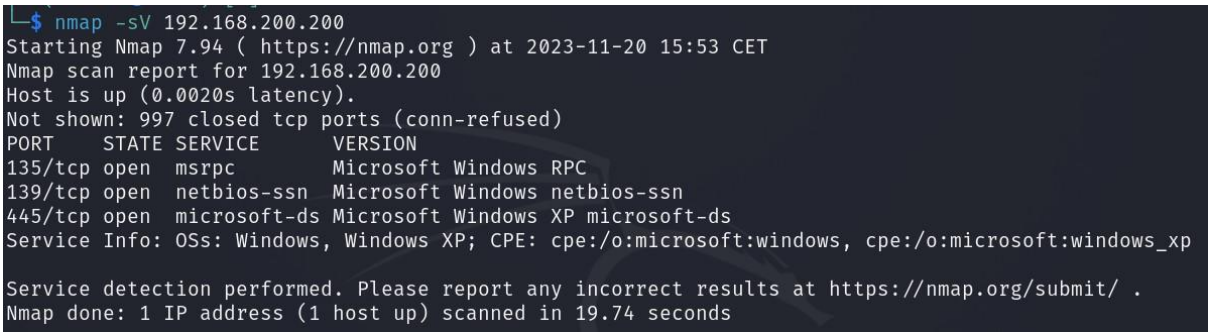
Progetto S9-L1

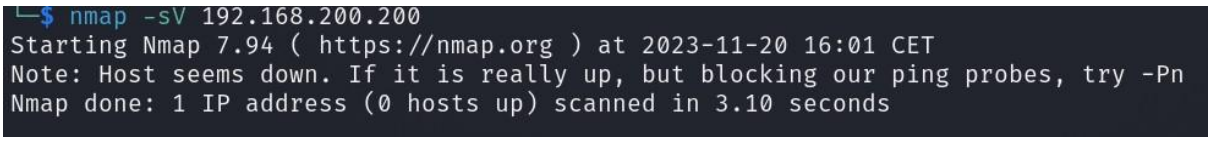
Studente: Simone Mininni

Task: Osservare il differente comportamento della scansione con nmap di windowsXP con il firewall on/off.

Nella situazione iniziale dove il firewall di windowsXP è disattivato notiamo che la scansione con nmap va facilmente a buon fine restituendoci il s.o. del target e i servizi attivi su determinate porte come il protocollo netbios e samba.



Con il firewall attivato, l ‘ output di nmap è poco esplicito.



Notiamo che il target su cui effettuiamo la scansione blocca il ping in entrata, infatti il firewall di windows blocca le icmp requests in entrata.

Inserendo lo switch -Pn(nmap durante la scansione non invia un pacchetto icmp), notiamo che l host è attivo ma le porte sono filtrate, quindi non riusciamo a stabilire quali porte sono effettivamente chiuse e quali aperte, questo dovuto proprio alla presenza del firewall.
Si potrebbe tentare di evadere il firewall utilizzando delle tecniche specifiche con nmap.