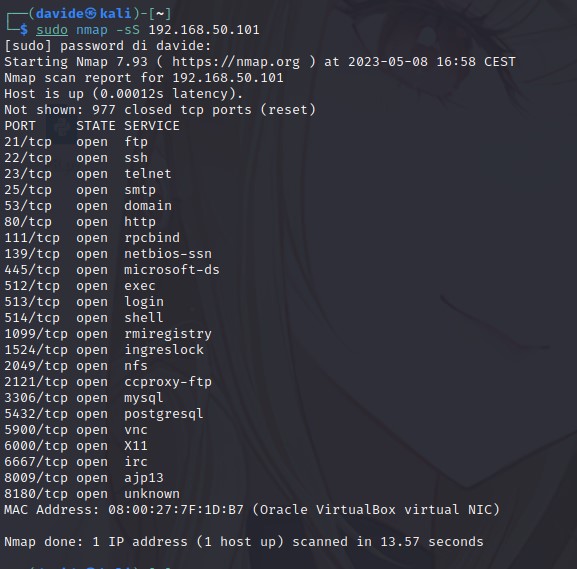
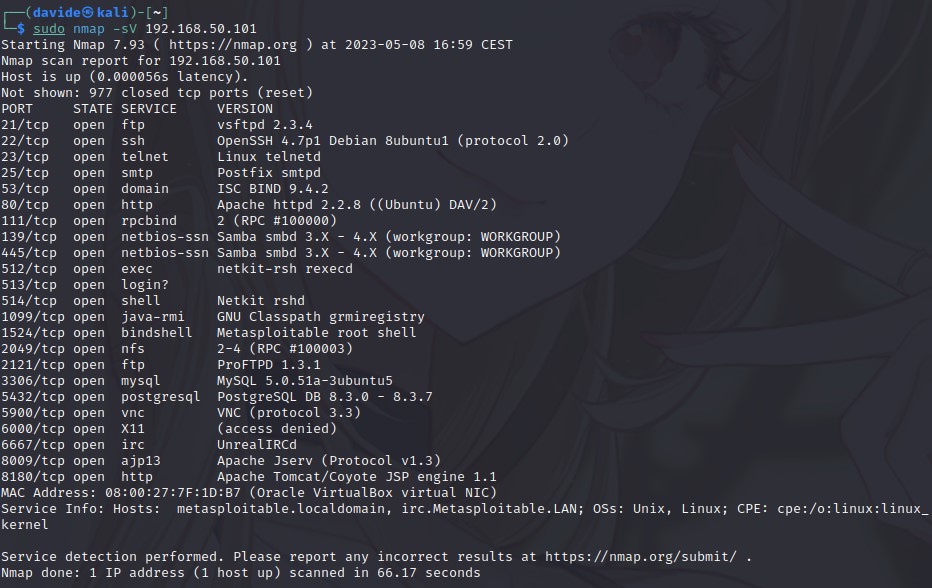
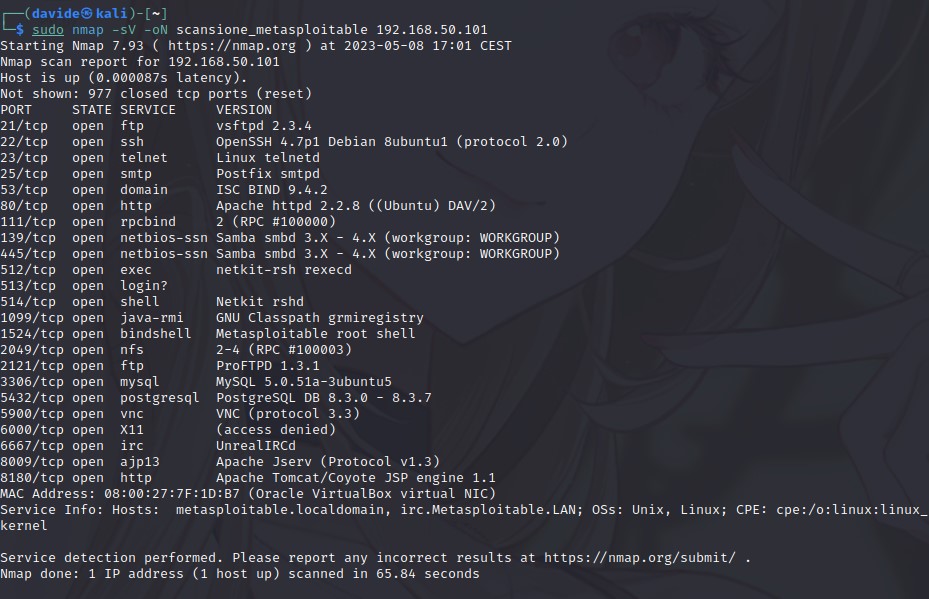
**-sS** (SYN scan stealth – opzione di base di nmap)



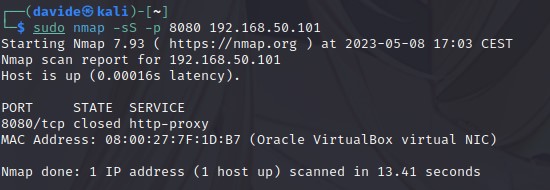
-**sV** (Abilita il version detection. In alternativa, è possibile utilizzare l'opzione -A che attiva il version detection, tra le altre cose.)



