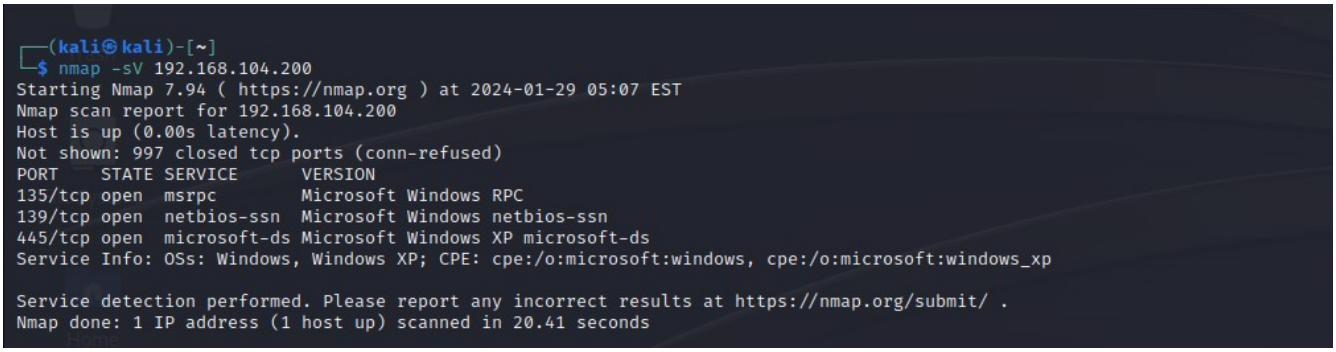
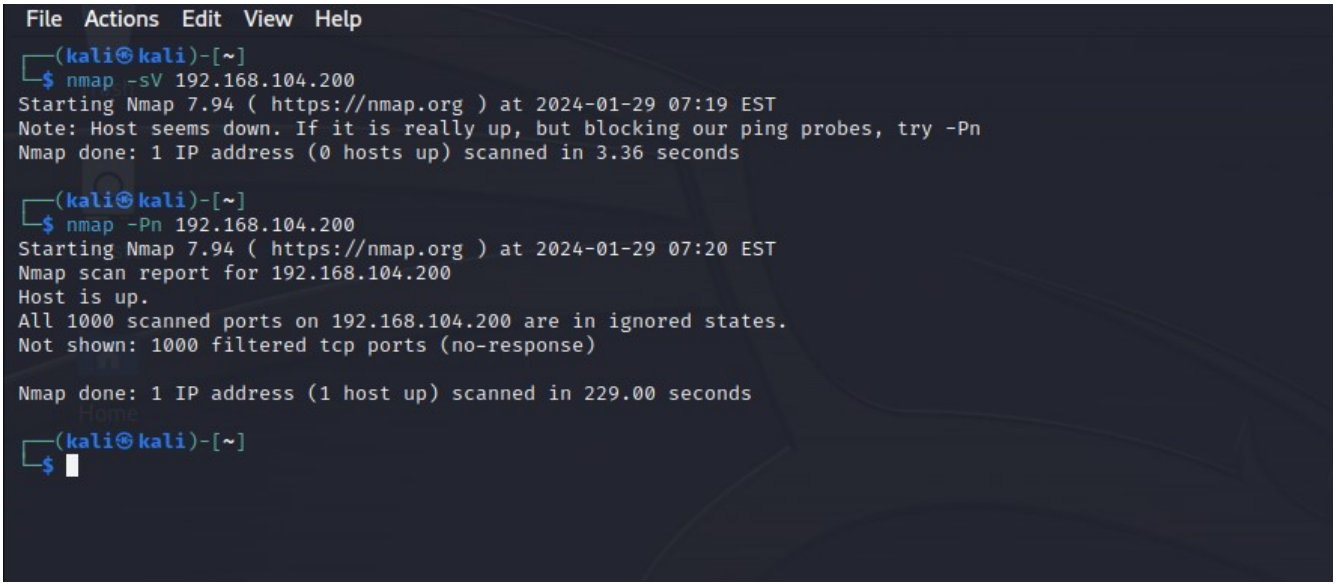
S9 LEZIONE 1

Traccia:
Durante la lezione teorica, abbiamo studiato le azioni preventive per ridurre la possibilità di attacchi provenienti dall'esterno. Abbiamo visto che a livello di rete, possiamo attivare / configurare Firewall e regole per fare in modo che un determinato traffico, potenzialmente dannoso, venga bloccato.
La macchina Windows XP in formato OVA che abbiamo utilizzato nella Unit 2 ha di default il Firewall disabilitato.
L'esercizio di oggi è verificare in che modo l'attivazione del Firewall impatta il risultato di una scansione dei servizi dall'esterno. Per questo motivo:
1. Assicuratevi che il Firewall sia disattivato sulla macchina Windows XP
2. Effettuate una scansione con nmap sulla macchina target (utilizzate lo switch –sV, per la service detection)
3. Abilitare il Firewall sulla macchina Windows XP
4. Effettuate una seconda scansione con nmap, utilizzando ancora una volta lo switch –sV.Traccia:
Che differenze notate? E quale può essere la causa del risultato diverso?



La scansione è stata eseguita con le opzioni -sV:

-s indica a Nmap di eseguire una scansione TCP SYN stealth, ovvero una scansione in cui il client invia un pacchetto SYN ad una porta. Se il target riponde con un pacchetto SYN/ACK, allora quella porta è aperta. Se il server non risponde allora quella porta è chiusa.
L'opzione -V, indica a Nmap di includere informazioni sulla versione del servizio.
Come si può notare l'host è attivo ed ha 3 porte aperte.



Attivando il firewall su windows XP ed eseguendo di nuovo la scansione l'host sembra essere down, nmap non riesce a stabilire una connessione il che potrebbe indicare che che l'host sia offline.
Con il comando -Pn si riesce che l'host è effettivamente attivo, 1000 porte sono state scansionate ma non è stata ricevuta nessuna risposta da esse.

In base a queste info, posso concludere che il firewall ha fatto il suo lavoro, bloccando ogni tipo di connessione