Consegna S9/L1

di Giuseppe Lupoi

Indice

Traccia

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.*

Che differenze notate? E quale può essere la causa del risultato diverso?

Requisiti:

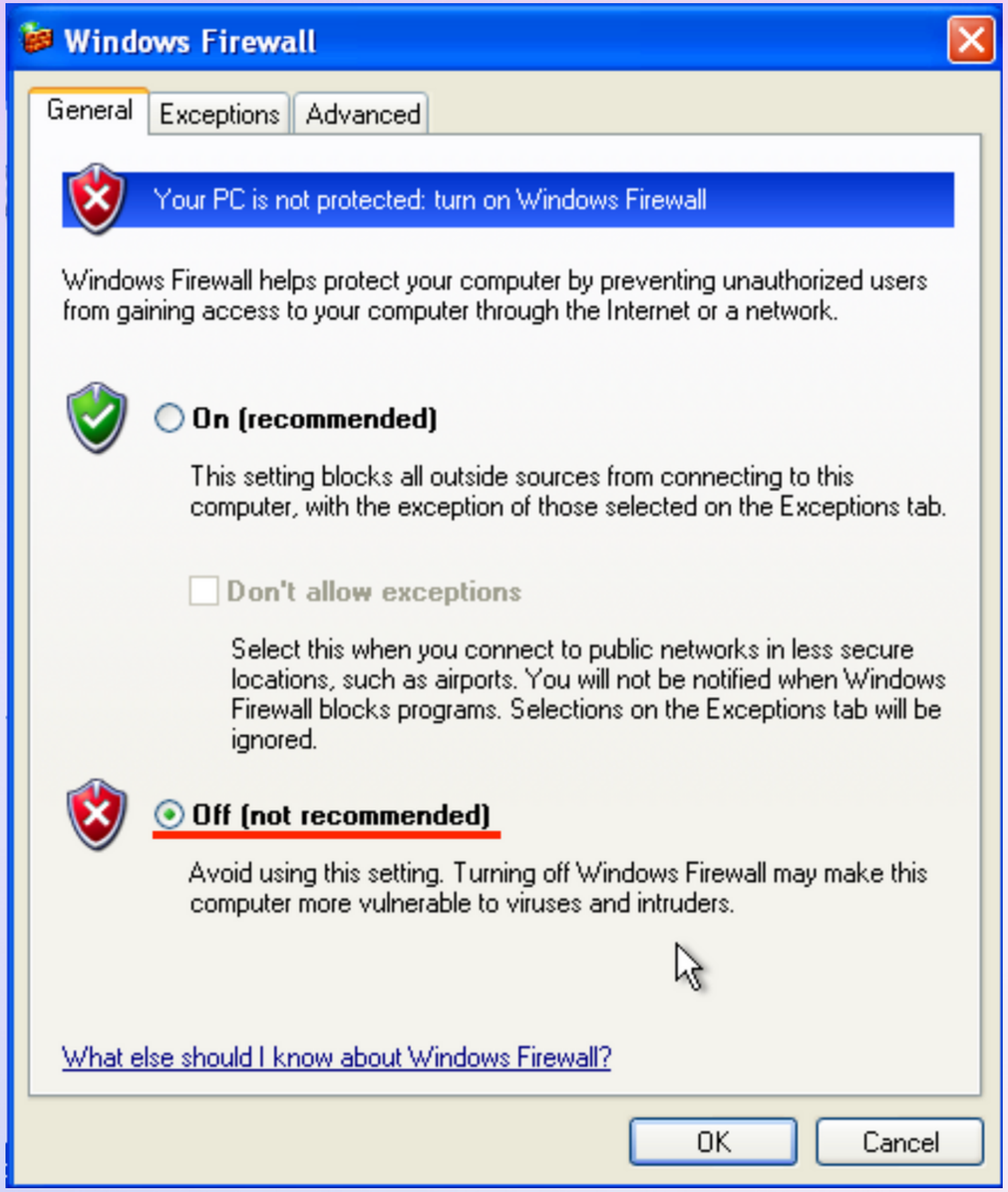
Configurate l’indirizzo di Windows XP come di seguito: ***192.168.240.150***

