SECURITY OPERATIONS

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 e -o nomefilereport per salvare in un file l'output)
3. Abilitare il Firewall sulla macchina Windows XP
4. Effettuate una seconda scansione con nmap, utilizzando ancora una volta lo switch –sV.
5. Trovare le eventuali differenze e motivarle.

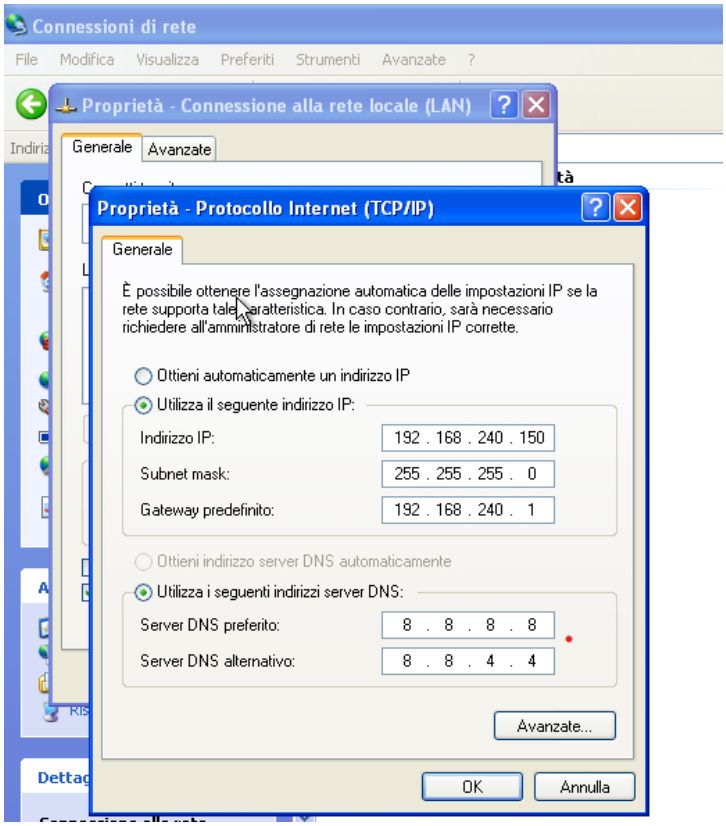
Che differenze notate? E quale può essere la causa del risultato diverso?

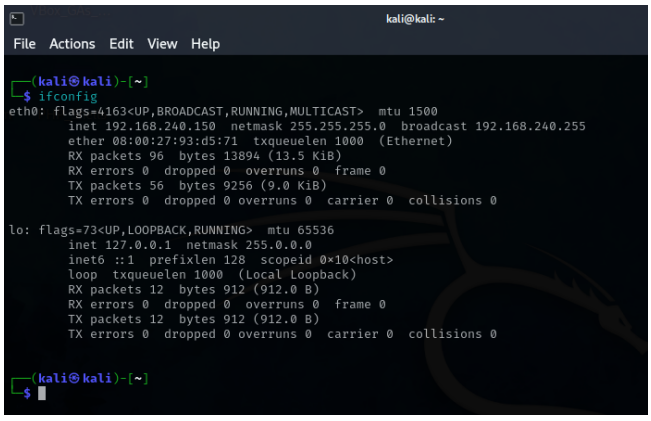
Requisiti:

- 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

Esecuzione:

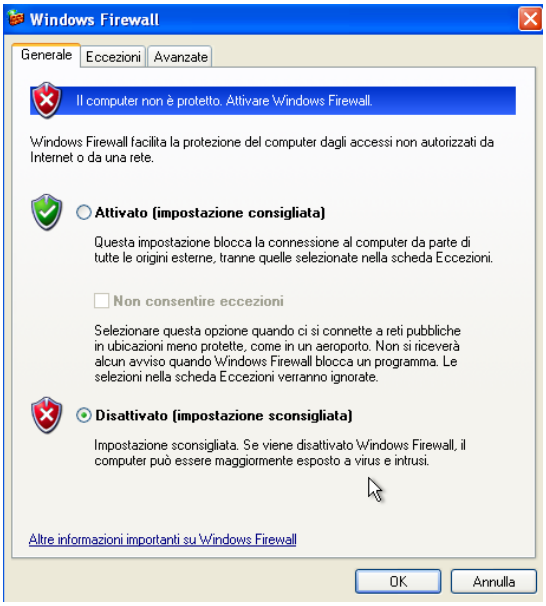
Effettuiamo i cambiamenti come richiesto dalla traccia.



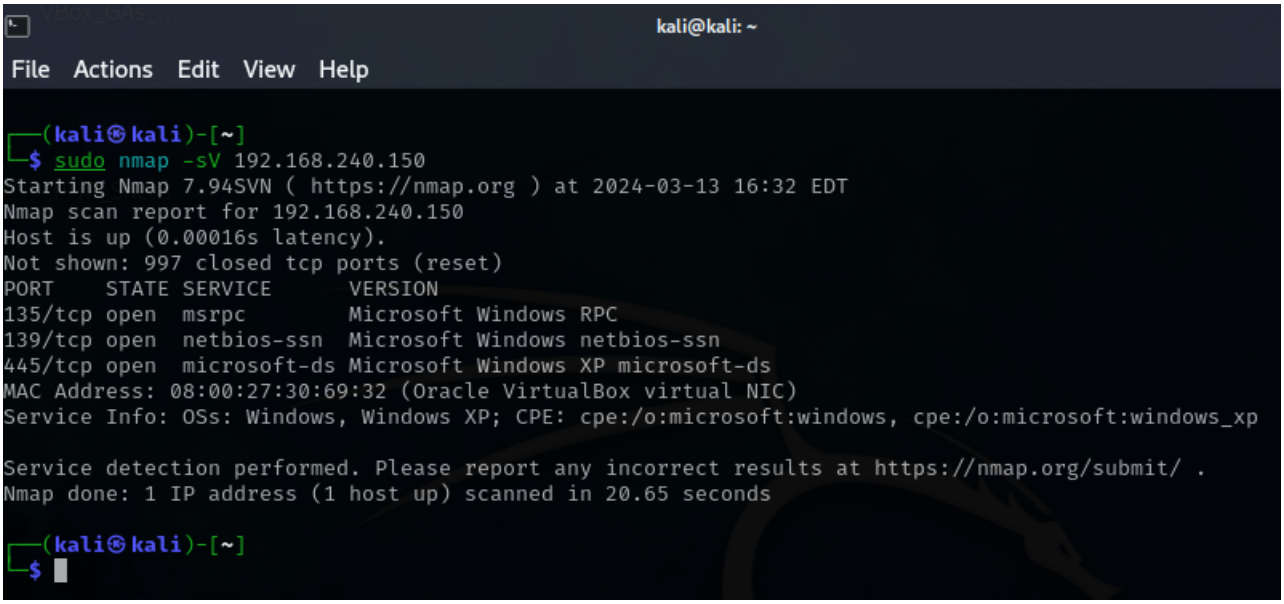


Primo Test: scansione con disattivazione del Firewall di Windows Xp

Disattiviamo il firewall come richiesto dalla traccia.

