REPORT

SECURITY OPERATION: AZIONI PREVENTIVE

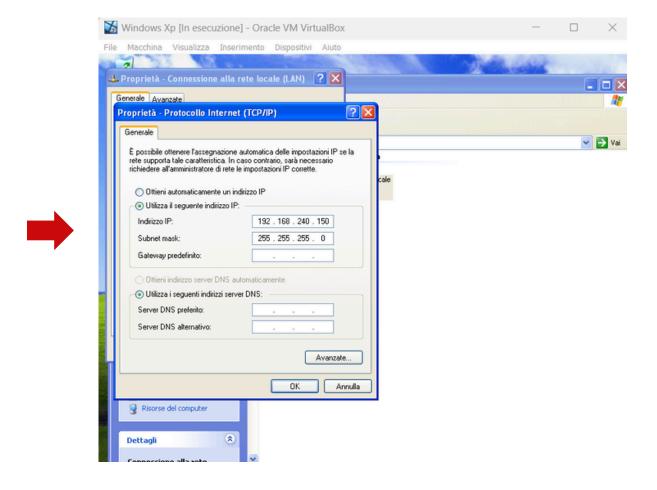
Alejandro Cristino S9-L1

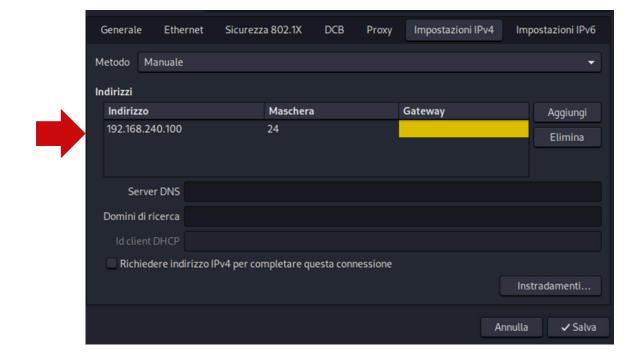
Obiettivo dell'esercizio:

L'obiettivo è verificare come l'attivazione del firewall su una macchina Windows XP/7 influisca sui risultati di una scansione dei servizi dall'esterno utilizzando nmap. Questo aiuta a comprendere l'efficacia del firewall nel bloccare le connessioni non autorizzate.

Setup dell'ambiente:

- Indirizzo IP della macchina Windows XP: 192.168.240.150
- Indirizzo IP della macchina Kali Linux: 192.168.240.100

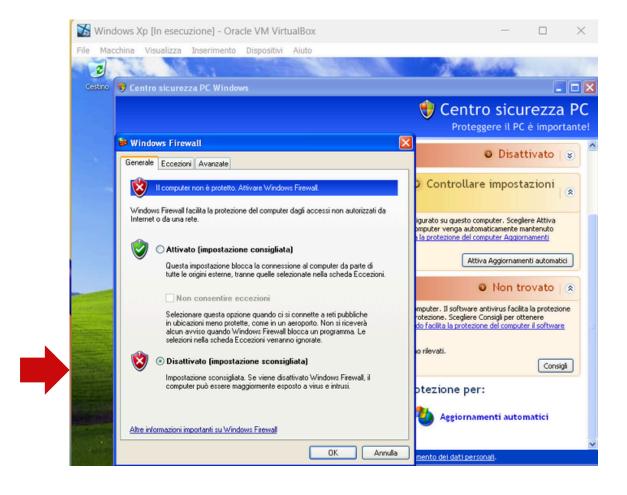




Passaggi svolti:

1. Assicurarsi che il firewall sia disattivato sulla macchina Windows XP:

• Il firewall è stato disattivato per eseguire una scansione completa dei servizi disponibili senza alcuna restrizione.



2. Effettuare una scansione con nmap sulla macchina target:

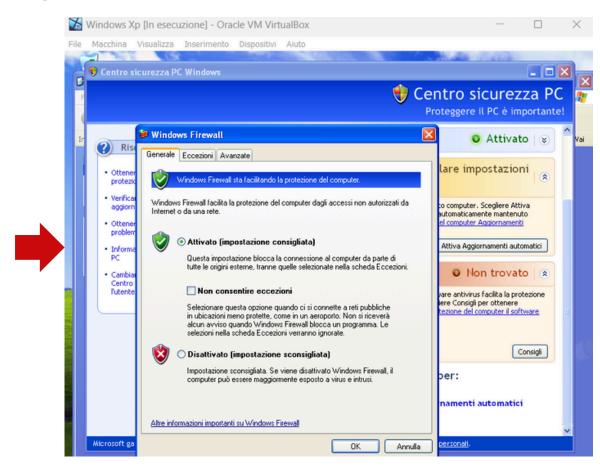
Comandi utilizzati:

nmap -sV -oN output_no_firewall 192.168.240.150 (lo switch-sV, per la service detection e -o nomefilereport per salvare in un file l'output)

cat output_no_firewall (visualizzare il contenuto di un file)

3. Abilitare il firewall sulla macchina Windows XP:

• Il firewall è stato abilitato per bloccare le connessioni non autorizzate.



4. Effettuare una seconda scansione con nmap:

Comando utilizzato:

- nmap -sV -oN output_with_firewall 192.168.240.150 (lo switch-sV, per la service detection e -o nomefilereport per salvare in un file l'output)
- cat output_no_firewall (visualizzare il contenuto di un file)

```
(kali® kali)-[~]
$ nmap -sV -oN output_with_firewall 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 09:40 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.10 seconds
(kali@ kali)-[~]
$ cat output_with_firewall
```

Nmap 7.94SVN scan initiated Mon Jul 22 09:40:59 2024 as: nmap -sV -oN output_with_firewall 192.168.240.150

Nmap done at Mon Jul 22 09:41:02 2024 -- 1 IP address (0 hosts up) scanned in 3.10 seconds

5. Provare ulteriori scansioni con il firewall attivato:

Comando per scansione differente:

• nmap -p- 192.168.240.150

```
(kali® kali)-[~]
$ nmap -p- 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 09:44 EDT
Stats: 0:00:02 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Ping Scan Timing: About 50.00% done; ETC: 09:44 (0:00:02 remaining)
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.03 seconds
```

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

- Differenze notate: La scansione senza firewall mostra tutte le porte e i servizi aperti, mentre la scansione con il firewall attivato non mostra alcuna porta aperta e il sistema risulta "down".
- Motivo delle differenze: Il firewall blocca le connessioni non autorizzate e le risposte ai ping, rendendo la macchina invisibile alle scansioni esterne. Questo dimostra l'efficacia del firewall nel proteggere il sistema dalle scansioni di rete e dagli accessi non autorizzati.