Script NMAP

Crear una carpeta

- mkdir scriptnmap

```
li@li:~$ mkdir scriptnmap
li@li:~$ ll
```

```
drwxrwxr-x  2 li   li   4096 oct 24 10:43 scriptnmap/
```

Entra en la carpeta

- cd scriptnmap

```
li@li:~$ cd scriptnmap
li@li:~/scriptnmap$
```

Crear un script

- sudo nano scriptnmap.sh

```
li@li:~/scriptnmap$ sudo nano scriptnmap.sh
```

Introduzca el siguiente contenido

- ScriptNMAP.txt

A continuación, conceda permisos al script

- sudo chmod -R 777 scriptnmap.sh

```
li@li:~/scriptnmap$ sudo chmod -R 777 scriptnmap.sh
li@li:~/scriptnmap$
```

Ejecuta el script

- ./scriptnmap.sh

Si nmap aún no está instalado, aparecerá el siguiente mensaje:

```
li@li:~/scriptnmap$ ./scriptnmap.sh
nmap no está instalado. Instálalo con: sudo apt update && sudo apt install -y nmap
```

Instalar nmap

- sudo apt update && sudo apt install -y nmap

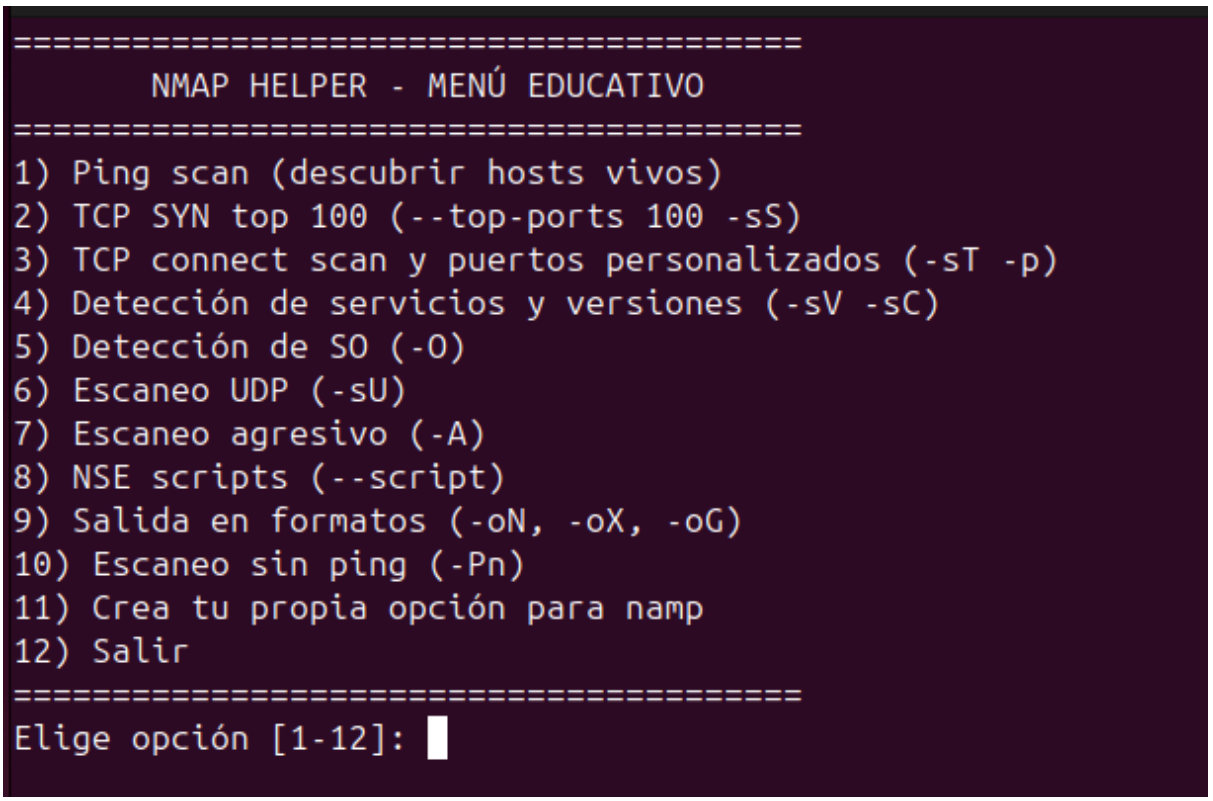
```
li@li:~/scriptnmap$ sudo apt update && sudo apt install -y nmap
Obj:1 http://archive.ubuntu.com/ubuntu noble InRelease
```