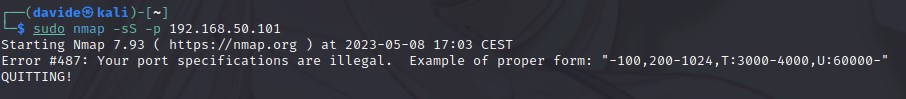
**-sV -oN** (System version + creazione di file txt)



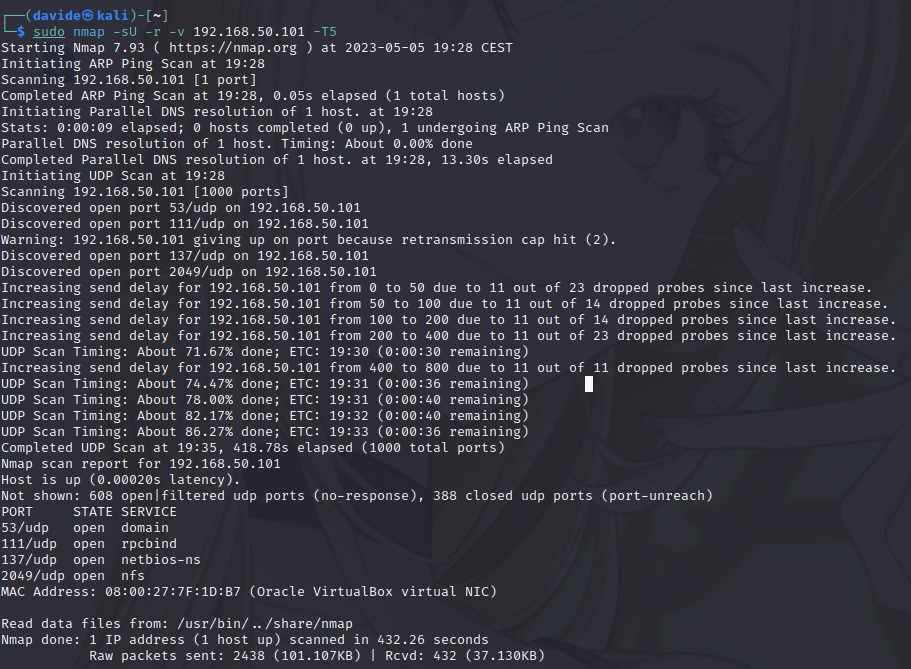
-**sS** porta 8080 (SYN stealth scan su porta singola 8080)



