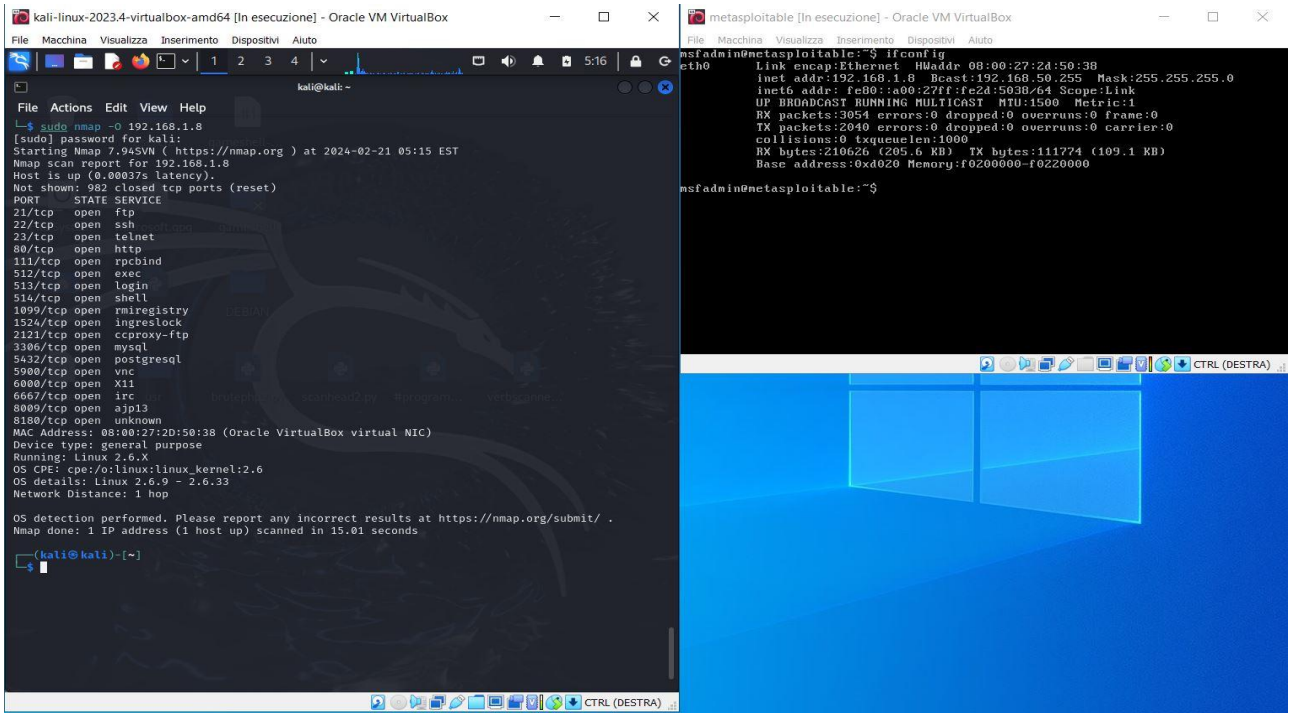
IP Kali: 192.168.1.1

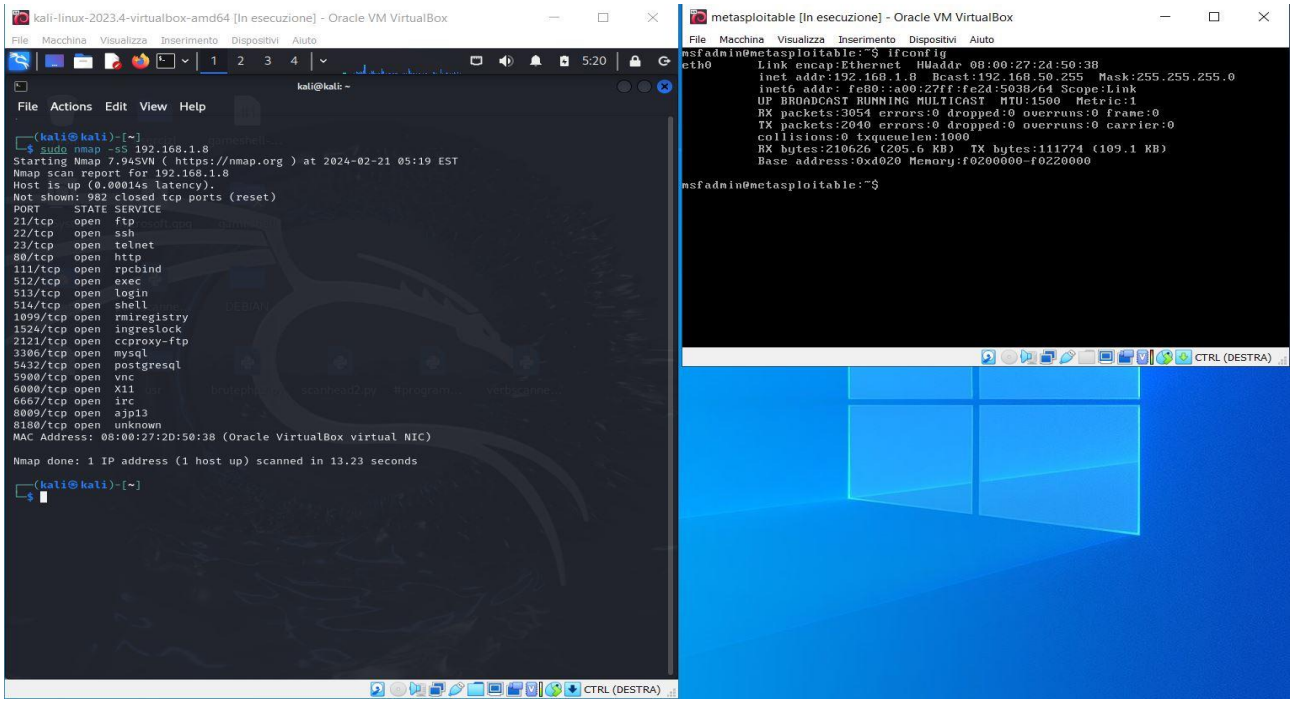
IP Metasploitable: 192.168.1.8

