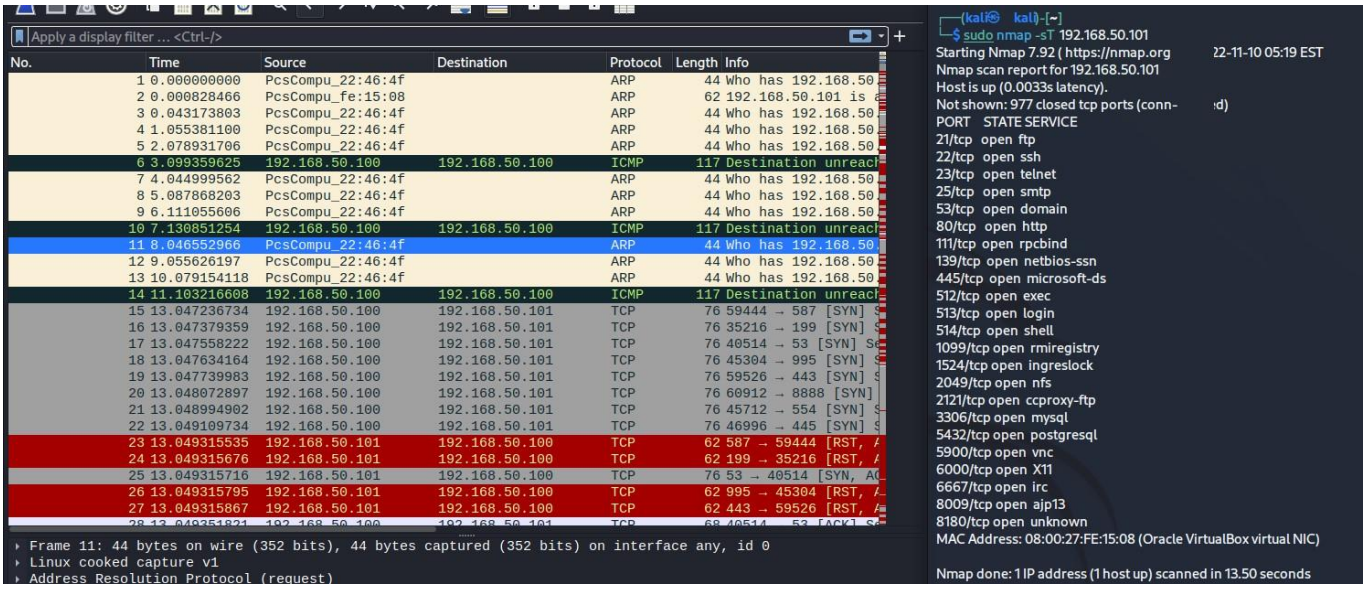
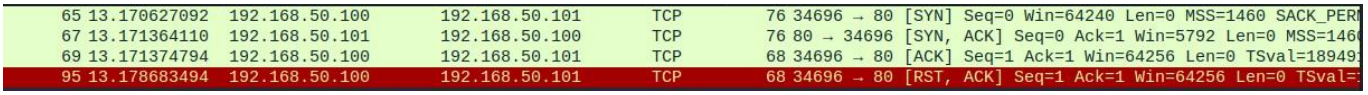
NMAP

Scansione nmap con wireshark da kali 192.168.50.100 a metasploitable2 192.168.50.101