Después de instalar nmap correctamente, vuelve a ejecutar el script

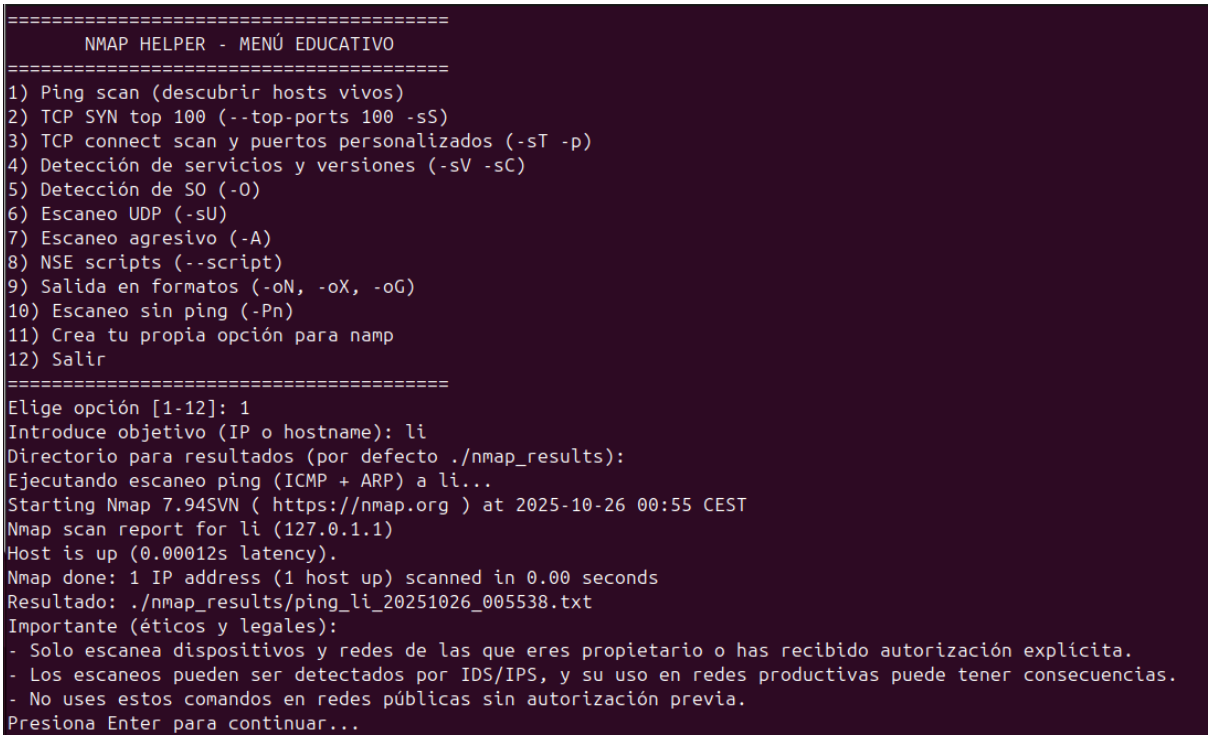
- ./scriptnmap.sh

```
li@li:~/scriptnmap$ ./scriptnmap.sh
```

Aparece el siguiente contenido:



