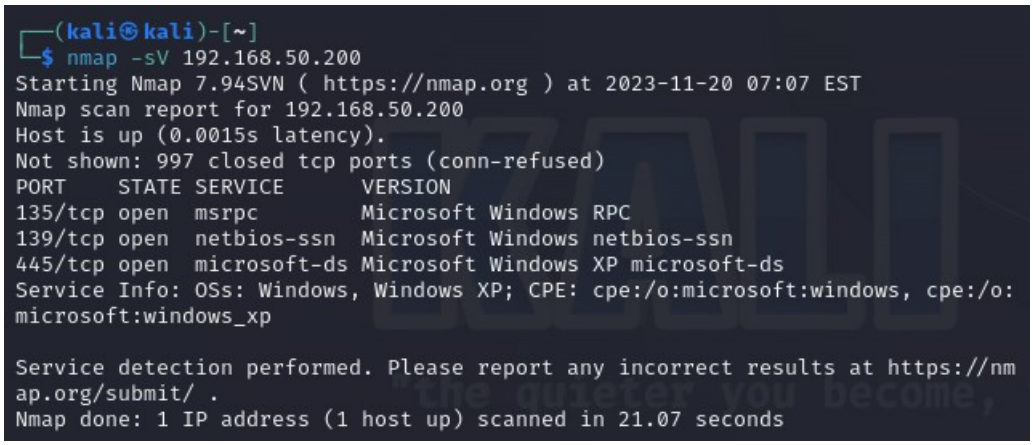
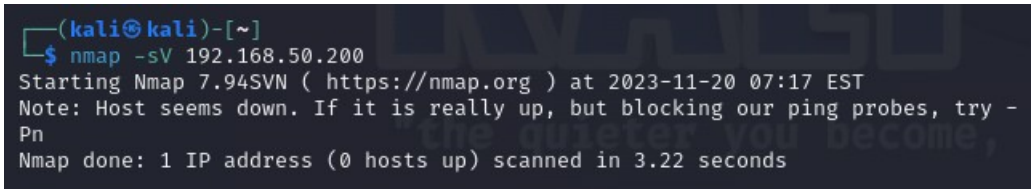
Esercizio S9 L1

Nell'esercizio di oggi compariamo due scansioni di Nmap su un sistema target prima e dopo aver abilitato il firewall su quel sistema.

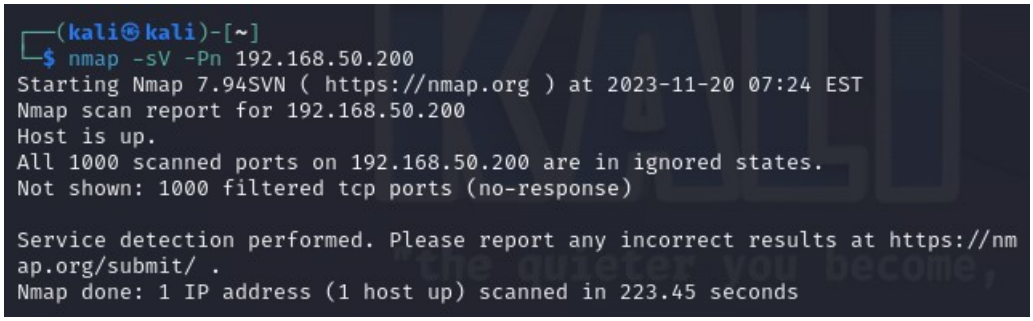
Abbiamo usato una scansione *version detection*, con cui andiamo ad implementare il *banner grabbing*, ovvero Nmap scansiona il sistema target in cerca della versione dei servizi attivi sul sistema.
Con questo tipo di scansione, che usa sia il ping che la stretta di mano a tre vie, abbiamo potuto recuperare tutte le informazioni che ci aspettavamo: porte aperte, servizi attivi su queste porte e la loro versione. Abbiamo anche informazioni sul sistema operativo presente sulla macchina vittima.



Dopo aver attivato il firewall su Windows XP andiamo a ripetere la stessa scansione, ma questa volta non otteniamo alcuna informazione. Nmap riporta solo che il sistema target potrebbe non essere attivo e suggerisce di usare una nuova scansione senza ping, nel caso siamo sicuri che il sistema sia invece attivo.



Riproviamo la scansione, questa volta senza usare il ping, e vediamo che ora Nmap riconosce il sistema come attivo, ma tutte le porte scansionate sono filtrate (succede quando è attivo un firewall).



Facendo una contro prova, abbiamo provato a lanciare un semplice ping verso Windows XP, ma nessun pacchetto ha potuto raggiungere l'host target.