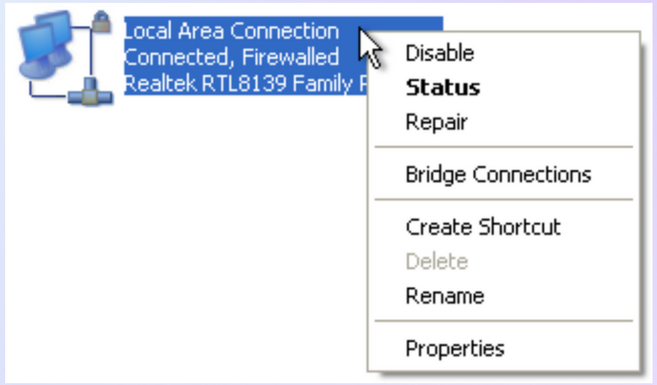
Configurate l’indirizzo della macchina Kali come di seguito: ***192.168.240.100***

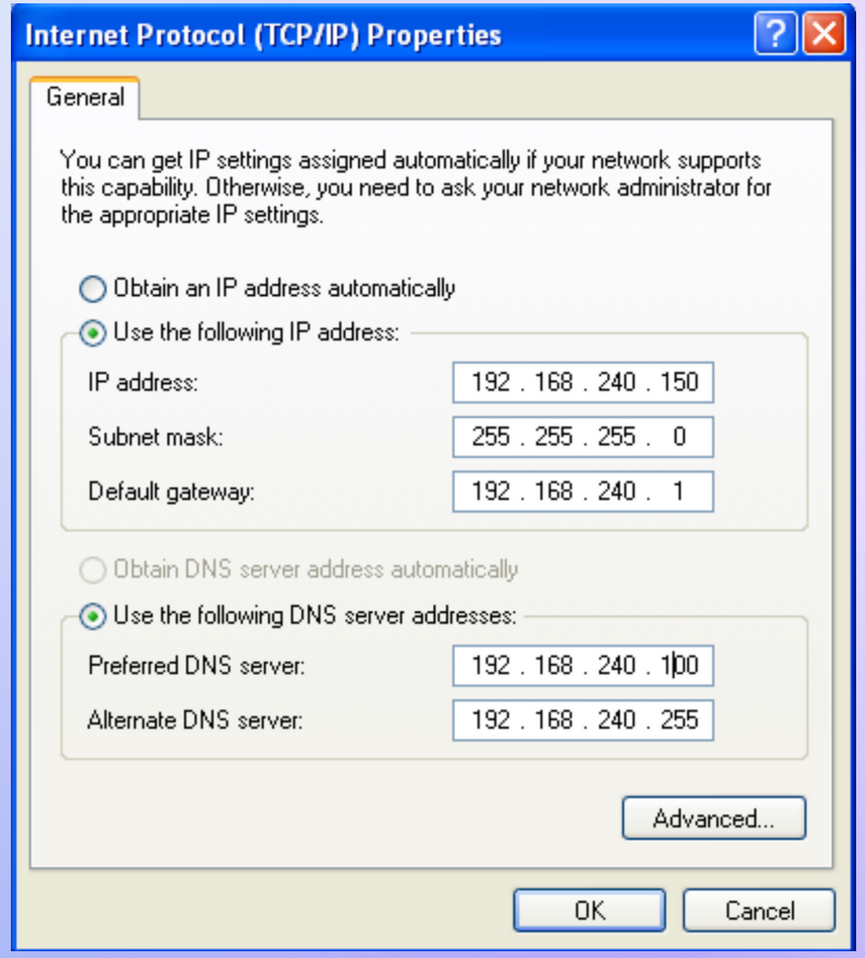
*Per iniziare l'esercizio di oggi, come prima cosa dopo aver avviato le macchine necessarie allo svolgimento ovvero **Windows XP** e **Kali Linux**, ci accerteremo che il **Firewall** di Windows XP sia disattivato per poter poi effettuare una prima scansione con **nmap**.*

*Una volta quindi nella schermata principale di Windows XP clicchiamo nel **triangolo rosso** in basso a destra per aprire il **Centro di Sicurezza**, in seguito clicchiamo su **Windows Firewall** come mostrato nella figura accanto.*

Noteremo il Firewall disattivato sull'impostazione ***Off (not recommended)****, se cosi non fosse, applichiamo la spunta sulla suddetta impostazione e salviamo il cambiamento cliccando su* ***OK*** *nella medesima finestra.*







Ora possiamo procedere con il cambio di indirizzo IP come richiesto dalla traccia.

Per fare ciò seguiremo questo percorso:

➡ *clicchiamo in basso a sinistra sul tasto dello* ***start***

➡ *apriamo il* ***Pannello di Controllo***

➡ *clicchiamo su* ***Network and Internet Connections***

➡ *in seguito su* ***Network Connections***

➡ *con il tasto destro su* ***Local Area Connection*** *andremo ad aprire le* ***Proprietà*** *in basso nella tendina come riportato in figura in alto a sinistra*

➡ *infine con un doppio click su* ***Internet Protocol (TCP/IP)*** *ci apparirà la schermata riportata qui a sinistra dove potremmo andare ad impostare l'indirizzo IP della macchina come richiesto*

*Per effettuare invece il cambio di IP sulla macchina Kali Linux, una volta eseguito l'accesso apriremo un terminale e con il comando "**sudo nano /etc/network/interfaces**" apriremo il file della scheda di rete come vedete nella figura sottostante.*
Procediamo impostando l'indirizzo come di seguito.

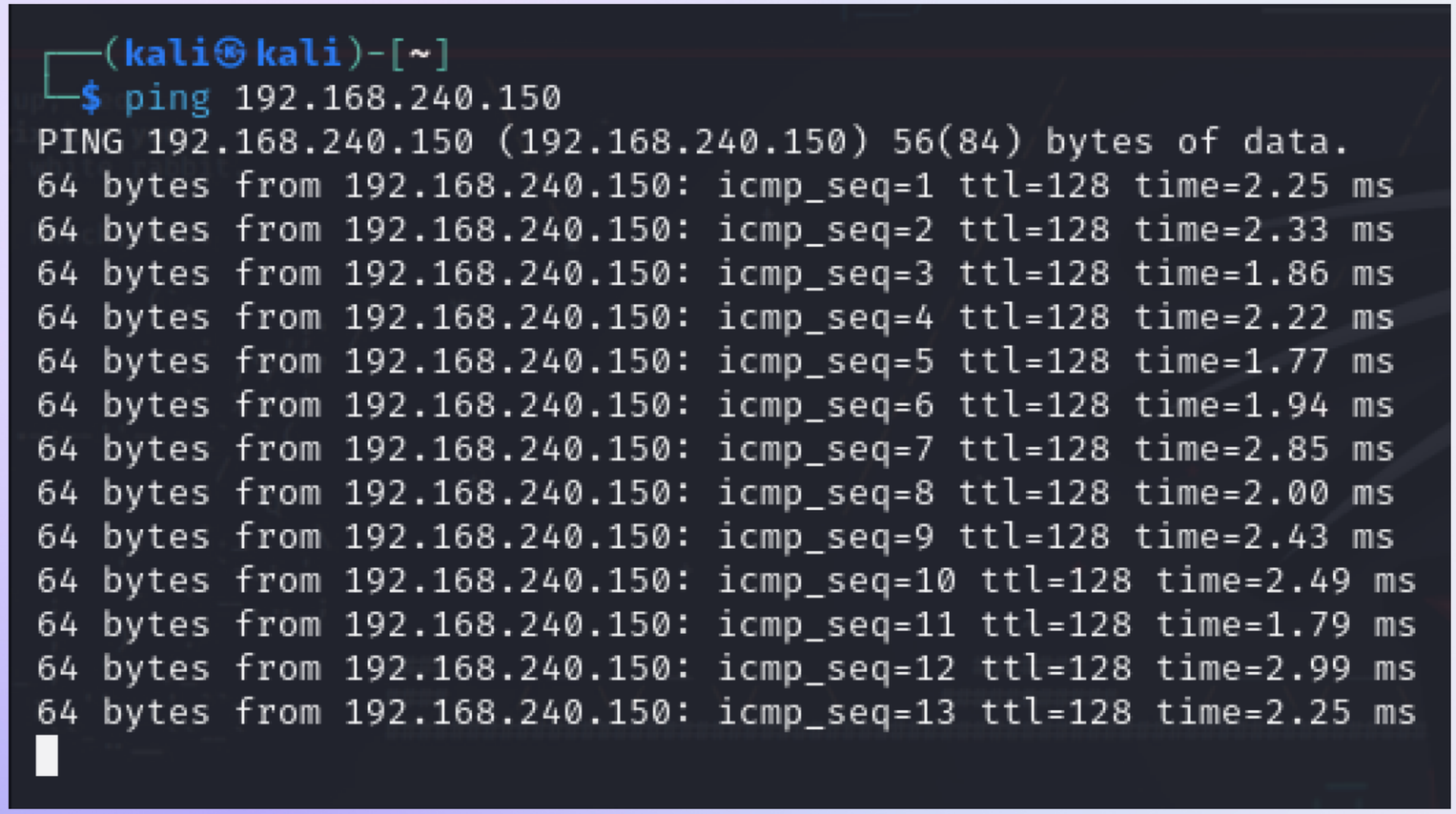
```
  GNU nano 7.2
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.240.100/24
gateway 192.168.240.1
```

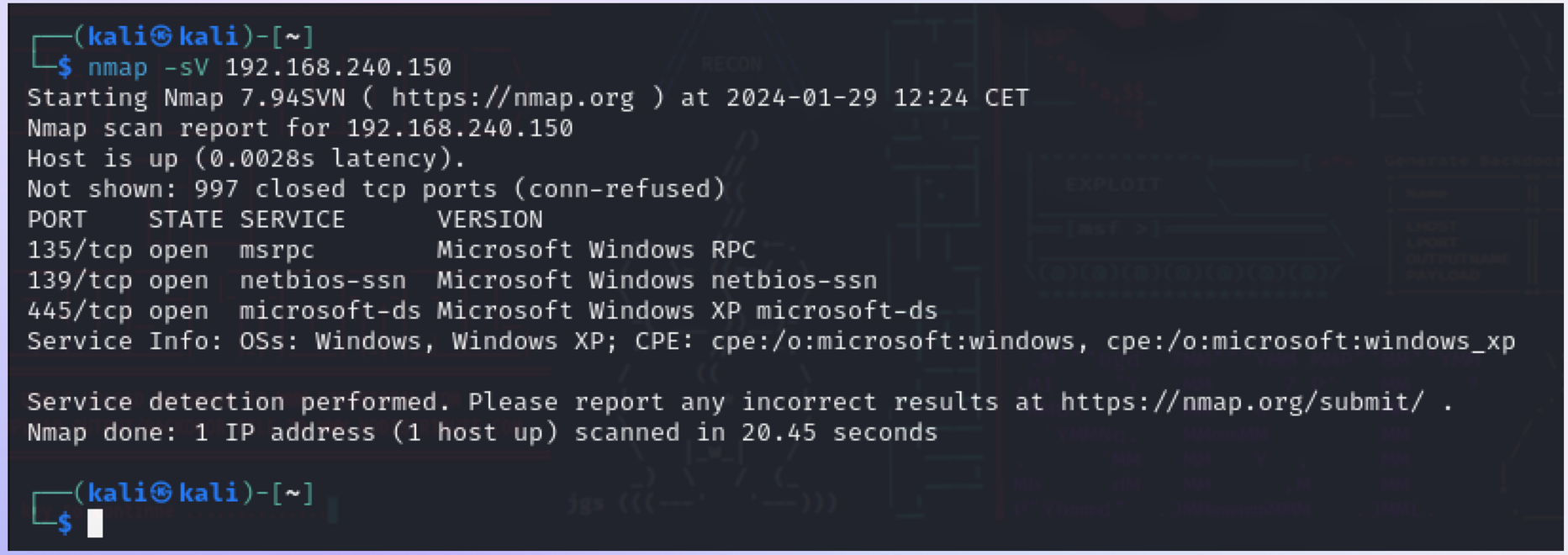
*A questo punto eseguiamo un riavvio di entrambe le macchine e per assicurarci che tutte le modifiche effettuate fino ad ora siano corrette eseguiamo il comando "**ping**" da Kali Linux verso la macchina Windows XP saremo cosi certi che le due macchine comunichino tra loro.*



*Siamo ora pronti per poter eseguire una prima scansione del **target Windows XP** con **nmap**. Digitiamo quindi il comando "**nmap -sV 192.168.240.150**".*

Nel dettaglio del comando notiamo:

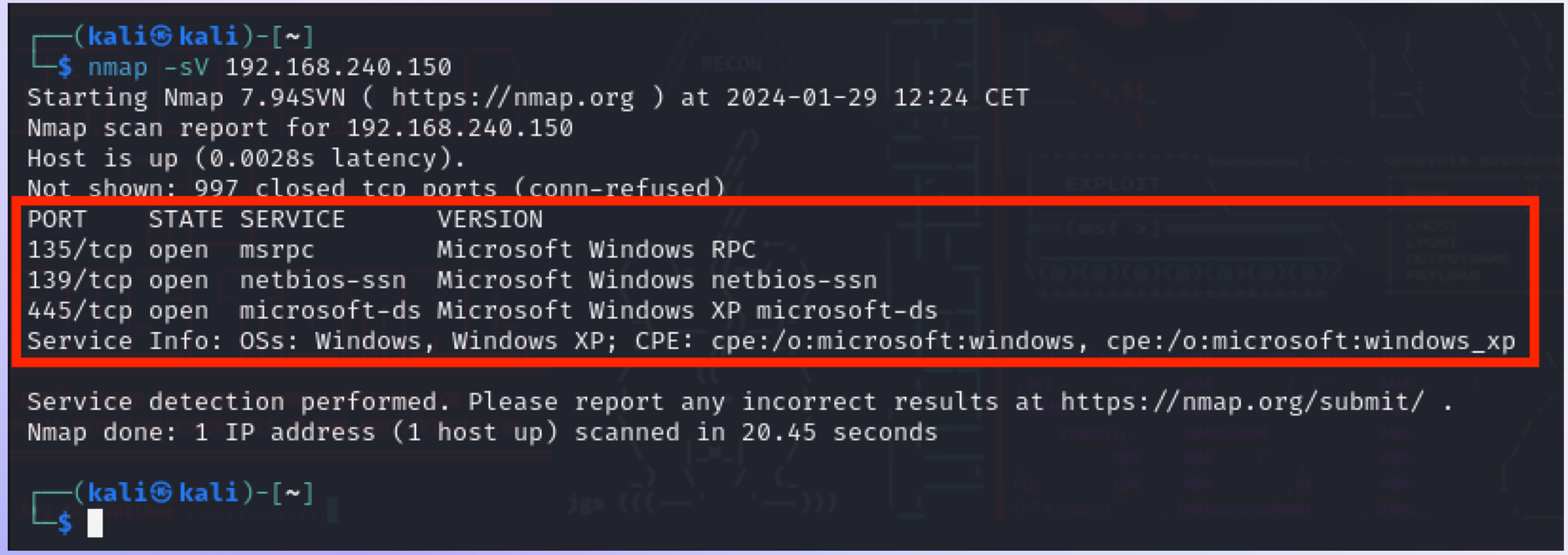
- "***nmap***", *sarà il servizio che utilizzeremo per effettuare la scansione*
- "***-sV***", *questa opzione attiva la rilevazione delle versioni dei servizi in esecuzione sulle porte aperte tenterà quindi di identificare la versione dei servizi*
- "***192.168.240.150***", *che sappiamo essere l'indirizzo IP della macchina target*



Da questa prima scansione possiamo infatti notare i seguenti servizi attivi compresi di porta, lo stato e la loro versione:

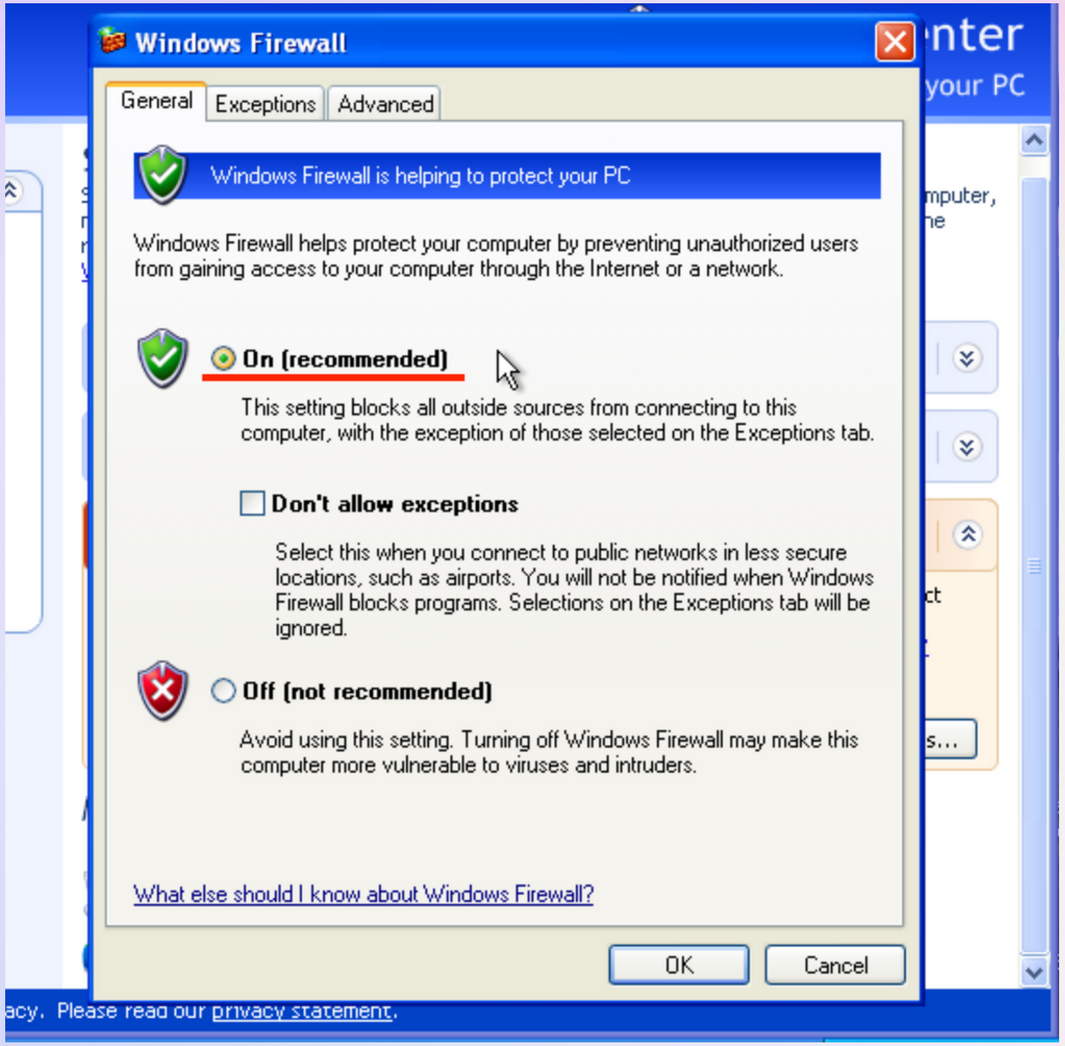
- ***SERVIZIO*** *msrpc* ***PORTA*** *135/tcp* ***STATO*** *open* ***VERSIONE*** *Microsoft Windows RPC*
- ***SERVIZIO*** *netbios-ssn* ***PORTA*** *139/tcp* ***STATO*** *open* ***VERSIONE*** *Microsoft Windows netbios-ssn*
- ***SERVIZIO*** *microsoft-ds* ***PORTA*** *445/tcp* ***STATO*** *open* ***VERSIONE*** *Microsoft Windows XP microsoft-ds*