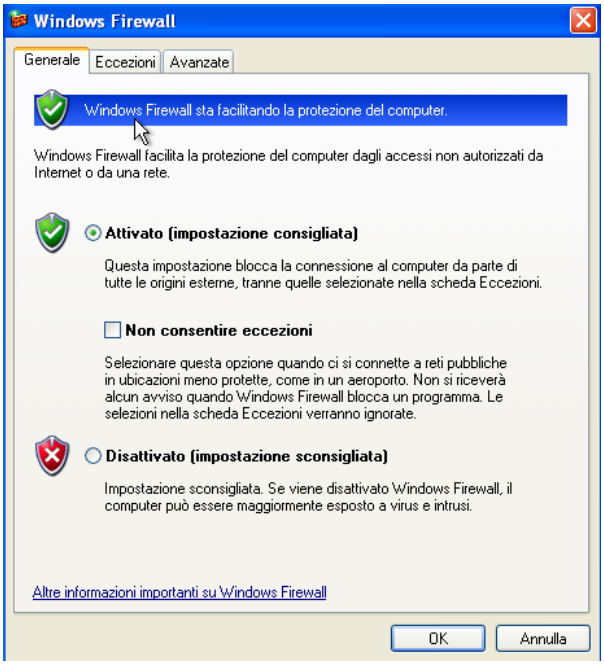


Una volta fatto, passiamo sulla macchina Kali ed effettuiamo una scansione con il comando **nmap** verso la macchina target.

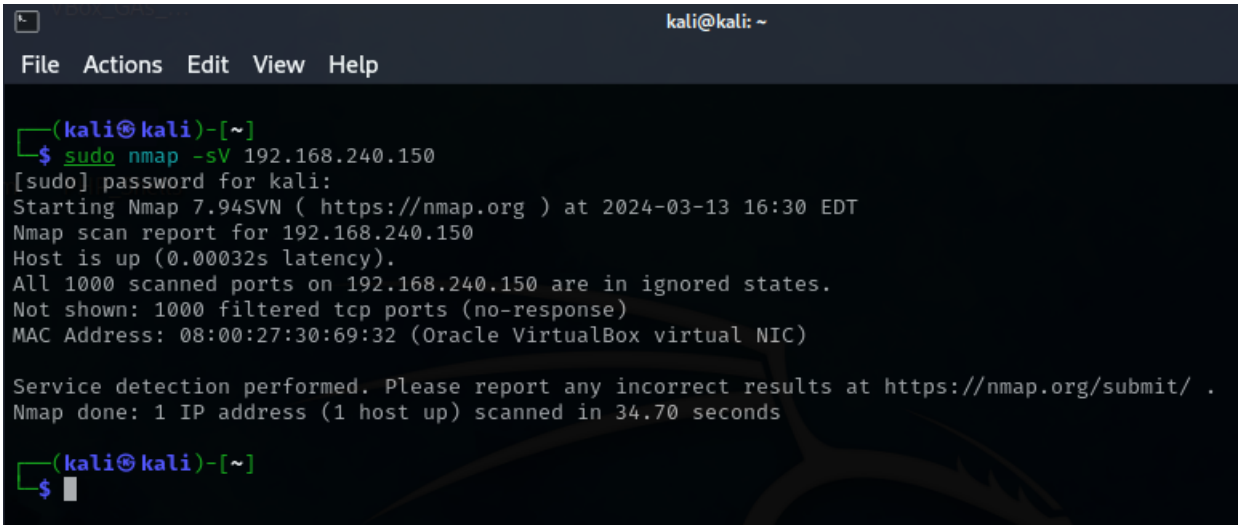


Secondo test: scansione con attivazione del Firewall di Windows Xp

Attiviamo il firewall come richiesto dalla traccia.



Una volta fatto, passiamo sulla macchina Kali ed effettuiamo una scansione con il comando **nmap** verso la macchina target.



Differenze

Dalle scansioni effettuate in precedenza si evince che se viene abilitato un Firewall sulla macchina target (o in protezione esterna allo stesso) questo impedisce di effettuare operazioni da parte di un potenziale attaccante.

Se invece questo risulta disattivo o non presente, un'attaccante potrebbe tranquillamente effettuare scansioni ed individuare delle potenziali vulnerabilità presenti nella macchina (come nel secondo test).

La differenza principale è che nonostante vi siano delle vulnerabilità di sistema presenti nella macchina XP:

- se il firewall risulta disattivato, la macchina è esposta a rischi
- se il firewall risulta attivato, nonostante siano ancora presenti, queste vengono difese, tutelando così la macchina da accessi malevoli.