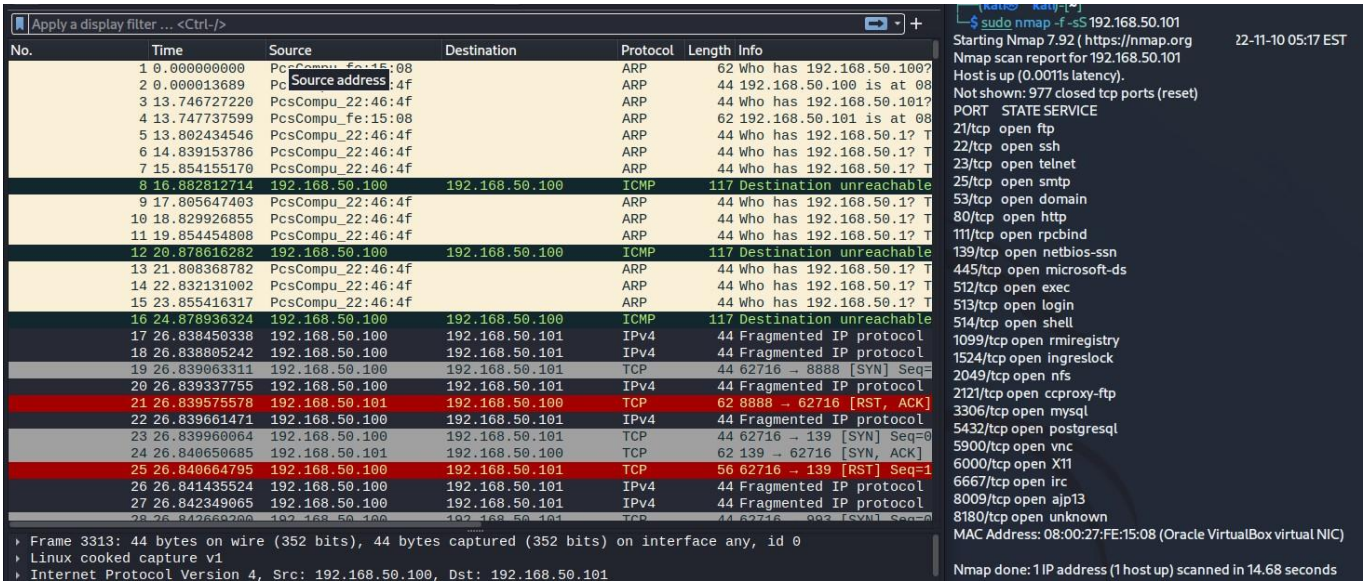
Scansione TCP >nmap -sT 192.168.50.101

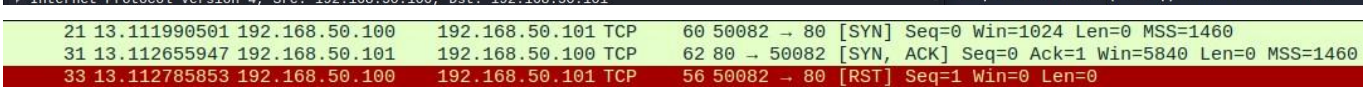




in totale c'è stato un traffico di circa 2000 pacchetti, e qui sopra c'é la cattura della porta 80 con la sequenza corretta.