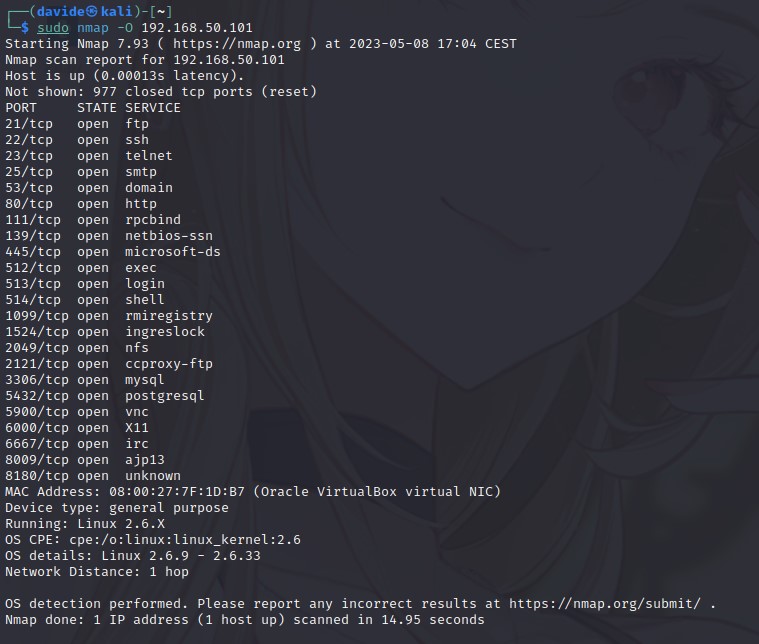
**-p** senza range di porte



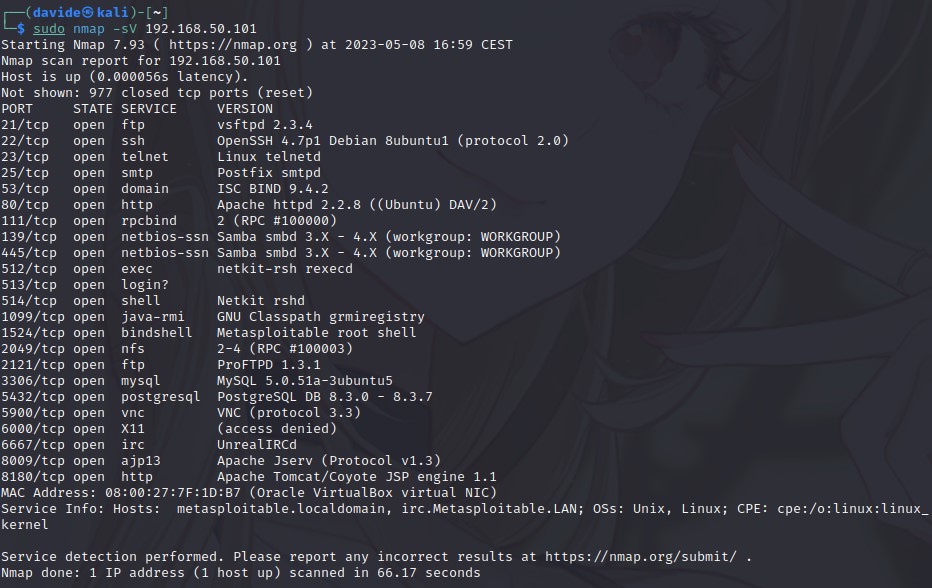
**-sU -r -v** (scan UDP in ordine numerico -r e aumento della verbosità della scansione con -v)



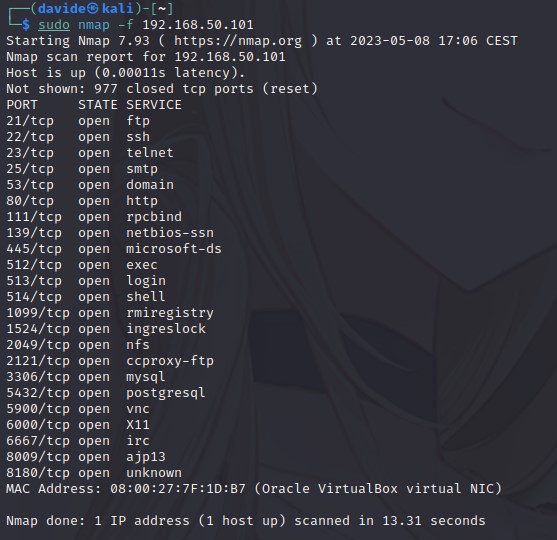
**-O** (Abilita la OS detection). In alternativa, è possibile utilizzare l'opzione -A per attivare sia l'OS detection, tra le altre cose.



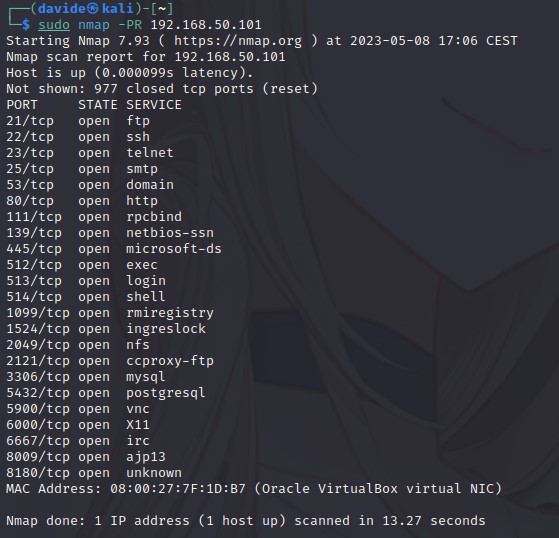
**-sV** (version detection – alias: *-sR*)



**-f** (fast scan)



**-PR** (ARP/Neighbor Discovery)



**-sP** (opzione -sn, ovvero senza port scan).

Port scan dopo un host discovery e di mostrare gli host che hanno risposto. Quest'opzione è spesso conosciuta come «ping scan», ma si può anche richiedere il traceroute ed eseguire script host NSE. Quest'azione è un gradino più invadente della List Scan, e spesso può essere usata per lo stesso scopo. Essa permette una mappatura di una rete obiettivo senza attrarre molta attenzione. Sapere quanti host sono attivi è più utile ad un attaccante rispetto ad una semplice List Scan di ogni indirizzo IP e nome di host.

