

Relazione – Esplorazione con Nmap

Durante questo esercizio ho avuto modo di esplorare Nmap, uno degli strumenti più famosi e utilizzati per le scansioni di rete. Serve per individuare host attivi, porte aperte e servizi in esecuzione su macchine remote. È molto utile anche in fase di ricognizione, quando si vuole raccogliere informazioni su un obiettivo.

Per iniziare ho aperto il manuale (`man nmap`) che serve a capire meglio come funziona e quali opzioni offre. Nmap ha tantissime possibilità, ma nella pratica ne ho provate alcune tra le più comuni, partendo da quelle più basilari fino ad arrivare a quelle più avanzate.

Ho eseguito una prima scansione con il comando:

```
nmap -A -T4 localhost
```

Questa permette di fare una scansione completa del sistema locale, cercando di identificare i servizi attivi e il sistema operativo, con una velocità di esecuzione aumentata grazie all'opzione `-T4`.

Poi ho eseguito una scansione su rete locale con questo comando:

```
nmap -sn 192.168.50.0/24
```

e ho identificato tutti i dispositivi presenti sulla mia rete locale (senza effettuare una scansione delle porte). Questo mi ha permesso di capire quali IP fossero attivi.

Successivamente ho eseguito una scansione su un host remoto messo a disposizione (`scanme.nmap.org`) con:

```
nmap -A -T4 scanme.nmap.org
```

Qui ho potuto osservare quali porte erano aperte e quali servizi erano disponibili su quell'indirizzo.

Per approfondire ho eseguito una scansione più complessa, dove ho combinato più opzioni:

```
nmap -sS -p 22,80,443 -T4 -A -v --script vuln 192.168.50.100
```

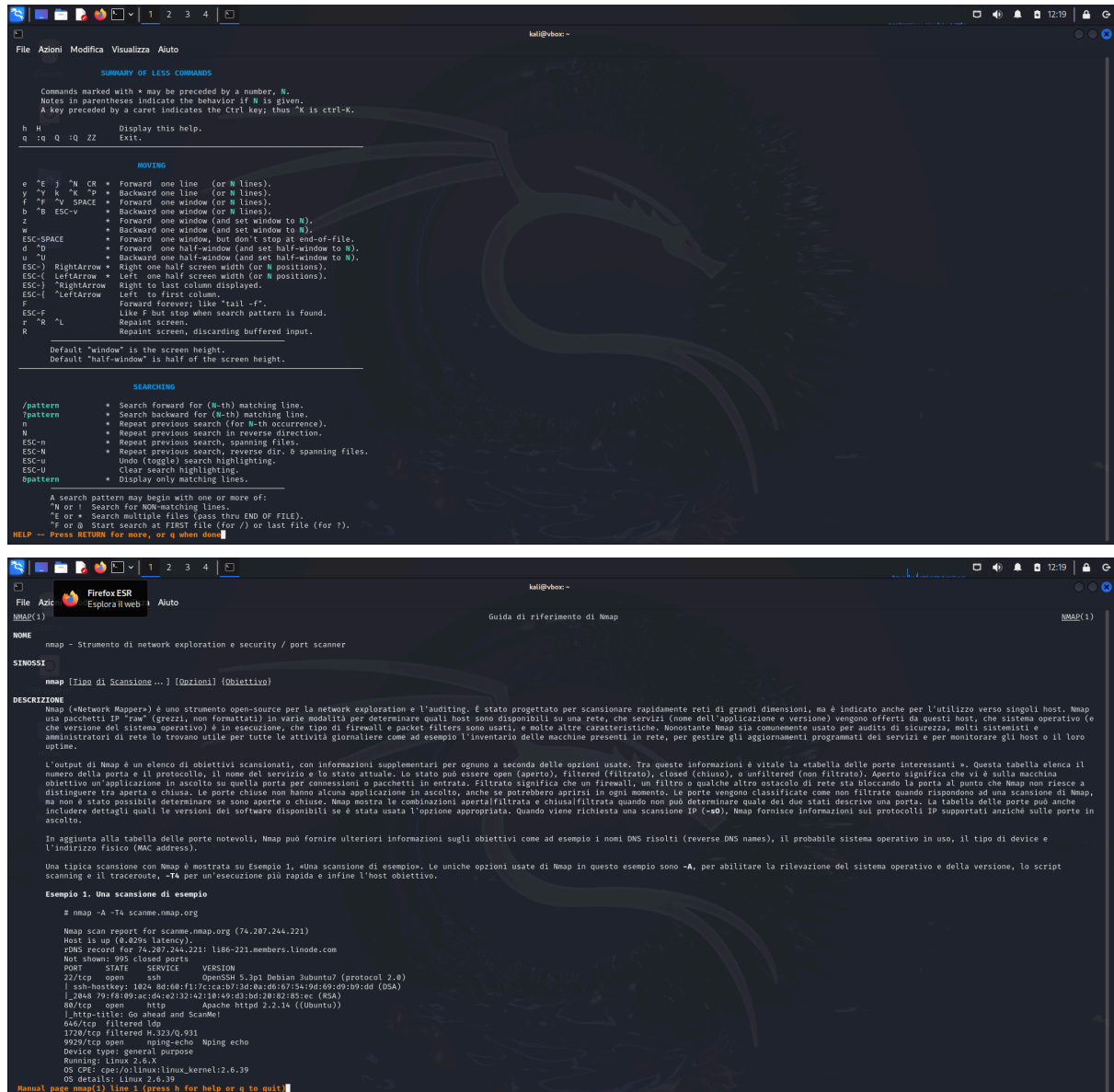
In questo caso:

- `-sS` avvia una scansione stealth (SYN scan),
- `-p` indica le porte specifiche da controllare,
- `-A` attiva l'analisi avanzata (OS detection, version detection, traceroute, ecc),

- **--script vuln** utilizza script per rilevare eventuali vulnerabilità.

Questa scansione ha permesso di vedere più nel dettaglio lo stato di sicurezza dell'host. È un esempio di come, con Nmap, si possano combinare più strumenti per avere un'analisi più completa.

Screenshot



```
kali@vbox: ~  
File Azioni Modifica Visualizza Aiuto  
[kali@vbox]~  
$ nmap -A -iL --reason scanme.nmap.org  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-11 12:26 CEST  
Warning: 45.33.32.156 giving up on port because retransmission cap hit (6).  
[kali@vbox]~  
$ nmap -SS -p 22,80,443 -TA -A -v --script vuln 192.168.50.100  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-11 12:26 CEST  
NSE: Loaded 191 scripts for scanning.  
NSE: Script Pre-scanning.  
Initiating NSE at 12:26  
Completed NSE at 12:27, 10.02s elapsed  
Initiating NSE at 12:27  
Completed NSE at 12:27, 0.00s elapsed  
Initiating Parallel DNS resolution of 1 host. at 12:27  
Completed Parallel DNS resolution of 1 host. at 12:27, 0.04s elapsed  
Initiating SYN Stealth Scan at 12:27  
Scanning 192.168.50.100 [3 ports]  
Completed SYN Stealth Scan at 12:27, 0.03s elapsed (3 total ports)  
Initiating Service scan at 12:27  
Initiating OS detection (try #1) against 192.168.50.100  
Retrying OS detection (try #2) against 192.168.50.100  
NSE: Script scanning 192.168.50.100.  
Initiating NSE at 12:27  
Completed NSE at 12:27, 0.01s elapsed  
Initiating NSE at 12:27  
Completed NSE at 12:27, 0.00s elapsed  
Nmap scan report for 192.168.50.100  
Host is up (0.000000s latency).  
  
PORT      STATE SERVICE VERSION  
22/tcp    closed ssh  
80/tcp    closed http  
443/tcp   closed https  
Too many fingerprints match this host to give specific OS details  
Network Distance: 0 hops  
NSE: Script Post-scanning.  
Initiating NSE at 12:27  
Completed NSE at 12:27, 0.00s elapsed  
Initiating NSE at 12:27  
Completed NSE at 12:27, 0.00s elapsed  
Read data files from: /usr/share/nmap  
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 12.22 seconds  
Raw packets sent: 15 (1.800KB) | Rcvd: 28 (2.868KB)  
[kali@vbox]~  
$  
  
[kali@vbox]~  
$ man nmap  
[kali@vbox]~  
$ nmap -A -iL localhost  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-11 12:21 CEST  
Nmap scan report for localhost (127.0.0.1)  
Host is up (0.000074s latency).  
Other addresses for localhost (not scanned): ::1  
All 1000 scanned ports on localhost (127.0.0.1) are in ignored states.  
Not shown: 1000 closed tcp ports (reset)  
Too many fingerprints match this host to give specific OS details  
Network Distance: 0 hops  
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 2.40 seconds  
[kali@vbox]~  
$ nmap -sn 192.168.50.0/24  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-11 12:21 CEST  
Nmap scan report for 192.168.50.1  
Host is up (0.00043s latency).  
MAC Address: 08:00:27:C6:0F:A9 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
Nmap scan report for 192.168.50.100  
Host is up  
Nmap done: 256 IP addresses (2 hosts up) scanned in 2.34 seconds  
[kali@vbox]~  
$ nmap -A -iL scanme.nmap.org  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-11 12:22 CEST  
Warning: 45.33.32.156 giving up on port because retransmission cap hit (6).  
[kali@vbox]~  
$
```

Conclusioni

L'esercizio mostra le potenzialità e l'utilità di Nmap e serve a capire quanto possa essere potente anche con pochi comandi. Naturalmente è importante usare questi strumenti con consapevolezza, anche in un contesto etico e legale.