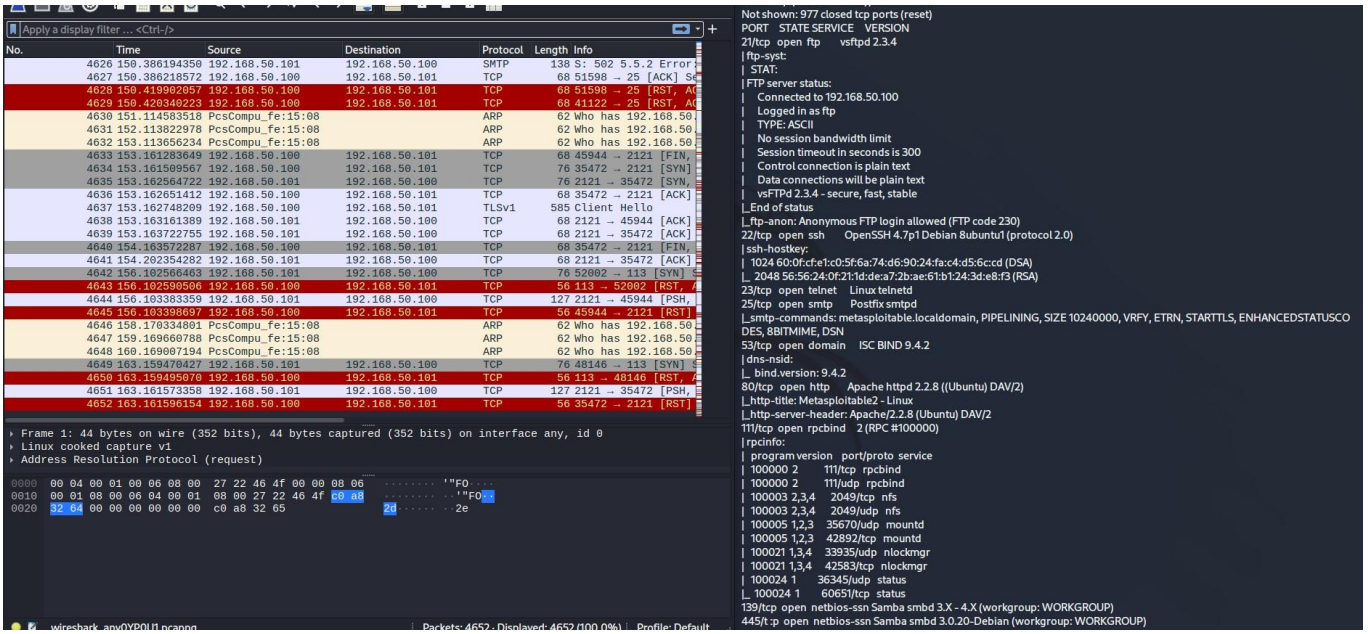
Scansione SYN >nmap -sS 192.168.50.101

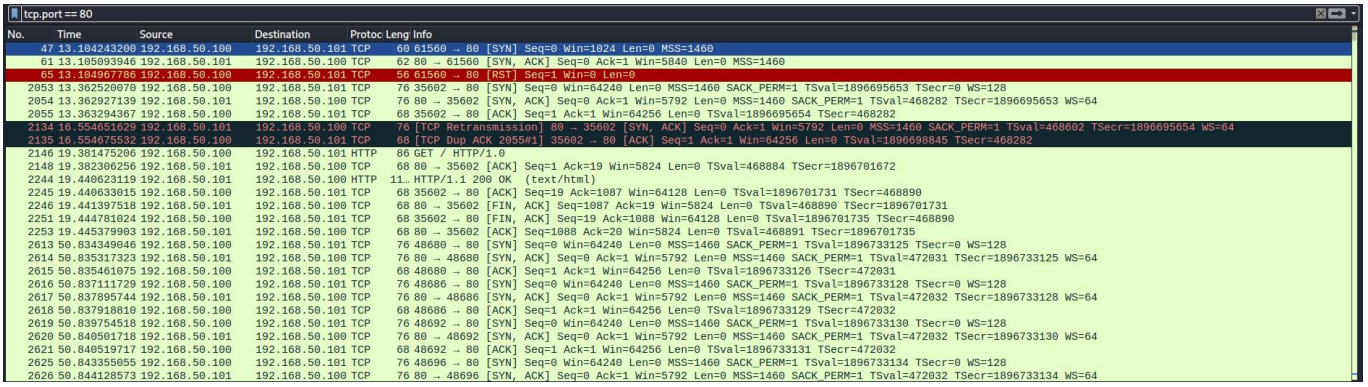




in totale c'è stato un traffico di circa 4000 pacchetti, e qui sopra c'é la cattura della porta 80 con la sequenza corretta.

Scansione ALL >nmap -A 192.168.50.101





in totale c'è stato un traffico di circa 4600 pacchetti, e qui sopra c'è la cattura della porta 80. Con lo scan all possiamo vedere molte piú informazioni rispetti agli altri due tipi di scan.

La differenza tra TCP(-sT>Scan TCP) e SYN(-sS>Scan Stealth) é che il TCP completa il 3 way handshake mentre SYN non lo completa ed é meno rilevabile rispetto al TCP scan.
Questo lo possiamo notare giá dagli screen in alto con la sequenza dei pacchetti.