SCANSIONE TCP CON NMAP (sT)

- **FONTE DELLO SCAN: METASPLOITABLE**
- **TARGET DELLO SCAN: porte 1-1024 (WELL KNOWN)**
- **TIPO DI SCAN: TCP**

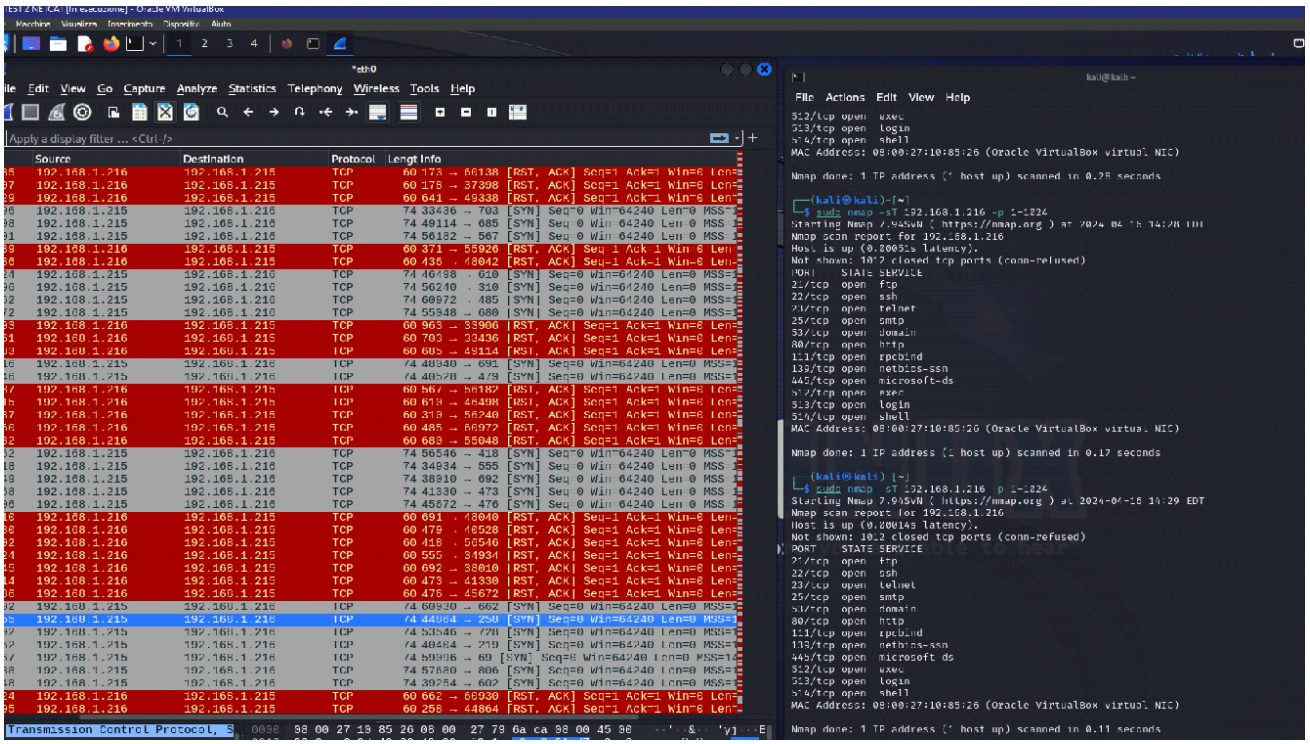
SVOLGIMENTO

Utilizziamo il comando:

sudo nmap -sT 192.168.1.216 -p 1-1024

Effettuiamo lo scan delle porte e la rilevazione dell'invio di pacchetti mediante Wireshark.
Possiamo da subito vedere i risultati: per le porte chiuse, con lo scan sT la macchina target ci invierà dei pacchetti con i flag [RST, ACK].

