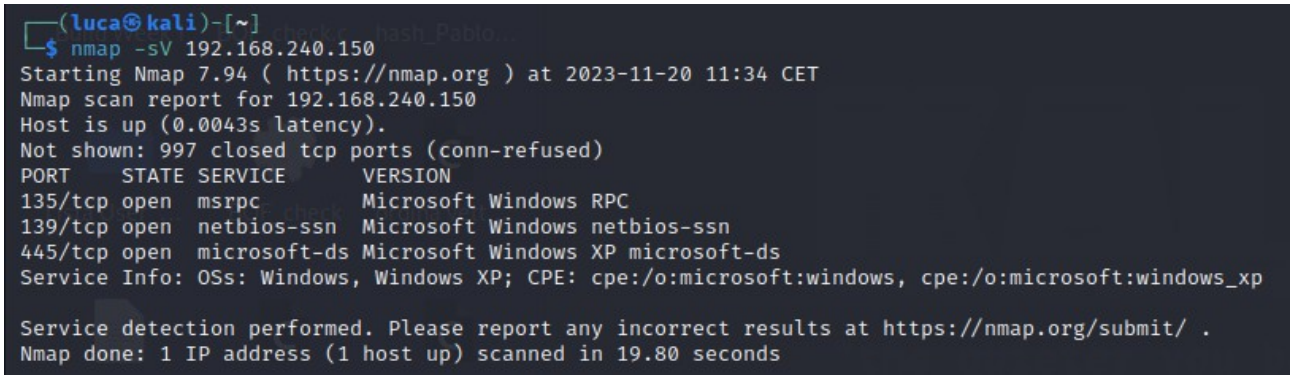
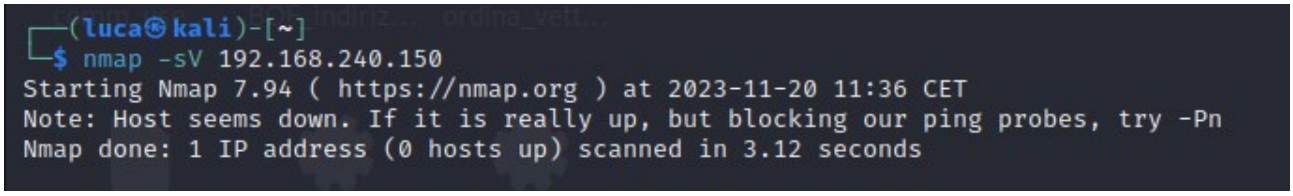
PRATICA S9L1

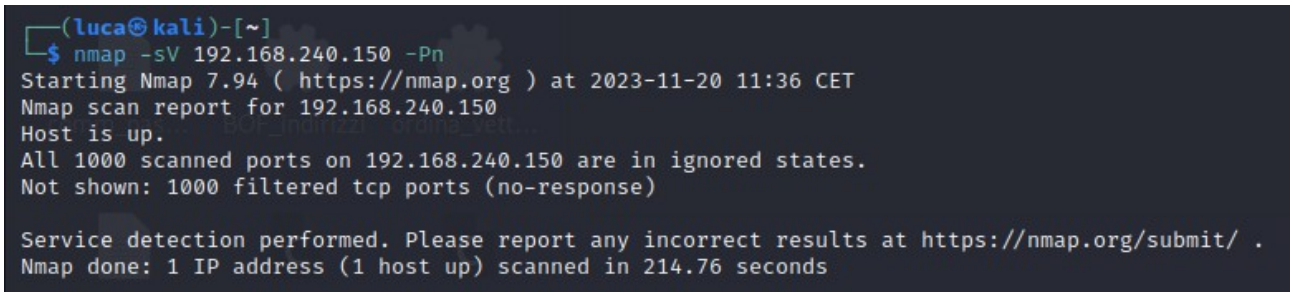
Dopo aver configurato gli indirizzi ip sulle macchine kali e windows xp, proviamo una scansione con lo switch -sV per verificare i servizi attivi e la relativa versione in ascolto sulla macchina target windows xp:



Troviamo diverse porte in ascolto, che potrebbero essere usate da una eventuale attaccante come possibili obiettivi di un exploit sulla macchina. Vediamo come cambia la situazione andando ad attivare il firewall su Windows XP. Facciamo due scansioni:



Notiamo che questa scansione ci informa che il target risulta (erronamente) essere down o irraggiungibile. Questo perché di default nmap usa il protocollo ICMP per verificare la raggiungibilità, ma questo protocollo viene rifiutato di default dal firewall di windows. Non ricevendo risposta quindi nmap trae la suddetta conclusione. Proviamo quindi ad inserire l'opzione -Pn, che tratta il target come se avesse ricevuto risposta positiva al ping e passa direttamente alla fase successiva di scansione vera e propria:



La risposta è leggermente diversa. Nmap conclude che il target è UP, ma anche in questo caso non riesce a concludere se vi siano porte in ascolto. Da una risposta di questo tipo possiamo quindi concludere che l'obiettivo della nostra scansione sia protetto da un firewall, che non consente quindi connessioni in ingresso (a meno che non abbia una policy specifica).