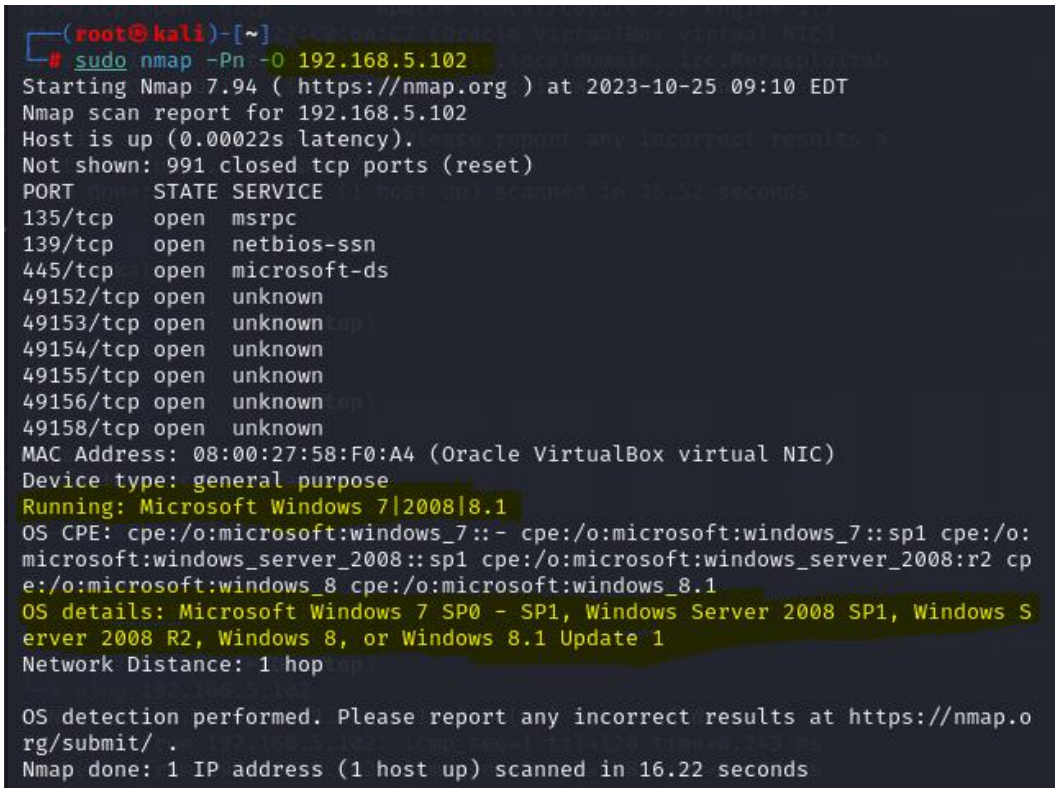
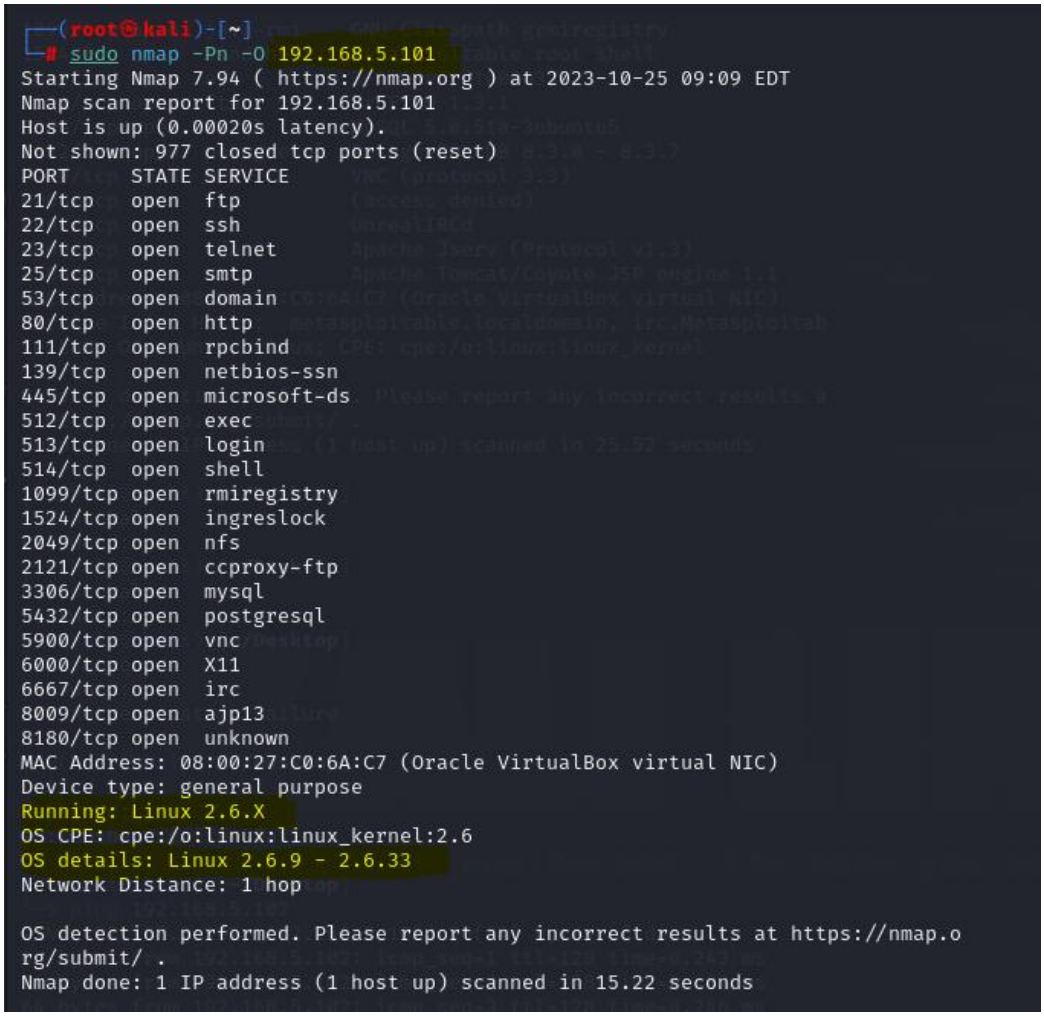
OS FINGER PRINT W7



IP: 192.168.5.101
OS: W7
PORTE APERTE: 135/msrpc porta usata per le comunicazioni
139/netbios-ssn porta usata per le comunicazioni di rete, usata in passato.
445/microsoft-ds porta usata per il protocollo SMB (Server Message Block) su reti Windows.

Qui possiamo osservare che il comando nmap scannerizza ip di W7 e mostra sia le porte aperte, il servizio ed il sistema operativo del dispositivo

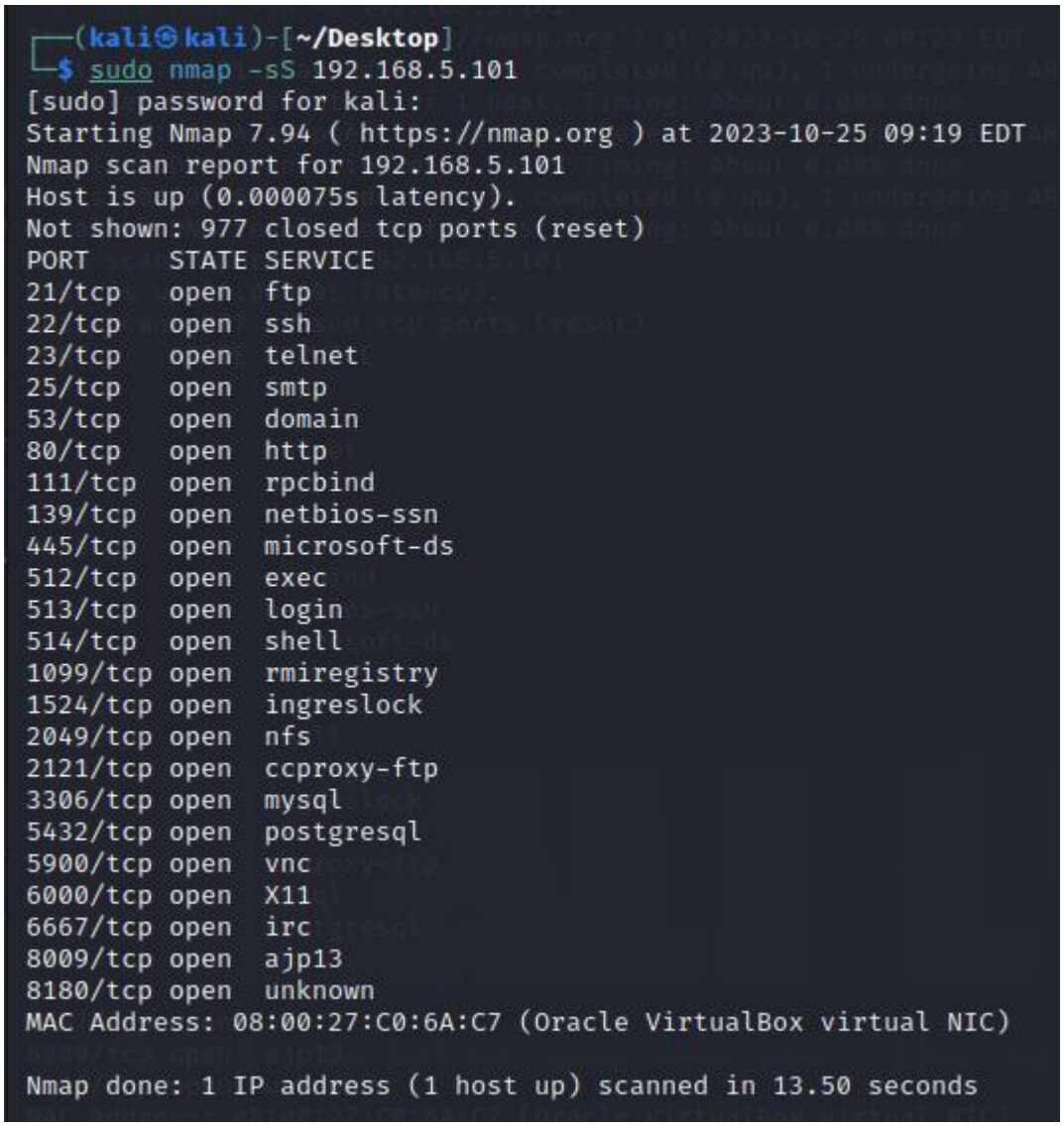
OS FINGER PRINT META



IP: 192.168.5.101
OS: W7
PORTE APERTE: tutte quella nell'immagine, che vengono ad essere le porte piu comuni.

Qui possiamo osservare che il comando nmap scannerizza ip di META e mostra sia le porte aperte, il servizio ed il sistema operativo del dispositivo.
Addifferenza di W7, Meta mostra piu porte aperte.