IP Windows 7: 192.168.1.20

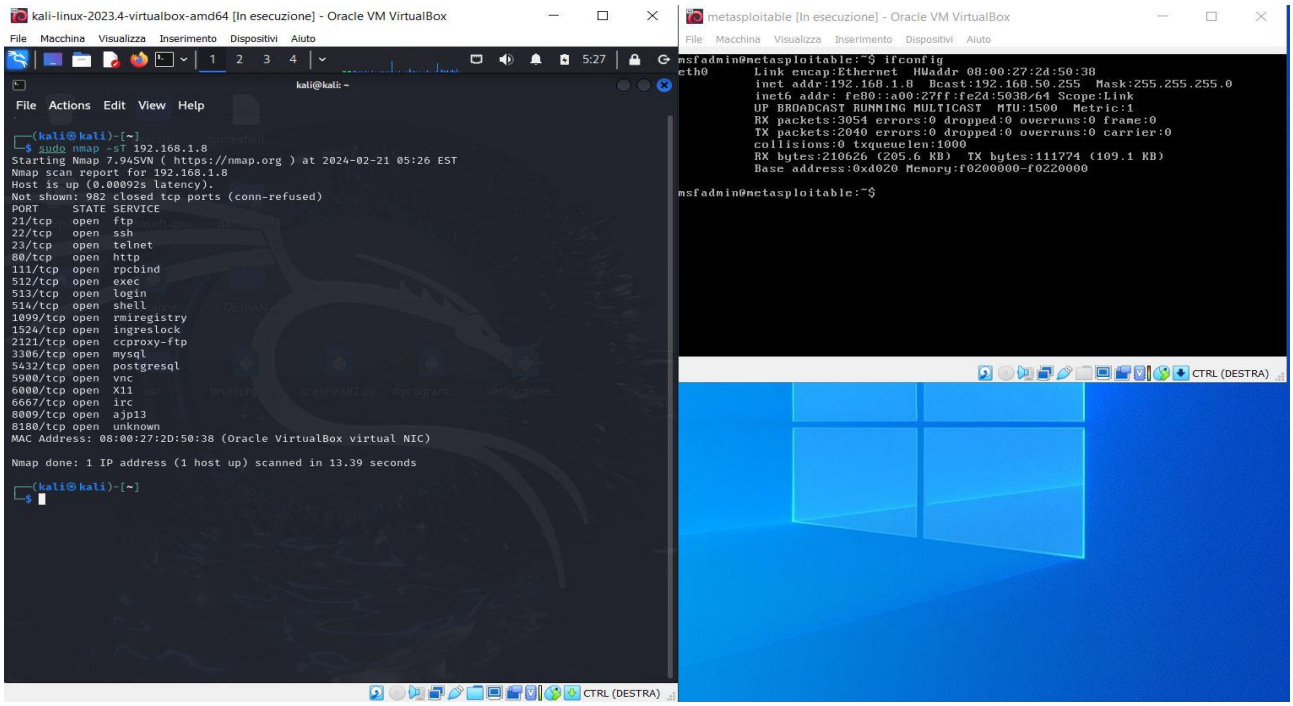
Scansione OS Fingerprint su Metasploitable:



Syn Scan su Metasploitable:

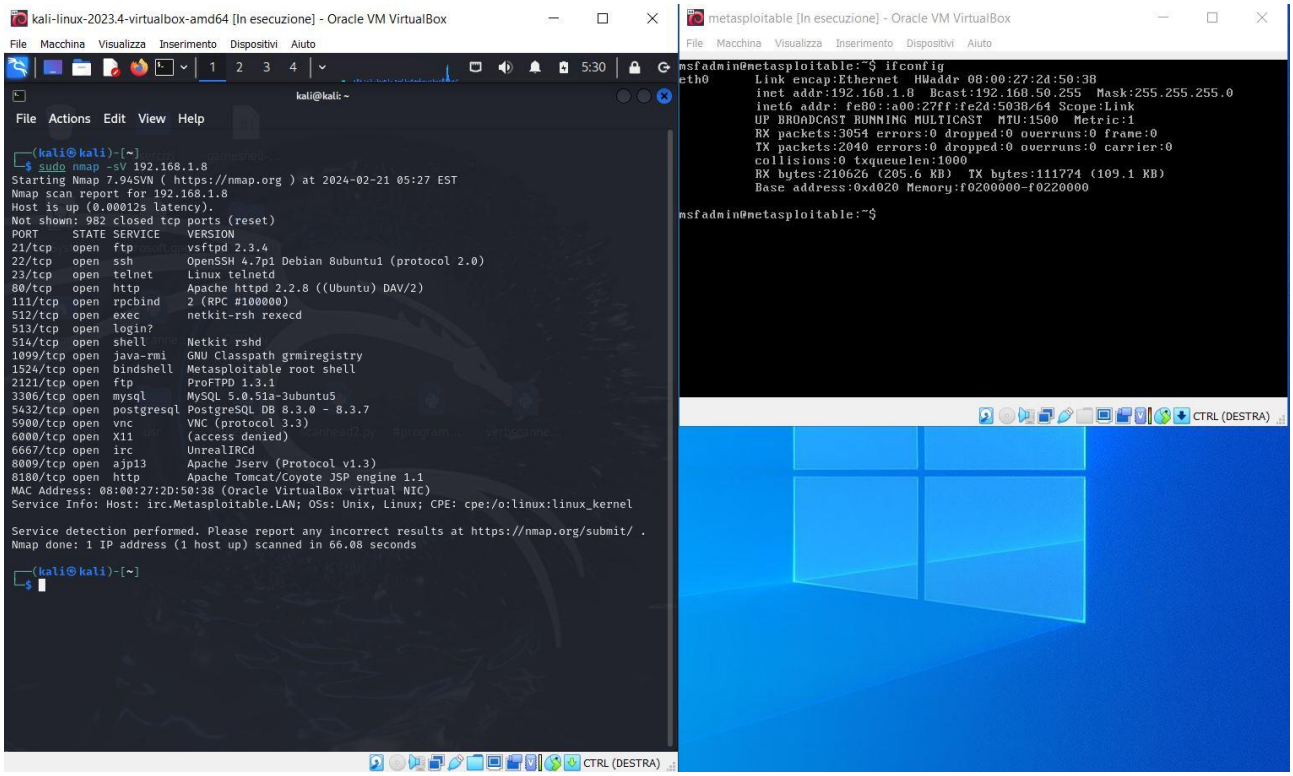


Scansione TCP connect su Metasploitable:

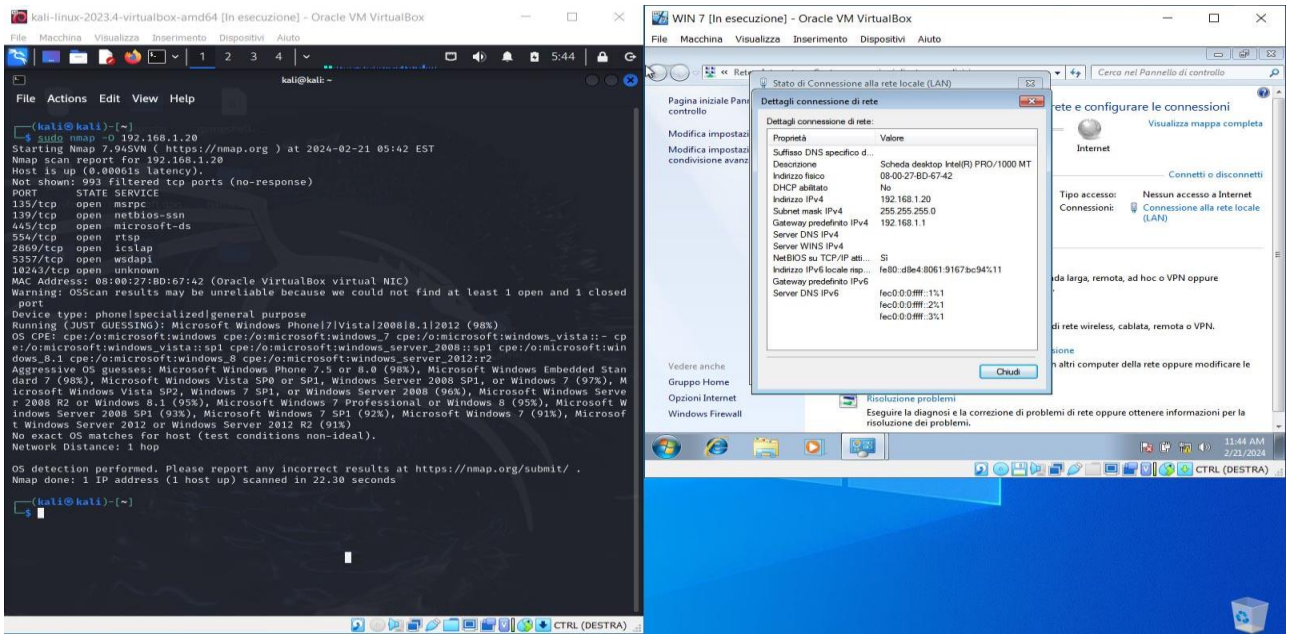


Come si può notare si denota un tempo di esecuzione leggermente maggiore, e un tipo di risposta sulle porte tcp diversa (“conn-refused” contro il “reset” del SYN scan).

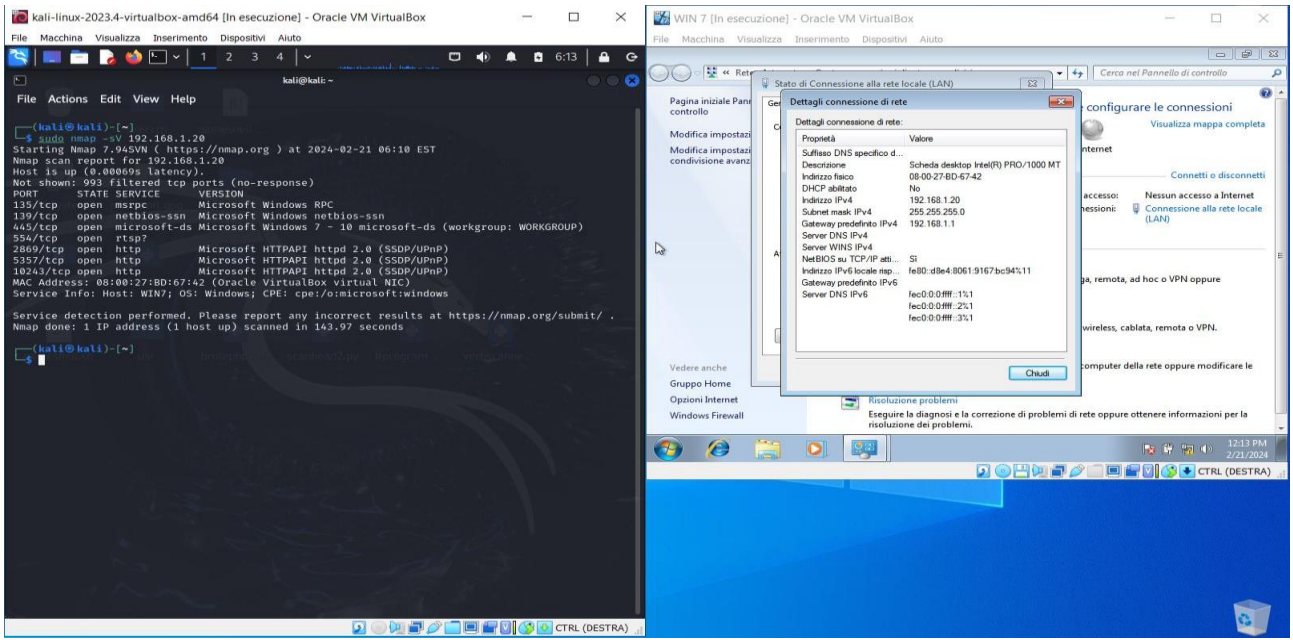
Scan Version detection su Metasploitable:



Scansione OS Fingerprint su Windows 7:



Come si può vedere nmap cerca di indovinare la versione di Windows arrivandoci molto vicino (97%), invece approfondendo lo scan con il Version detection otteniamo questi risultati:



Così otteniamo evidenza che l'OS in questione è proprio Windows 7.

Forzando uno scan ancora più aggressivo con l'ausilio di T5 (insane scan) otteniamo gli stessi risultati già estrapolati poc'anzi: