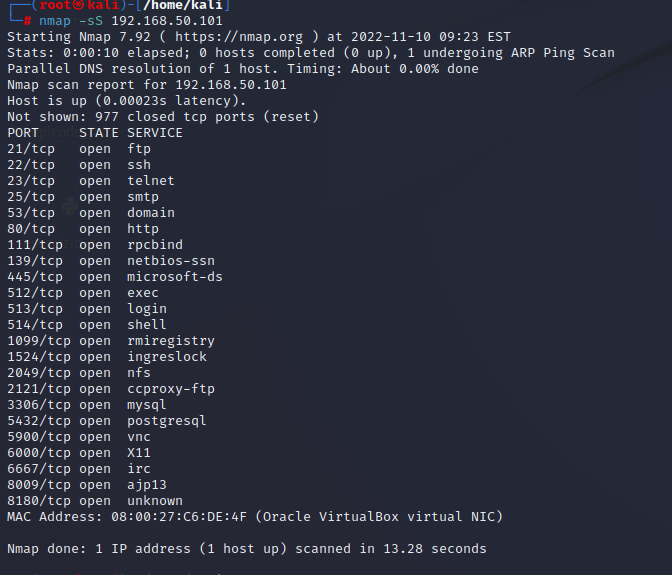
REPORT SCAN

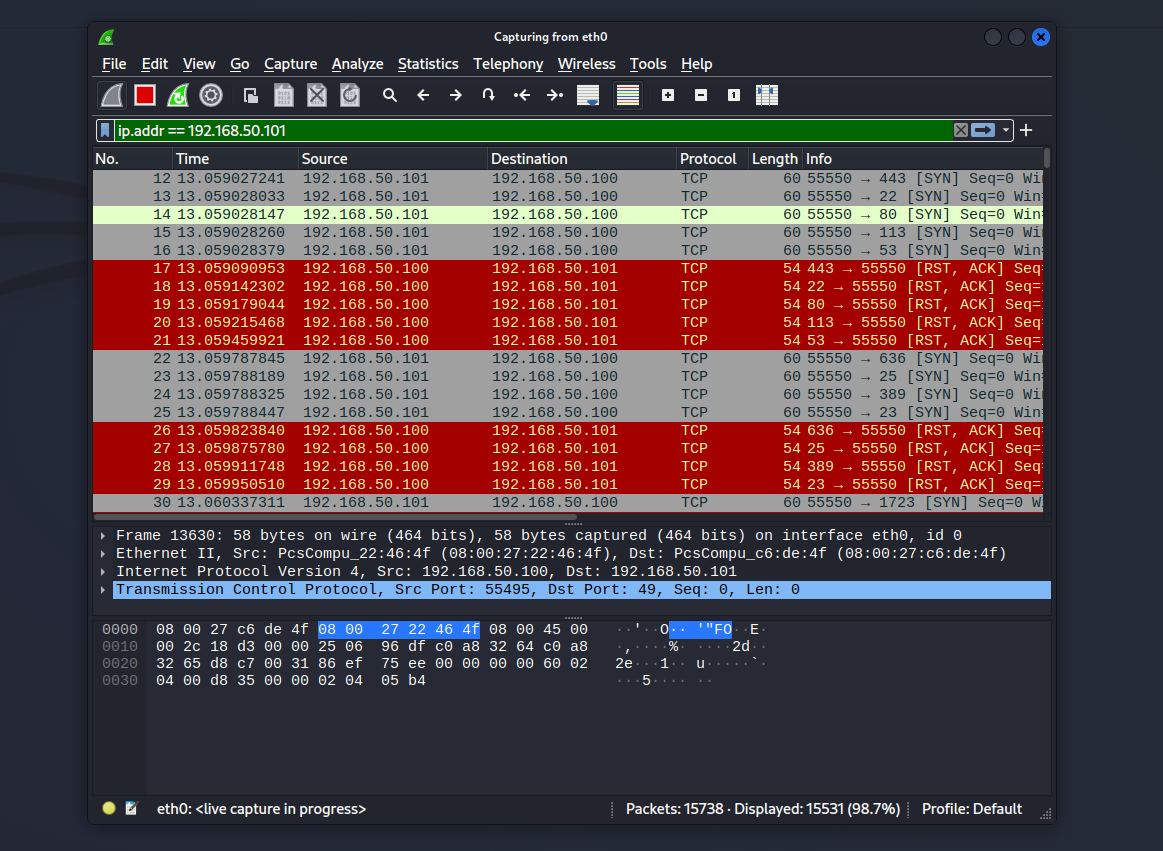
* Scan tcp sulle porte well-known
* Scan SYN sulle porte well-known
* Scansione switch <-A> sulle porte well-known

Per questo esercizio abbiamo utilizzato diverse tecniche di port scanning:

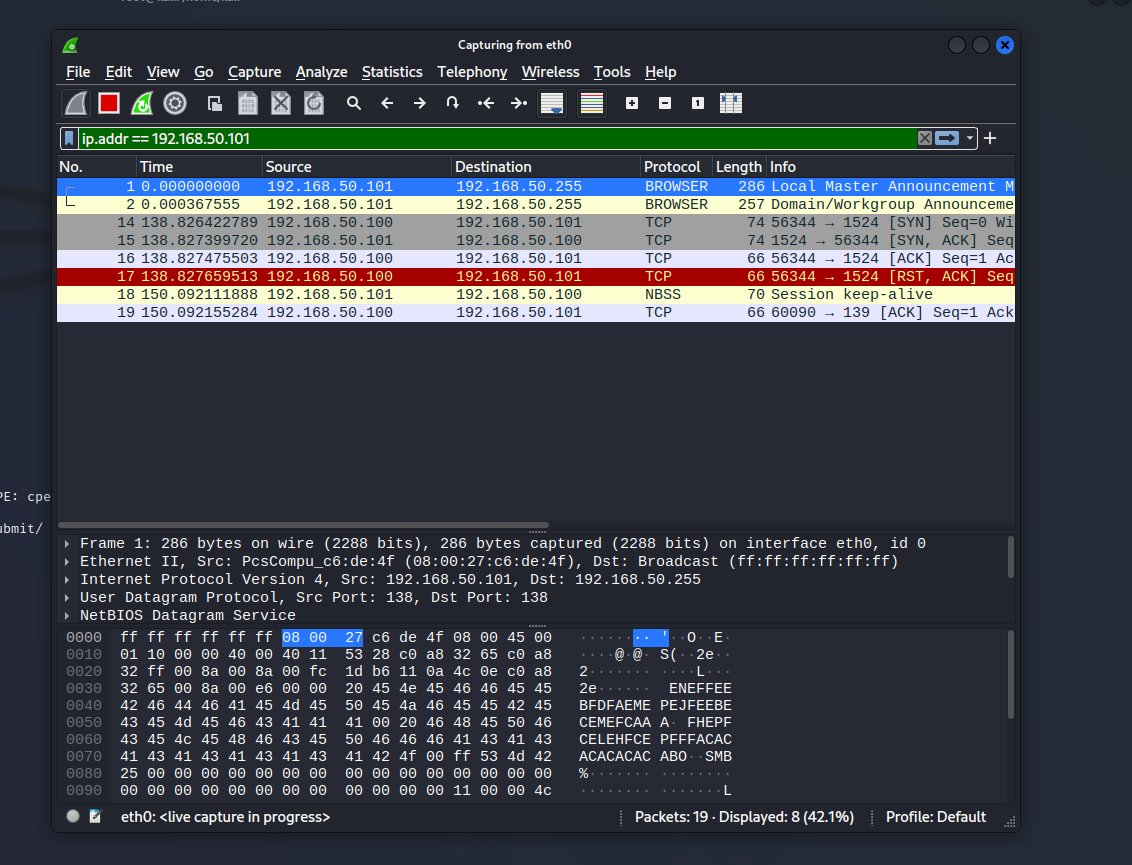


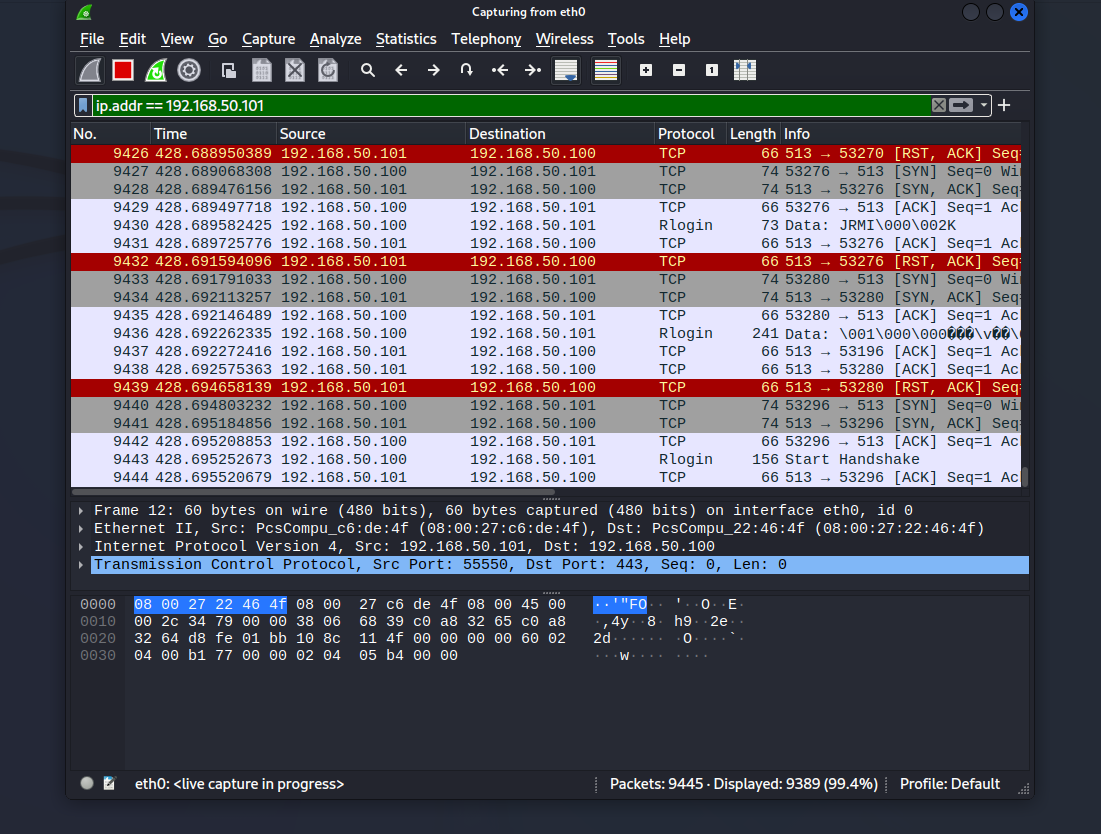
Con << -sS>> possibile effettuare una veloce scansione su migliaia di porte al secondo su una rete veloce. Il SYN scan è però poco invasivo anche se permette una differenziazione chiara tra delle porte dividendole in open/filtered/closed.

Possiamo quindi 23 porte aperte di un host in 13.28 secondi.



In questo caso grazie a Wireshark noteremo un SYN che non riceve risposta in quanto questo tipo di scan è un half-open scan, perché non viene aperta una connessione TCP completa.

Con <<-sT>> ossia una scansione di tipo connect , questo tipo di scan assicura la connessione tra le porte in ascolto via three-way handshaketra la sorgente ed il target. In questo caso la cattura wireshark apparirà come in figura.

Infine con lo switch andiamo a restringere il range di ricerca ottenendo una cattura di dati più approfondita

Inoltre utilizzando diversi comandi è stato possibile effettuare scan più approfonditi

