W9D1

SCANSIONE DI SERVIZI DI RETE

La traccia

La traccia prevede di svolgere un esercizio di scansione dei servizi di rete:

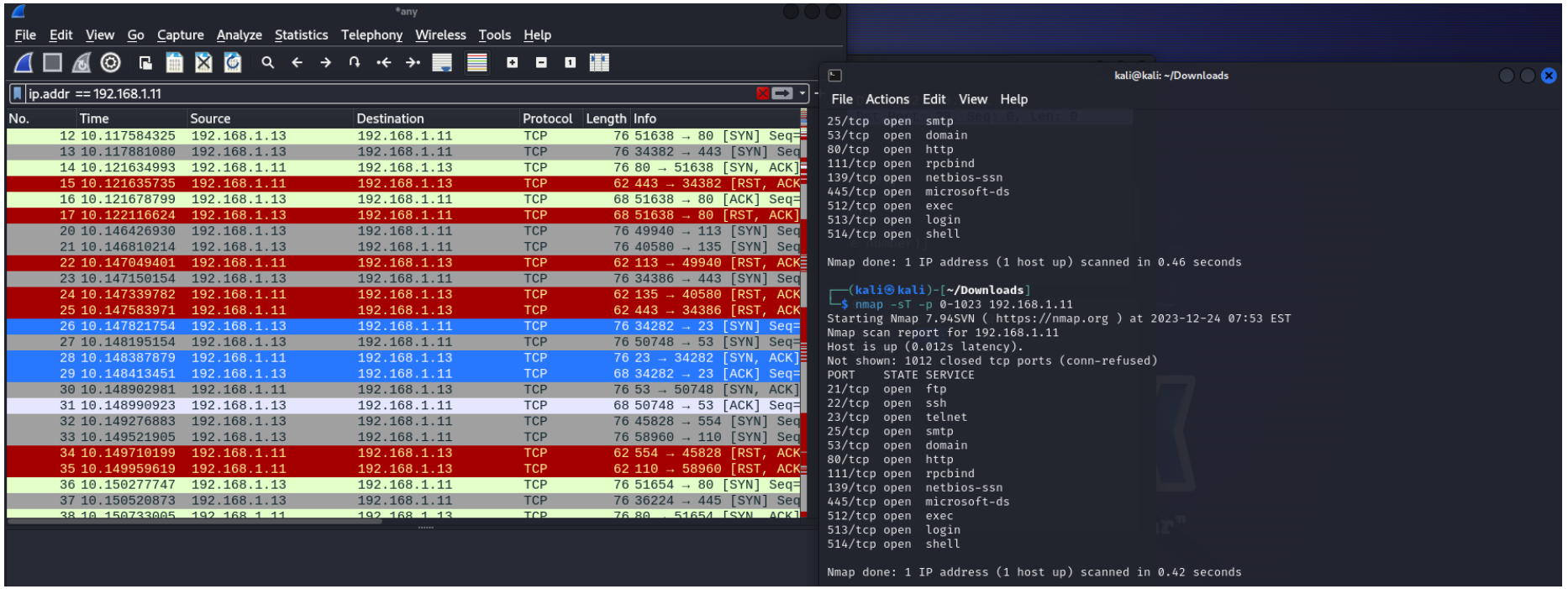
Vedremo da vicino nmap e i suoi comandi.
Sulle base delle nozioni viste nella lezione teorica eseguiremo diversi tipi di scan sulla macchine metasploitable, come di seguito:

- Scansione TCP sulle porte well-known
- Scansione SYN sulle porte well-known
- Scansione con switch «-A» sulle porte well-known

Evidenziare la differenza tra la scansione completa TCP e la scansione SYN intercettando le richieste inviate dalla macchine sorgente con Wireshark.