Le porte aperte invece mostreranno un



SCANSIONE SYN CON NMAP

FONTE DELLO SCAN: METASPLOITABLE

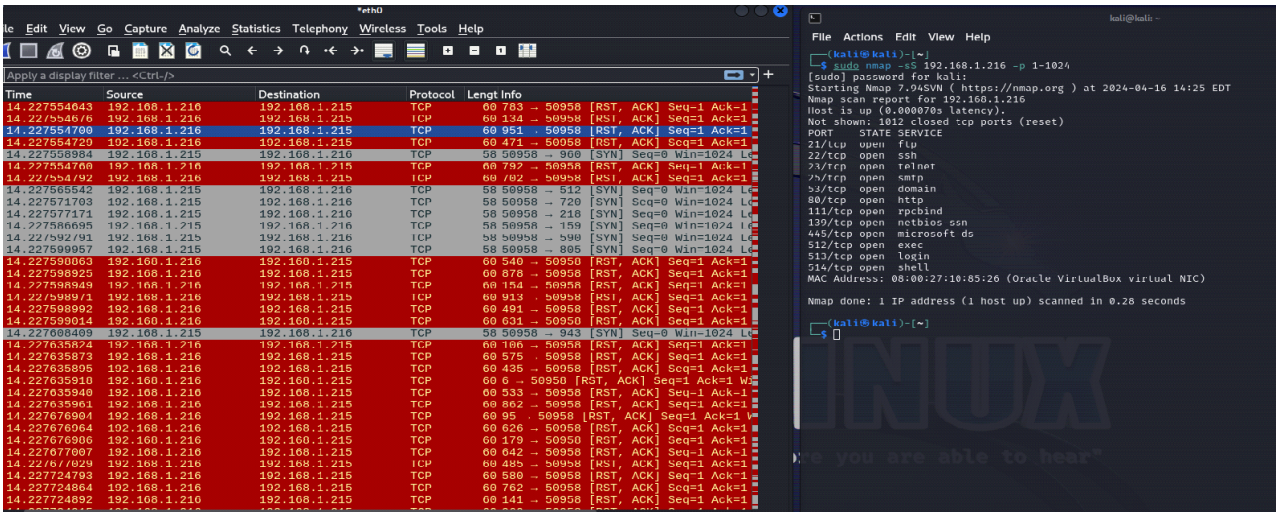
TARGET DELLO SCAN: Porte 1-1024

TIPO DI SCAN: SYN

SVOLGIMENTO

Utilizziamo il comando:
sudo nmap -sS 192.168.1.216 -p 1-1024

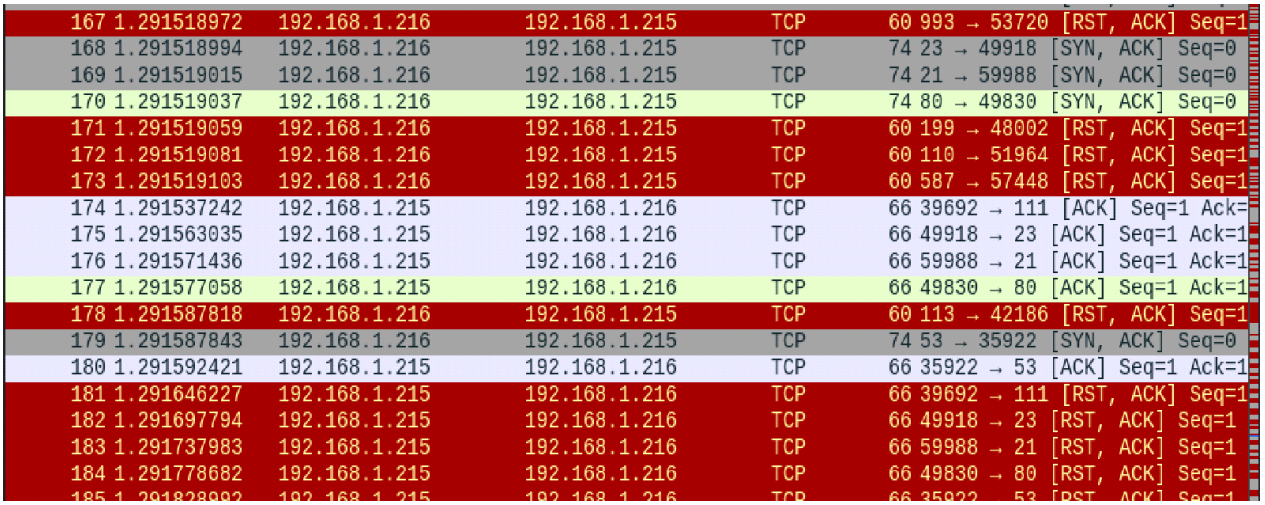
Avviamo la scansione con Wireshark. I pacchetti vengono catturati e mostrano le caratteristiche dello scan con il SYN.



-sS sono richieste dove il TCP handshake non viene concluso, ma viene inviato solamente il pacchetto SYN.

-I pacchetti con un [RST,ACK] segnalano che la porta è chiusa, e non ci sono servizi attivi.

- le porte aperte vengono segnalate con un pacchetto [SYN, ACK]. Tuttavia, poiché nella scansione SYN l'obiettivo è non portare a termine il 3way handshake, viene immesso un RST, ACK in modo da interromperlo.



SCANSIONE CON SWITCH -A CON NMAP

- **FONTE DELLO SCAN: METASPLOITABLE**
- **TARGET DELLO SCAN: porte 1-1024**

- **TIPO DI SCAN: TCP -A**

SVOLGIMENTO

Effettuiamo lo scan con Nmap usando il comando:
sudo nmap -A 192.168.1.216 -p 1-1024

Lasciamo che Wireshark colga i pacchetti scansionati.

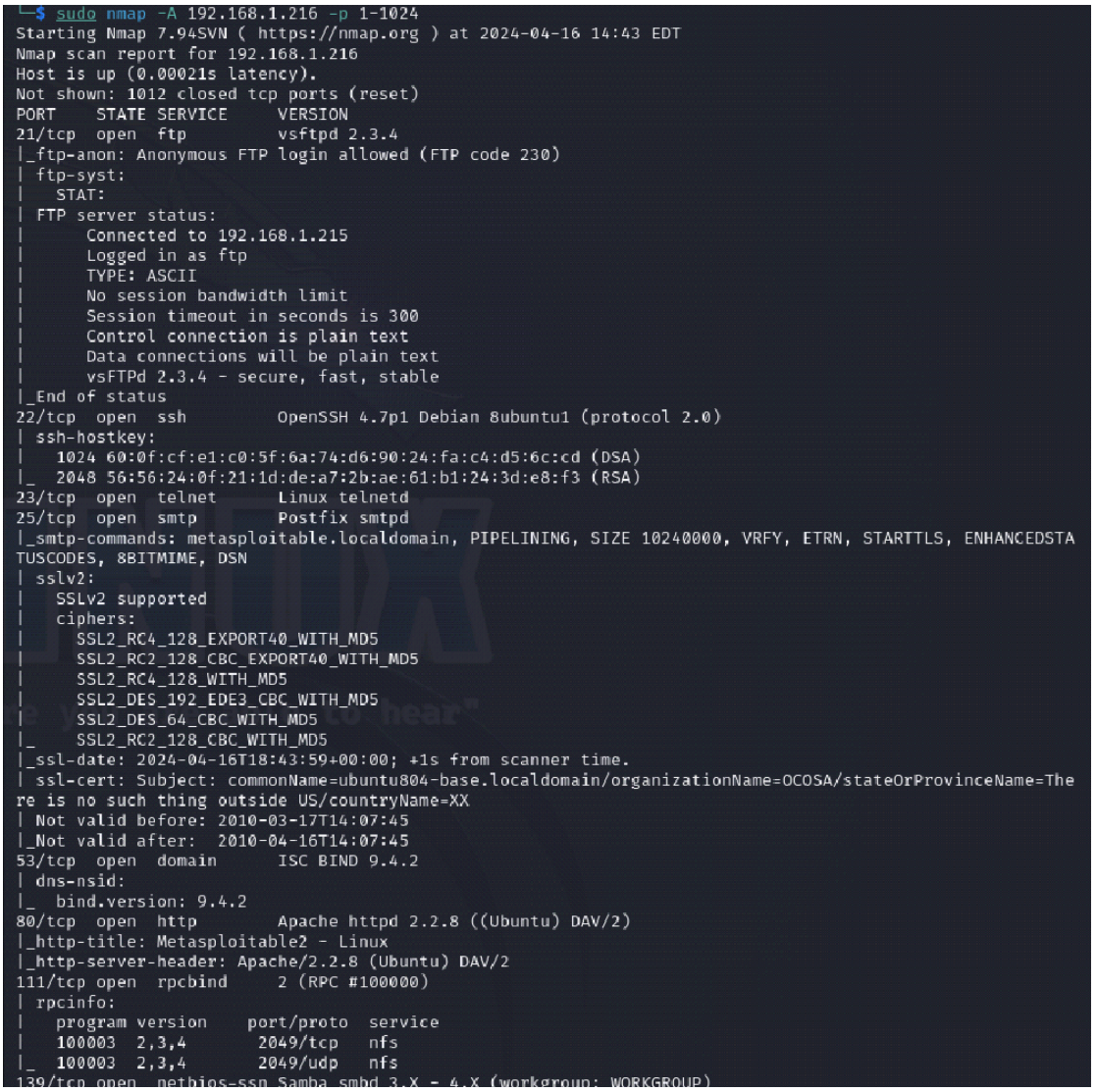
A differenza degli scan precedenti, il processo di scansione impiega maggiore tempo, portando con sé però numerose altre informazioni riguardanti le porte e il sistema scansionato.

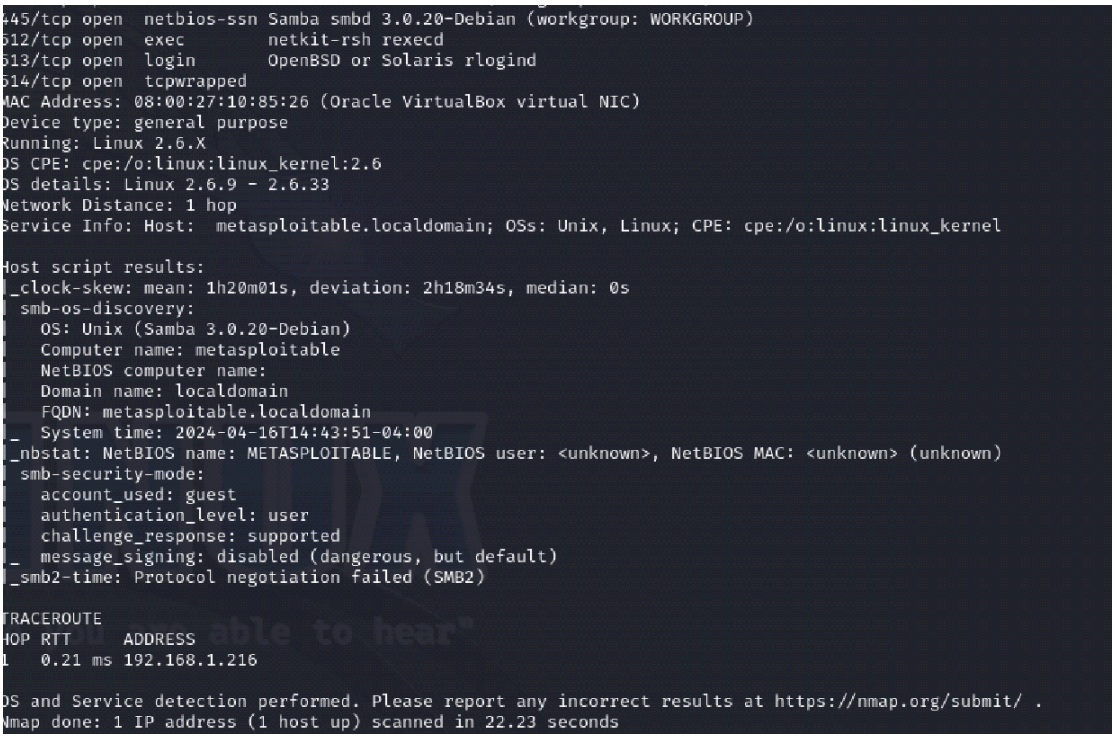
Lo switch -A fornisce una visione molto più approfondita dello scan con Nmap.

- Viene fornito lo stato del server FTP.

- Viene fornito il nome del sistema operativo e della macchina analizzata (Unix - Metasploitable)

- Viene fornito il nome del dominio





DIFFERENZE TRA TCP E SYN

La differenza tra scan TCP (-sT) e SYN (-sS) che possiamo verificare da queste analisi sta nel modo in cui la macchina si comporta a seconda della scansione.

Nel primo caso, i pacchetti effettuano il ciclo completo del 3way handshake, creando un rumore maggiore all'interno del network.

Per quanto riguarda il SYN scan, quando si rileva una porta aperta il ciclo viene interrotto volontariamente.