SOC:
Azioni Preventive

Scan con Nmap di Windows XP

Firewall on/off

Set up IP

Come prima cosa andiamo ad inmpostare gli Ip delle VM come richiesto dalla traccia

KALI: 192.168.240.100

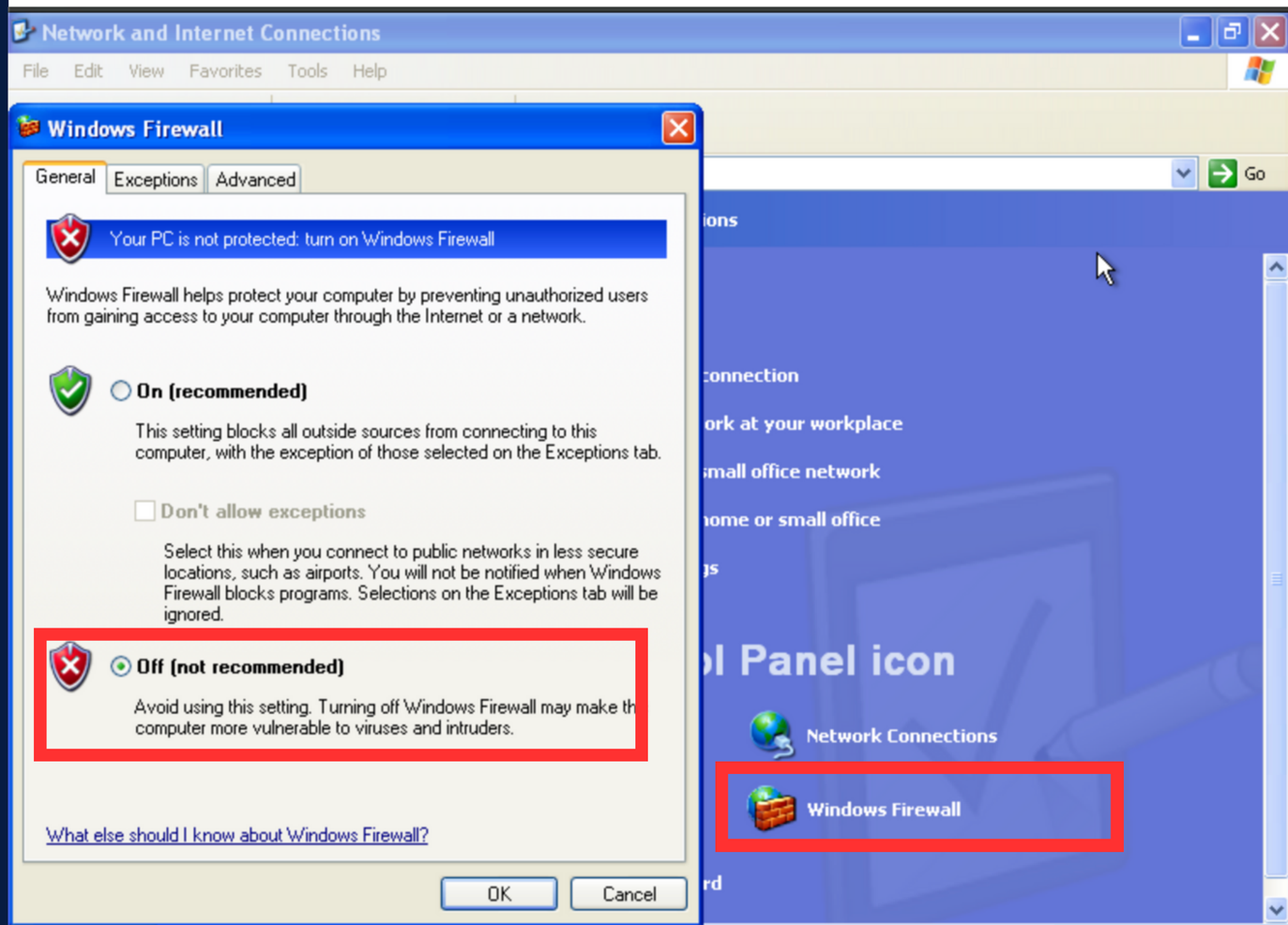
WINDOWS XP: 192.168.240.150

Set up Firewall

Poi impostiamo il firewall di windows su off:

- accediamo al pannello di controllo
- clicchiamo sulla voce network and internet connections
- quindi su Windows Firewall

COME MOSTRATO IN FIGURA



Scan con Nmap: Firewall OFF

Spostiamoci su Kali e da terminale digitiamo il comando per la scansione con nmap: ***sudo nmap -sV -O 192.168.240.150***

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -O 192.168.240.150
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-29 10:08 GMT
Nmap scan report for 192.168.240.150
Host is up (0.0021s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
MAC Address: 52:E1:4D:29:07:B8 (Unknown)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp cpe:/o:microsoft:windows_server_2003
OS details: Microsoft Windows XP SP2 or SP3, or Windows Server 2003
Network Distance: 1 hop
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:w
indows_xp

OS and Service detection performed. Please report any incorrect results at https://nmap.o
rg/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.50 seconds
```

Spieghiamo il comando:

- **-sV** sta per scan Verbouse per avere maggiori informazioni
- **-O** è un elemento in più per conoscere il sistema operativo nel dettaglio

Conclusione

Possimo vedere che nmap è riuscita a riportare tutte le informazioni richieste:

- le porte aperte con i relativi servizi e versioni
- i dettagli del OS target

Scan con Nmap: Firewall ON

Dopo aver impostato il firewall di Windows Xp su ON spostiamoci su Kali e da terminale digitiamo lo stesso comando fatto in precedenza per la scansione con nmap: ***sudo nmap -sV -O 192.168.240.150***

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -O 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-29 10:12 GMT
Nmap scan report for 192.168.240.150
Host is up (0.00054s latency).
All 1000 scanned ports on 192.168.240.150 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 52:E1:4D:29:07:B8 (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at https://nmap.
rg/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 37.31 seconds
```

Spieghiamo il comando:

- **-sV** sta per scan Verbouse per avere maggiori informazioni
- **-O** è un elemento in più per conoscere il sistema operativo nel dettaglio

Conclusione

Possimo vedere che nmap non è riuscita a riportare tutte le informazioni richieste:

- non c'è stata alcuna risposta dalle porte, tutti i pacchetti sono stati ignorati
- e non c'è stato possibile recuperare informazioni sul OS

In altre parole il firewall ha bloccato tutti i pacchetti impedendoci di avere risposte da Windows con le relative informazioni

Scan con Nmap: Firewall ON Eventuali Soluzioni

Una possibile escamotage è quello di utilizzare questo comando: ***sudo nmap -sM -vv -p 445 192.168.240.150***

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sM -vv -p 445 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-29 10:25 GMT
Initiating ARP Ping Scan at 10:25
Scanning 192.168.240.150 [1 port]
Completed ARP Ping Scan at 10:25, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:25
Completed Parallel DNS resolution of 1 host. at 10:26, 13.00s elapsed
Initiating Maimon Scan at 10:26
Scanning 192.168.240.150 [1 port]
Completed Maimon Scan at 10:26, 0.23s elapsed (1 total ports)
Nmap scan report for 192.168.240.150
Host is up, received arp-response (0.00064s latency).
Scanned at 2024-01-29 10:26:02 GMT for 0s

PORT    STATE         SERVICE      REASON
445/tcp open|filtered microsoft-ds no-response
MAC Address: 52:E1:4D:29:07:B8 (Unknown)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 13.37 seconds
           Raw packets sent: 3 (108B) | Rcvd: 1 (28B)
```

Spieghiamo il comando:

- **-sM** sta per scansione TCP Maimon: che serve per eludere alcune regole firewall
- **-vv** serve per aumentare il dettaglio dell info in output
- **-p** identifica una porta specifica dascannerizzare

Conclusione

In questo modo possiamo andare a provare la scansione attraverso porte di comune utilizzo per capire se sono aperte o meno seppur protette da firewall come mostrato in figura.
Nel dettaglio **-sM** permette di inviare pacchetti FIN/ACK con delle flags ed in base alla risposta determina se le porte sono aperte o chiuse, anche qualora il pacchetto venisse ignorato, come nel caso di un firewall.