Introduzca 1 para probar Ping scan



Acceda a nmap_results para ver

- cd scriptnmap/nmap_results

```
li@li:~$ cd scriptnmap/nmap_results
li@li:~/scriptnmap/nmap_results$ ls
ping_li_20251026_005538.txt
li@li:~/scriptnmap/nmap_results$ cat ping_li_20251026_005538.txt
# Nmap 7.94SVN scan initiated Sun Oct 26 00:55:38 2025 as: nmap -sn -oN ./nmap_results/ping_li_20251026_005538.txt li
Nmap scan report for li (127.0.1.1)
Host is up (0.00012s latency).
# Nmap done at Sun Oct 26 00:55:38 2025 -- 1 IP address (1 host up) scanned in 0.00 seconds
li@li:~/scriptnmap/nmap_results$
```

Prueba TCP SYN top 100

```
========================================
Elige opción [1-12]: 2
Introduce objetivo (IP o hostname): li
Directorio para resultados (por defecto ./nmap_results):
Ejecutando escaneo TCP SYN (--top-ports 100 -sS -T4) a li...
[sudo] contraseña para li:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-10-26 01:02 CEST
Initiating SYN Stealth Scan at 01:02
Scanning li (127.0.1.1) [100 ports]
Discovered open port 80/tcp on 127.0.1.1
Discovered open port 10000/tcp on 127.0.1.1
Completed SYN Stealth Scan at 01:02, 0.02s elapsed (100 total ports)
Nmap scan report for li (127.0.1.1)
Host is up (0.0000010s latency).
Not shown: 98 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
10000/tcp open  snet-sensor-mgmt

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.05 seconds
           Raw packets sent: 100 (4.400KB) | Rcvd: 100 (4.008KB)
Resultado: ./nmap_results/syn_top_li_20251026_010226.txt
Importante (éticos y legales):
- Solo escanea dispositivos y redes de las que eres propietario o has recibido autorización explícita.
- Los escaneos pueden ser detectados por IDS/IPS, y su uso en redes productivas puede tener consecuencias.
- No uses estos comandos en redes públicas sin autorización previa.
Presiona Enter para continuar...
```

Ver los resultados en nmap_results

```
li@li:~/scriptnmap/nmap_results$ ll
total 16
drwxrwxr-x 2 li   li   4096 oct 26 01:02 ./
drwxrwxr-x 3 li   li   4096 oct 26 00:55 ../
-rw-rw-r-- 1 li   li    277 oct 26 00:55 ping_li_20251026_005538.txt
-rw-r--r-- 1 root root  468 oct 26 01:02 syn_top_li_20251026_010226.txt
li@li:~/scriptnmap/nmap_results$ cat syn_top_li_20251026_010226.txt
# Nmap 7.94SVN scan initiated Sun Oct 26 01:02:43 2025 as: nmap -sS --top-ports 100 -T4 -v -oN ./nmap_results/syn_top_li_20251026_010226.
txt li
Nmap scan report for li (127.0.1.1)
Host is up (0.0000010s latency).
Not shown: 98 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
10000/tcp open  snet-sensor-mgmt

Read data files from: /usr/bin/../share/nmap
# Nmap done at Sun Oct 26 01:02:43 2025 -- 1 IP address (1 host up) scanned in 0.05 seconds
```

Prueba TCP connect scan y puertos personalizados

```
Elige opción [1-12]: 3
Introduce objetivo (IP o hostname): li
Directorio para resultados (por defecto ./nmap_results):
Introduce puertos (p.ej. 22,80,443 o 1-1024): 80
Ejecutando escaneo TCP connect (-sT -p 80) a li...
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-10-26 01:13 CEST
Initiating Ping Scan at 01:13
Scanning li (127.0.1.1) [2 ports]
Completed Ping Scan at 01:13, 0.00s elapsed (1 total hosts)
Initiating Connect Scan at 01:13
Scanning li (127.0.1.1) [1 port]
Discovered open port 80/tcp on 127.0.1.1
Completed Connect Scan at 01:13, 0.00s elapsed (1 total ports)
Nmap scan report for li (127.0.1.1)
Host is up (0.00011s latency).

PORT   STATE SERVICE
80/tcp open  http

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.01 seconds
Resultado: ./nmap_results/connect_li_20251026_011312.txt
Importante (éticos y legales):
- Solo escanea dispositivos y redes de las que eres propietario o has recibido autorización explícita.
- Los escaneos pueden ser detectados por IDS/IPS, y su uso en redes productivas puede tener consecuencias.
- No uses estos comandos en redes públicas sin autorización previa.
Presiona Enter para continuar...
```

