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
```

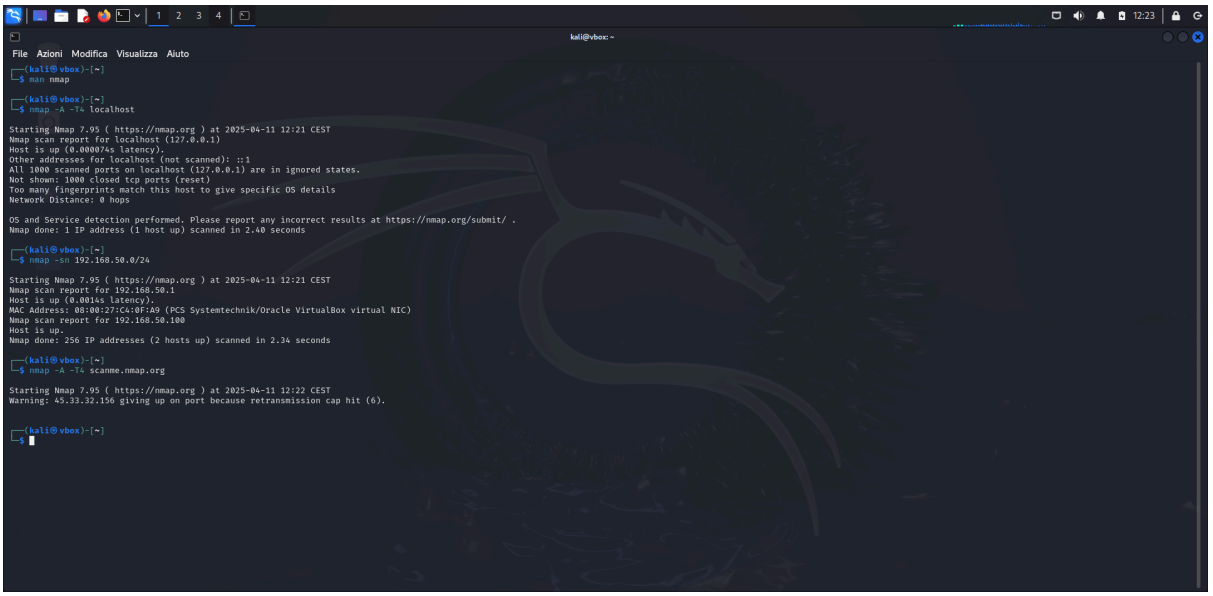
In questo caso:

- `-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



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.