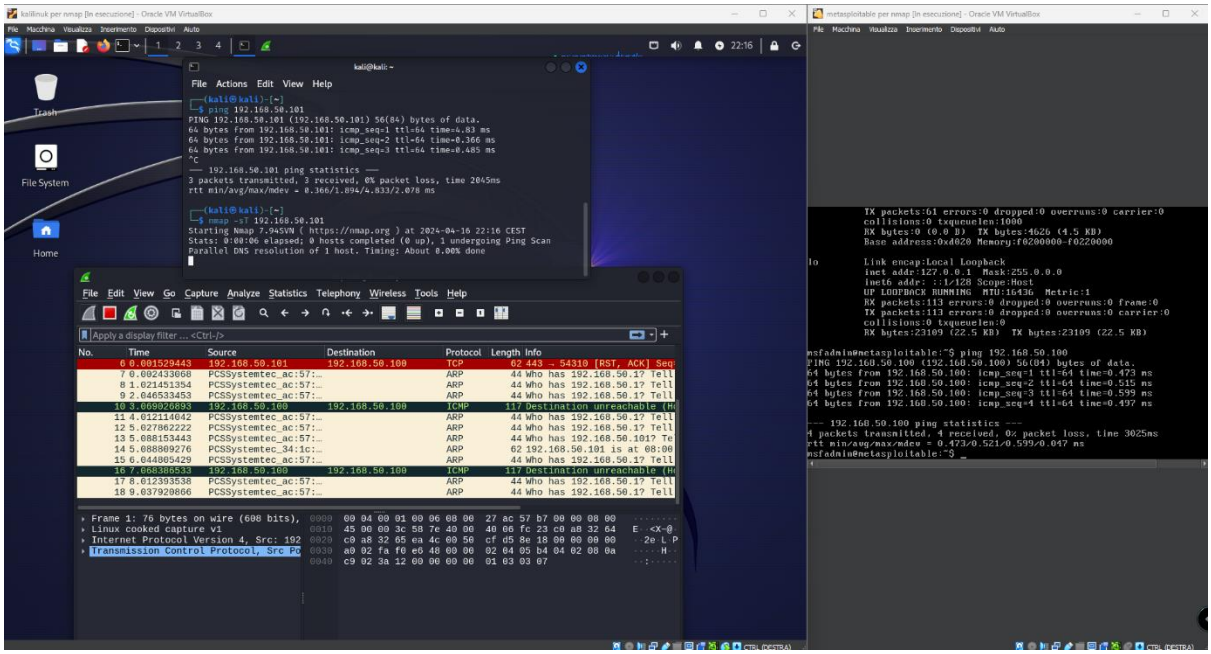
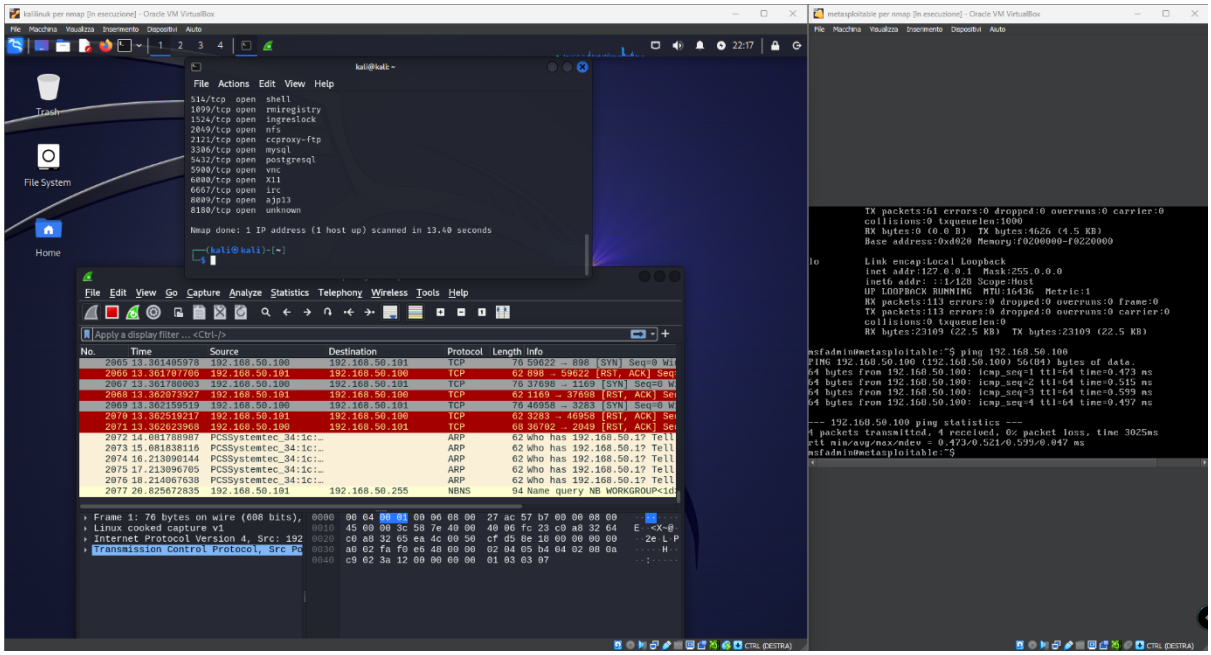
Tipi di scansioni Nmap

Il fulcro dell'esercizio di oggi era nel confrontare e nel valutare le differenze dei dati raccolti nei diversi tipi scansione con Nmap, vediamoli:



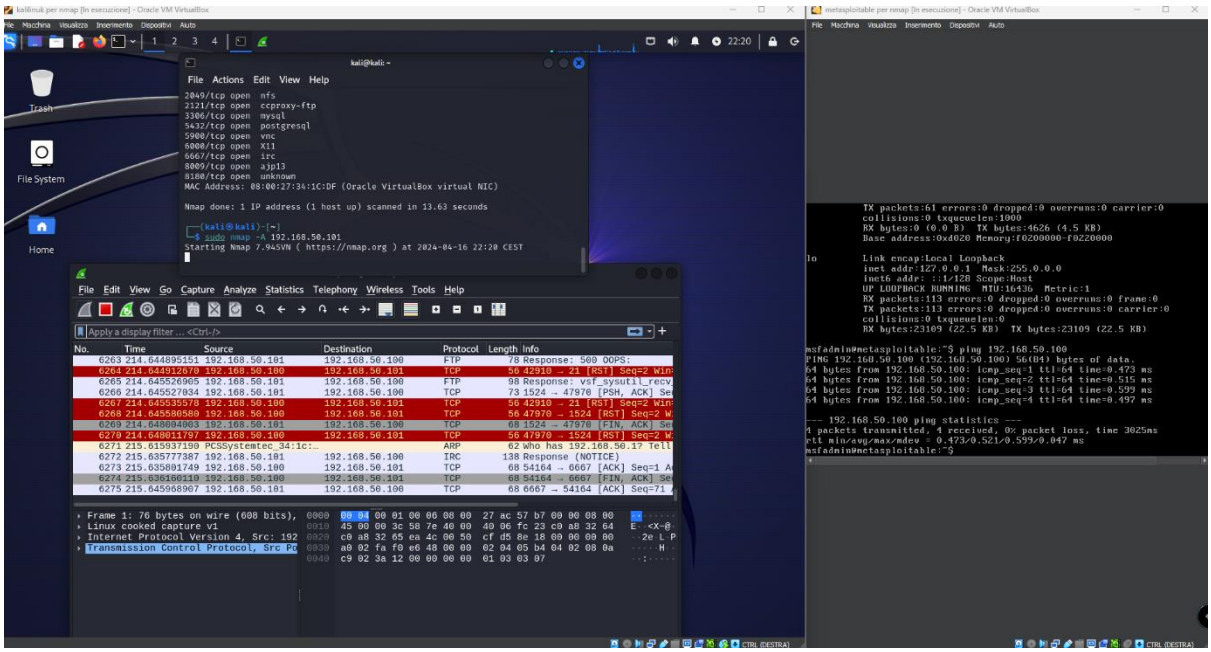
nmap -sT <indirizzo_IP>

Scansione TCP (o scansione completa): Questa è la scansione più basilare e completa, nota anche come scansione connect(), poiché Nmap tenta di completare la connessione TCP con ogni porta specificata. Esegue il normale "handshake" a tre vie per stabilire una connessione TCP completa: SYN, SYN-ACK, ACK. Se la porta è in ascolto, la connessione sarà stabilita, altrimenti verrà rifiutata. Questo metodo è facile da rilevare e loggare dai sistemi di rilevamento intrusioni.



nmap -sS <indirizzo_IP>

Scansione SYN (o scansione stealth): Invece di aprire una connessione TCP completa, questa scansione invia solo un pacchetto SYN e aspetta una risposta. Se riceve un pacchetto SYN-ACK, significa che la porta è aperta; se riceve un RST, significa che la porta è chiusa. La scansione SYN non completa il "handshake" TCP e quindi è meno invasiva e meno probabile che sia registrata dai sistemi di sicurezza, da qui il termine "stealth" (occultamento).



nmap -sA <indirizzo_IP>

Scansione con switch -A (ACK scan): Questa scansione viene utilizzata per mappare le regole di filtraggio di un firewall, inviando pacchetti ACK non sollecitati. Il firewall, basato sulle sue regole, potrebbe lasciar passare questi pacchetti, bloccarli o alterarli. L'ACK scan non è usato per determinare se una porta è aperta o chiusa, ma piuttosto per comprendere come il firewall sta manipolando il traffico.

```
8312 275.735094027 192.168.50.100 192.168.50.101 TCP 68 50396 → 80 [FIN, ACK] Seq=19 Ack=1067 Win=64128 Len=0 TSval=
8313 275.735812571 192.168.50.101 192.168.50.100 TCP 68 80 → 50396 [ACK] Seq=1067 Ack=20 Win=5888 Len=0 TSval=28222
8314 275.736058469 192.168.50.100 192.168.50.101 TCP 76 50408 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TS
8315 275.736328946 192.168.50.101 192.168.50.100 TCP 76 80 → 50408 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SA
8316 275.736461401 192.168.50.100 192.168.50.101 TCP 68 50408 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=337264209
```

Qui si riassume la fonte dello scan, il target ecc….

Conclusione:

Le tracce di una scansione TCP completa mostreranno l'intero processo di handshake a tre vie se la porta è aperta.

Le tracce di una scansione SYN mostreranno molti pacchetti SYN inviati senza i corrispondenti pacchetti ACK se le porte sono filtrate o chiuse.

Le tracce di una scansione ACK riveleranno come i pacchetti ACK non sollecitati vengono trattati dal firewall o dal filtro di rete, fornendo indizi sulla configurazione delle regole del firewall.