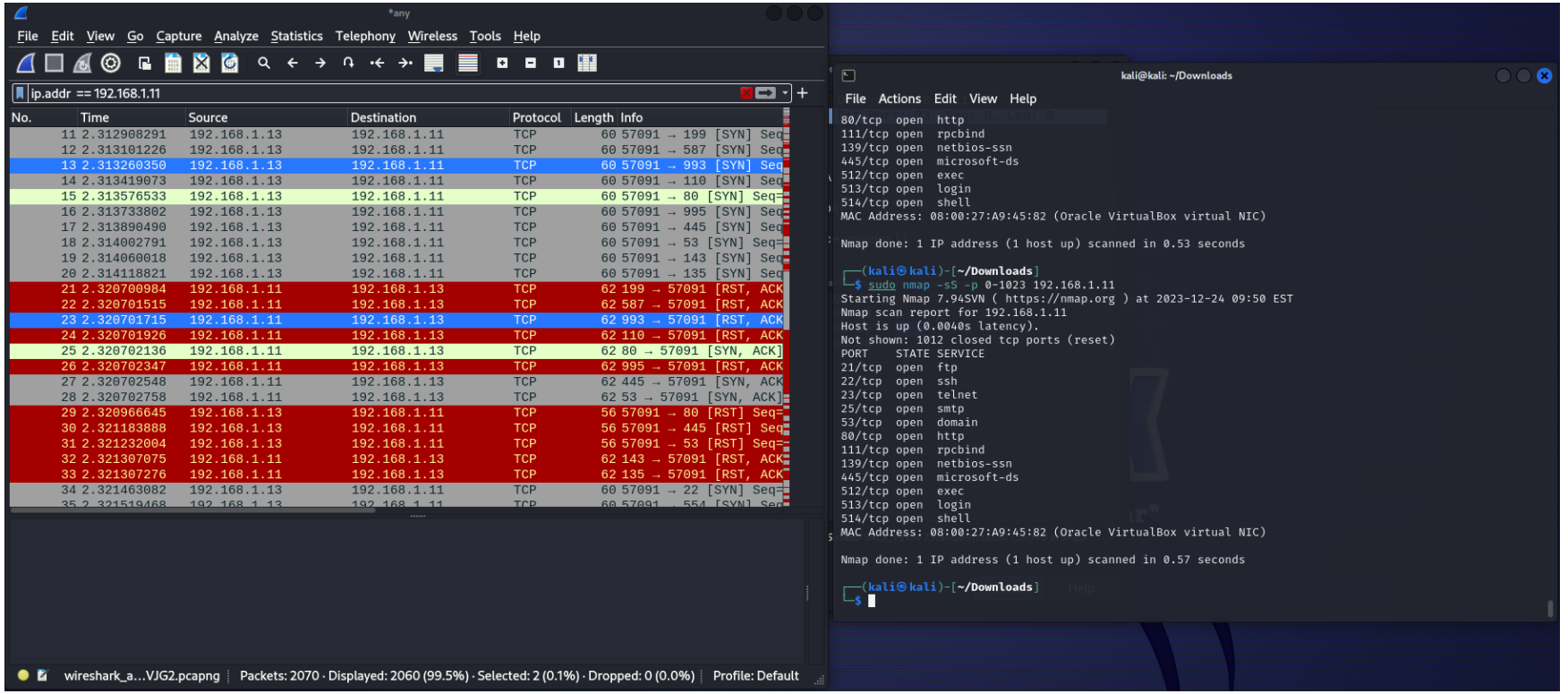
Scansione Tcp

In questo caso, durante la scansione TCP delle well-known ports possiamo osservare che nmap completa i 3 passaggi del 3 way handshake.



Scansione Syn

In questo caso, durante la scansione SYN delle well-known ports possiamo osservare che nmap NON completa i 3 passaggi del 3 way handshake.



Scansione -A

In questo caso, durante la scansione -A delle well-known ports possiamo osservare che nmap completa i 3 passaggi del 3 way handshake e aggiunge diverse informazioni.