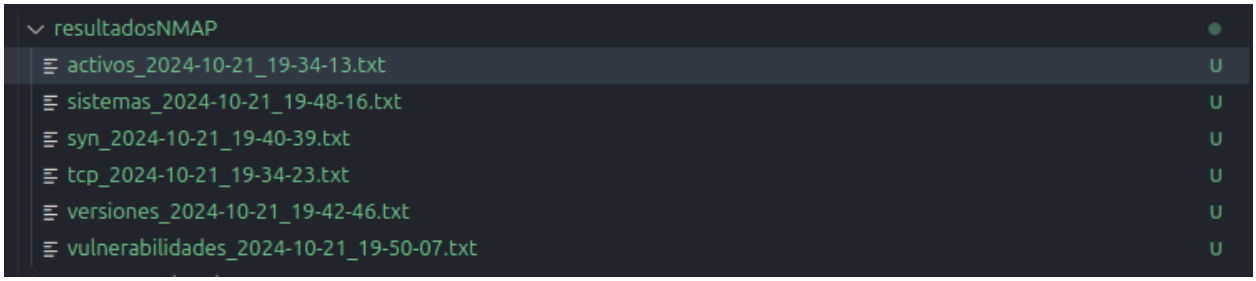
- **Dispositivos activos** (`activos.txt`): Este archivo muestra todos los dispositivos que respondieron al ping. Básicamente, te dice qué dispositivos están conectados a tu red.

- **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.




# 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*