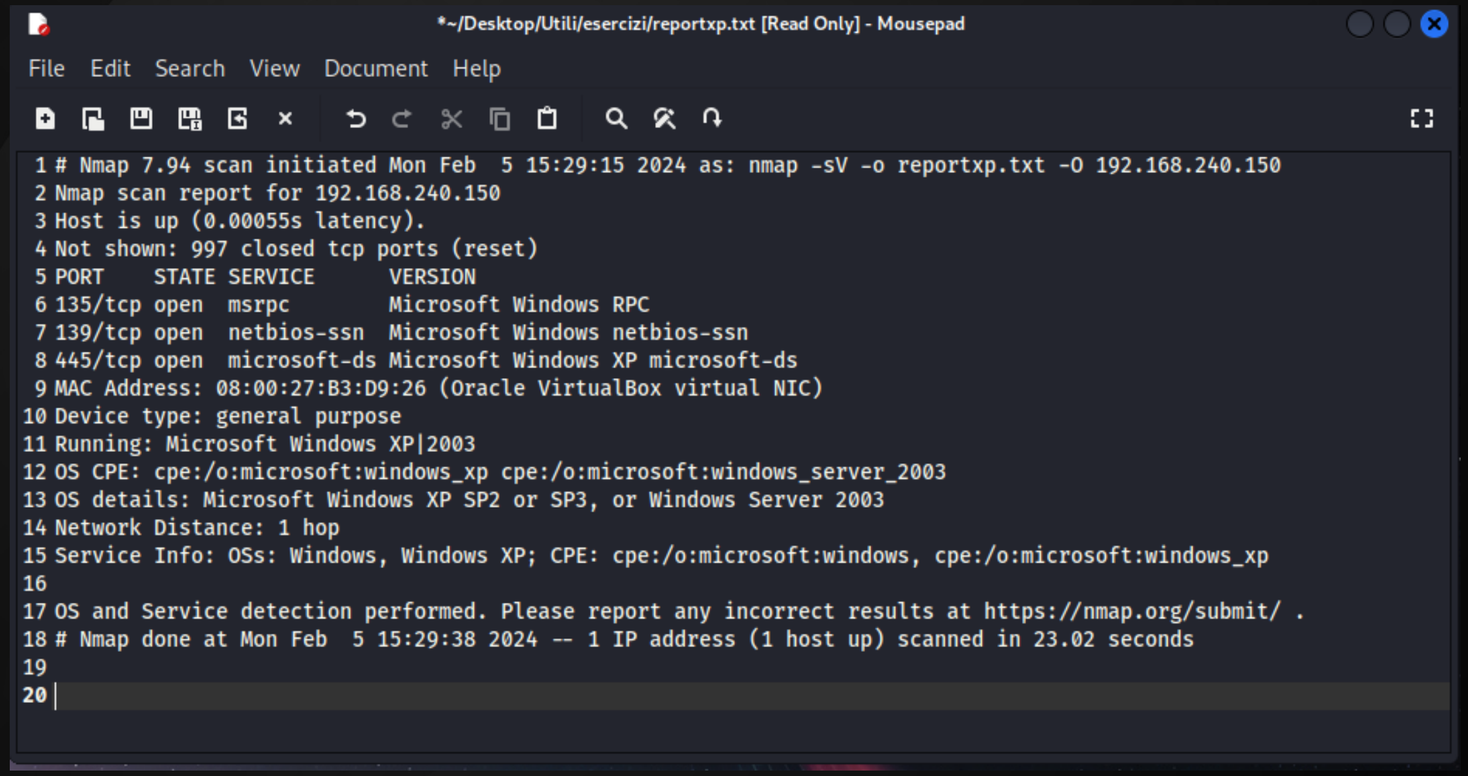
S9-L1

Overview

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 che abbiamo utilizzato 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.

Dopo aver modificato i file di configurazione di rete e avviato la scansione di nmap, come indicato nella traccia, possiamo notare che risultano presenti alcuni servizi attivi (sulle porte: 135, 139, 445).
Proviamo ora a effettuare una nuova scansione con nmap ma abilitando il firewall.



Come possiamo notare una volta attivato il firewall non saremo più in grado di rintracciare i servizi precedentemente ottenuti, infatti tutte le porte risulteranno chiuse. I firewall possono prevenire le scansioni di software come nmap in diversi modi, tra cui:

- Alcuni firewall sono in grado di rilevare pattern di traffico sospetti o comportamenti anomali associati a Nmap e possono bloccare le sue attività di scansione.
- Il firewall può limitare il numero di richieste o di pacchetti inviati da un singolo indirizzo IP in un determinato periodo di tempo.
- Alcuni firewall possono ispezionare i pacchetti di dati in transito e rilevare firme o modelli di traffico associati a Nmap, bloccando quindi le sue attività.