Ver los resultados en nmap_results

```
li@li:~/scriptnmap/nmap_results$ ll
total 20
drwxrwxr-x 2 li   li   4096 oct 26 01:13 ./
drwxrwxr-x 3 li   li   4096 oct 26 01:11 ../
-rw-rw-r-- 1 li   li    375 oct 26 01:13 connect_li_20251026_011312.txt
-rw-rw-r-- 1 li   li    277 oct 26 00:55 ping_li_20251026_005538.txt
-rw-r--r-- 1 root root  468 oct 26 01:02 syn_top_li_20251026_010226.txt
li@li:~/scriptnmap/nmap_results$ cat connect_li_20251026_011312.txt
# Nmap 7.94SVN scan initiated Sun Oct 26 01:13:29 2025 as: nmap -sT -p 80 -v -oN ./nmap_results/connect_li_20251026_011312.txt li
Nmap scan report for li (127.0.1.1)
Host is up (0.00011s latency).

PORT   STATE SERVICE
80/tcp open  http

Read data files from: /usr/bin/../share/nmap
# Nmap done at Sun Oct 26 01:13:29 2025 -- 1 IP address (1 host up) scanned in 0.01 seconds
```

Introduzca 12 para salir

```
=======================================
       NMAP HELPER - MENÚ EDUCATIVO
=======================================
1) Ping scan (descubrir hosts vivos)
2) TCP SYN top 100 (--top-ports 100 -sS)
3) TCP connect scan y puertos personalizados (-sT -p)
4) Detección de servicios y versiones (-sV -sC)
5) Detección de SO (-O)
6) Escaneo UDP (-sU)
7) Escaneo agresivo (-A)
8) NSE scripts (--script)
9) Salida en formatos (-oN, -oX, -oG)
10) Escaneo sin ping (-Pn)
11) Crea tu propia opción para namp
12) Salir
=======================================
Elige opción [1-12]: 12
Importante (éticos y legales):
- Solo escanea dispositivos y redes de las que eres propietario o has recibido autorización explícita.
- Los escaneos pueden ser detectados por IDS/IPS, y su uso en redes productivas puede tener consecuencias.
- No uses estos comandos en redes públicas sin autorización previa.
Saliendo...
```

Si la entrada es un número fuera del rango especificado, aparecerá el siguiente mensaje:

```
========================================
       NMAP HELPER - MENÚ EDUCATIVO
========================================
1) Ping scan (descubrir hosts vivos)
2) TCP SYN top 100 (--top-ports 100 -sS)
3) TCP connect scan y puertos personalizados (-sT -p)
4) Detección de servicios y versiones (-sV -sC)
5) Detección de SO (-O)
6) Escaneo UDP (-sU)
7) Escaneo agresivo (-A)
8) NSE scripts (--script)
9) Salida en formatos (-oN, -oX, -oG)
10) Escaneo sin ping (-Pn)
11) Crea tu propia opción para namp
12) Salir
========================================
Elige opción [1-12]: 144
Opción inválida. Inténtalo de nuevo.
Importante (éticos y legales):
- Solo escanea dispositivos y redes de las que eres propietario o has recibido autorización explícita.
- Los escaneos pueden ser detectados por IDS/IPS, y su uso en redes productivas puede tener consecuencias.
- No uses estos comandos en redes públicas sin autorización previa.
Presiona Enter para continuar...
```