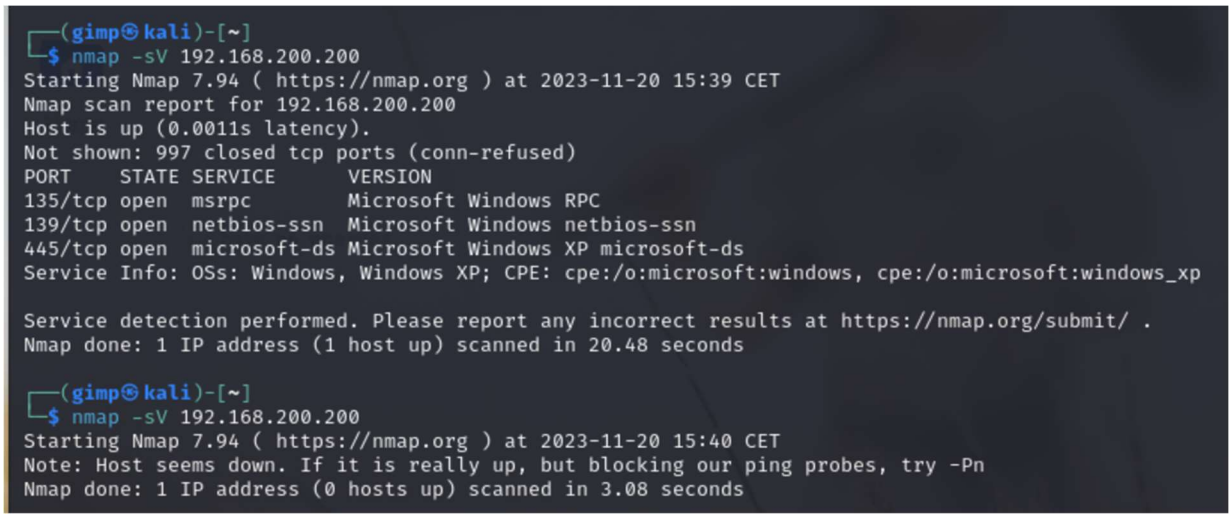
Esercizio S9-L1

L'esercizio prevedeva di fare un test sulle differenze percepite da due scan nmap verso macchina windows xp, la prima con firewall disattivato, la seconda con firewall attivo.



La prima scansione con firewall disattivato non ha creato problemi, vengono restituite tre porte aperte.

Nella scansione con firewall disattivato invece l'host non viene proprio raggiunto. Questo è ricollegabile alla funzione del firewall dinamico. Provando infatti a fare un altro test, usando il ping, esso che prima non aveva problemi a raggiungere il dispositivo ora non lo rilevava neanche. Queste perche il firewall dinamico blocca ogni connessione esterna e autorizza connessioni esterne sono se prima la richiesta è stata fatta dall'interno. Infatti, provando a pingare il dispositivo kali da windows xp non si hanno problemi di connessione.

Ho provato a fare un ulteriore test, usando la stessa scansione nmap ma togliendo il ping, quindi utilizzando solo la 3way handshake del protocollo tcp. In questo caso viene rilevato che l'host è attivo ma le porte non vengono mostrate, rimangono nello stato di porte filtrate.