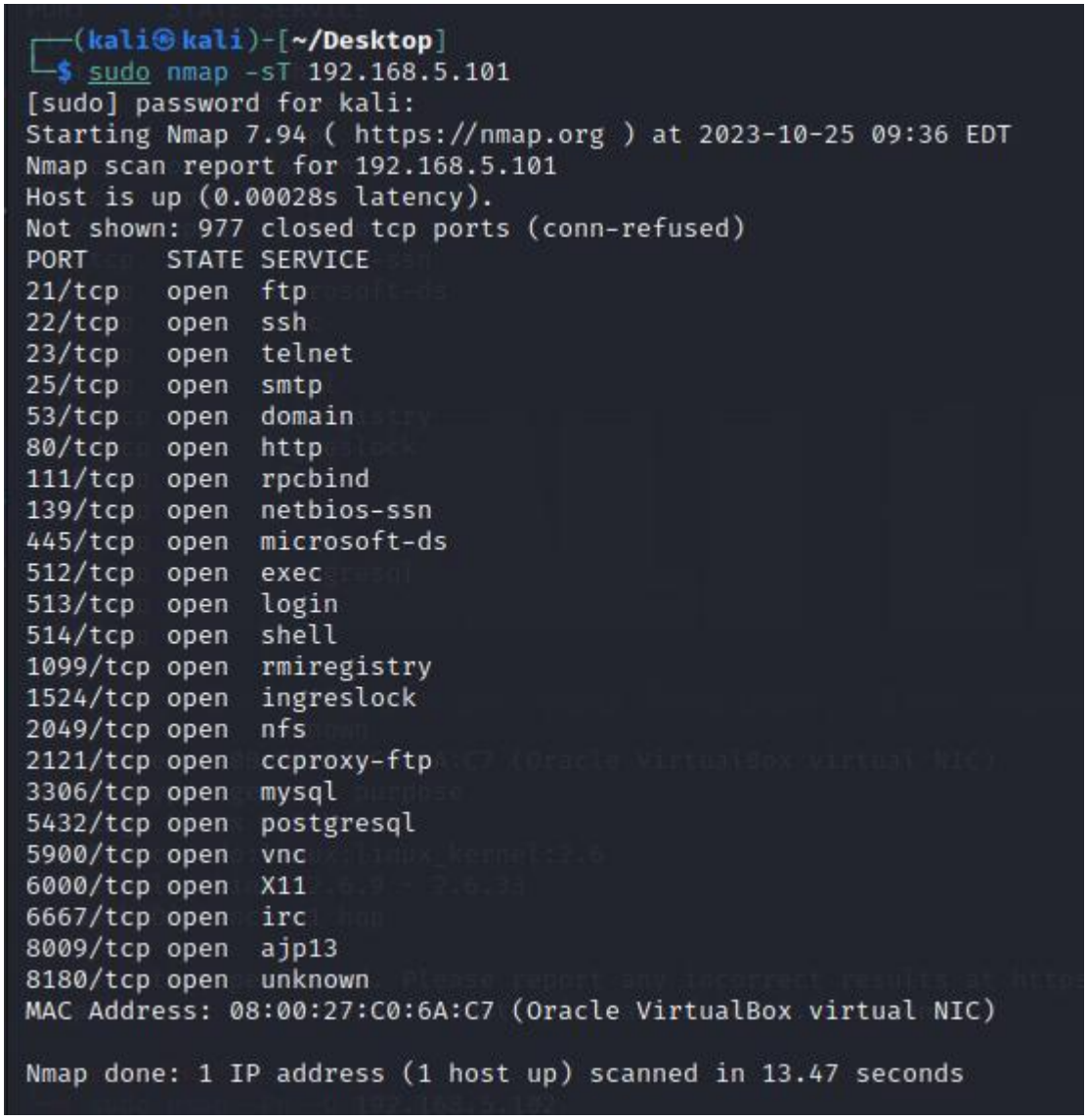
SYN SCAN META



Comando nmap, usando il metodo “sS”, scannerizza le porte aperte ni modo meno invasivo.

Il pacchetto non conclude il 3 way handshake, si interrompe nella fase SYN/ACK, per rimandare indietro NON ACK ma RST(reset).

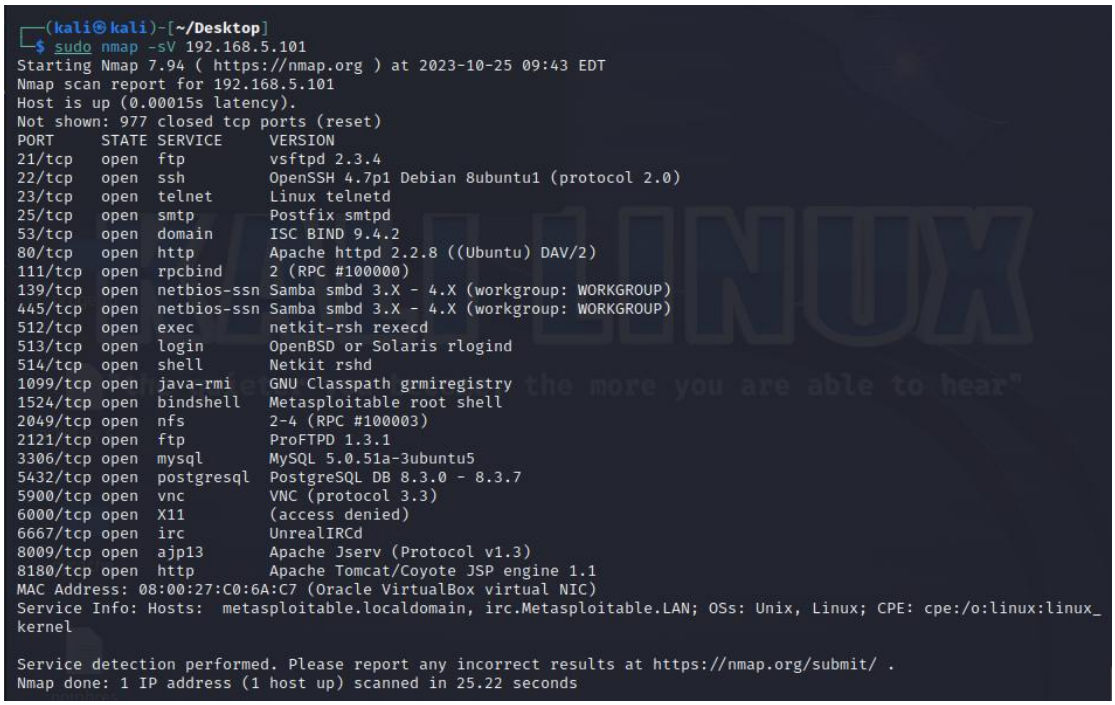
TCP CONNECTION META



Comando nmap, usando il metodo “sT”, scannerizza le porte aperte ni modo molto invasivo/rumoroso.

Il pacchetto conclude il 3 way handshake, a differenza del “sS”, quindi recupera info sullo stato della porta, ma crea grosse congestioni di rete per quanto invasivo sia.

VERSION DETECTION META



Comando nmap, usando il metodo “sV” esegue ua scansione abilitando la feature di “version detection”, grazie alla quale oltre al servizio recuperiamo anche la versione e relativi dettagli.