Ed infine nell'ultima riga sottolineata dal rettangolo in rosso le informazioni relative al sistema operativo.



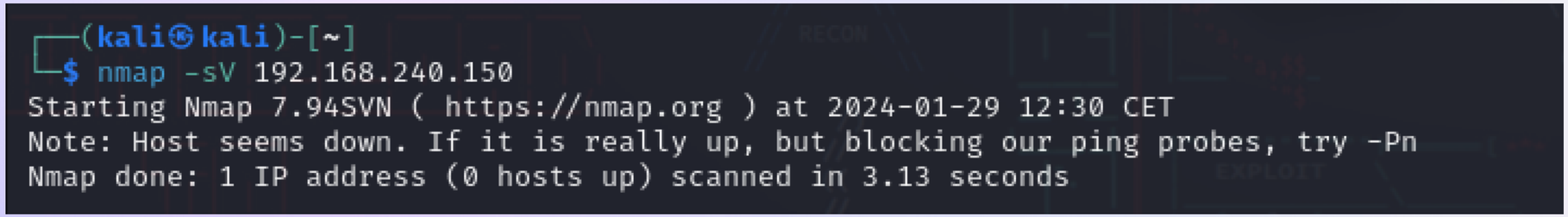
Una volta terminata la prima scansione con il Firewall attivo torneremo sulla macchina Windows XP questa volta per attivare il Firewall ed eseguire una seconda scansione.

Procediamo come visto in ***pagina 4 e 5*** *questa volta però andando a spuntare l'opzione* ***On (recommended)*** *per attivare appunto il Firewall, salviamo l'impostazione cliccando* ***OK*** *nella medesima finestra.*



*Avviamo quindi la seconda scansione con **nmap** dopo aver attivato il Firewall.*

Come possiamo notare dall'immagine riportata in calce, questa volta nmap non è riuscito a scansionare il sistema target, di conseguenza non è riuscito ad ottenere nessun tipo di informazione relativa al sistema.



Conclusioni

Come abbiamo quindi potuto notare dalle due scansioni effettuate nelle slide precedenti, si può notare la differenza tra la scansione effettuata con il firewall spento e con il firewall attivo. Dove nella prima, non essendoci appunto nessun tipo di blocco delle connessioni in entrata si riesce ad ottenere un'enumerazione dei servizi attivi sulla macchina.
Mentre, una volta attivato il firewall, quest'ultimo protegge il sistema e blocca le connessioni non autorizzate provenienti dall'esterno.
Notiamo infatti nella seconda scansione ***nmap*** *ci dirà che:*
*"****Il sistema sembra spento. Se invece è realmente acceso, sta probabilmente bloccando le comunicazioni****".*

Questa esercitazione di oggi ci fa capire l'importanza della corretta configurazione dei sistemi con cui andremo a lavorare, ovvero delle "azioni preventive" per evitare o per lo meno mitigare eventuali attacchi che porterebbero alla perdita di dati importanti, account o addirittura compromettere l'intero sistema.