REPORT 19/12/2022 LORENZO SCORBAIOLI

TASK:

Verificare in che modo l'attivazione del Fireall di Windows XP impatta il risultato di una scansione dei servizi dall'esterno. Per questo motivo:

1. Assicurarsi che il Firewall sia disattivato sulla macchina XP
2. Effettuare una scansione con Nmap sulla macchina target (utilizzare lo switch -sV e -o)
3. Abilitare il Firewall sulla macchina XP
4. Effettuare una seconda scansione con Nmap
5. Trovare le differenze e motivarle

REQUISITI:

1. Configurare l'indirizzo IP di Windows XP: 192.168.240.150
2. Configurare l'indirizzo IP di Kali: 192.168.240.100

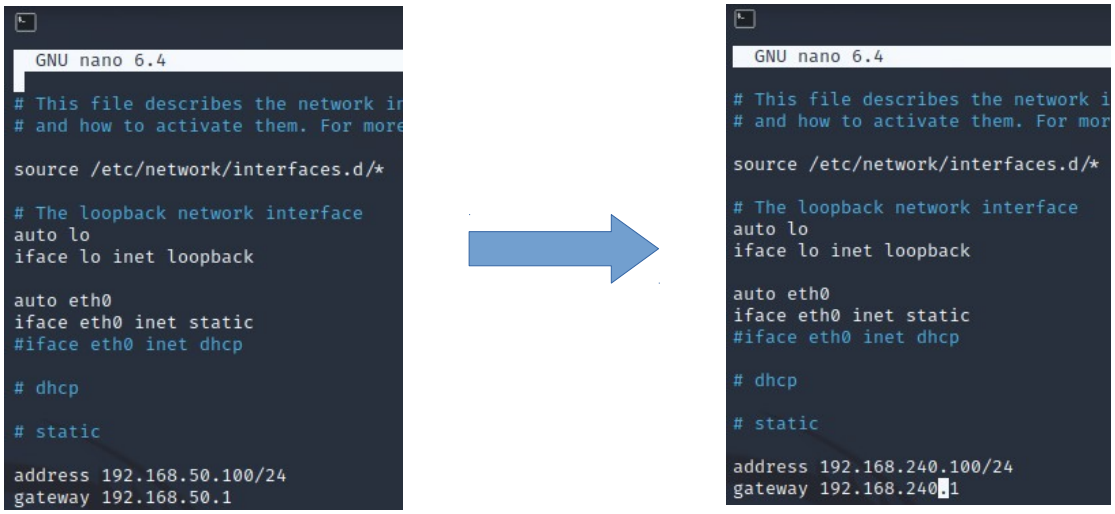
BONUS:

Monitorare i Log di Windows:

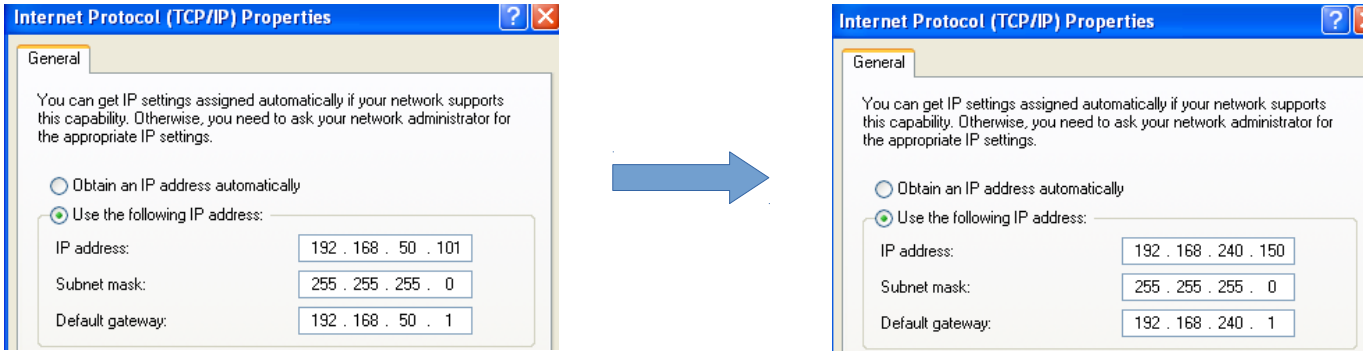
1. Quali log vengono modificati?
2. Cosa riesce a trovare?

Il primo passo per la risoluzione di questo esercizio è stato quello di andare a modificare gli indirizzi IP della macchina attaccante, Kali, e quello della macchina attaccata, Windows XP, andandoli a cambiare con quelli richiesti dalla traccia:

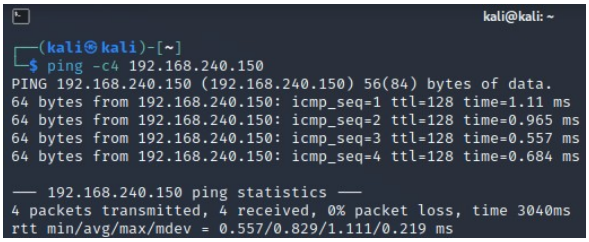
KALI

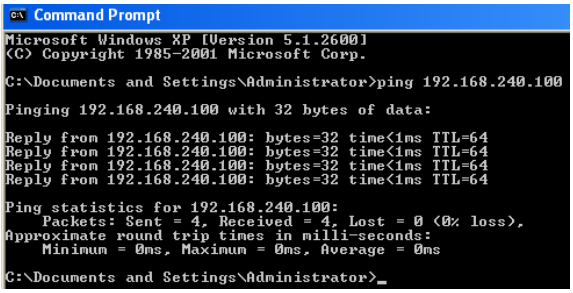


WINDOWS XP

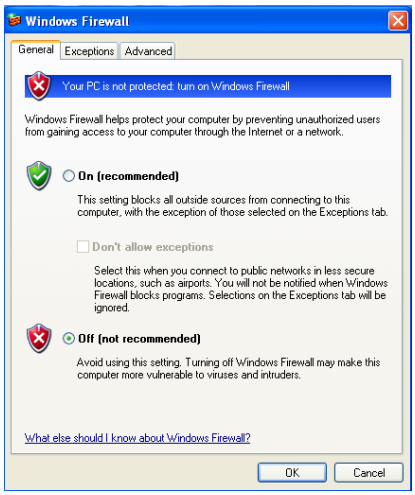


Dopo avere riavviato la configurazione di rete ho proceduto a lanciare il comando ping sia sulla macchina Kali che Windows XP:





A questo punto sono andato su windows XP a confermare che il Firewall fosse spento:



Avuta la conferma sono tornato sulla macchina Kali dove ho eseguito una scansione con Nmap verso la macchina Windows con lo switch -sV e -o come richiesto dalla traccia, per ottenere così la versione dei servizi attivi e generare un report della scansione:

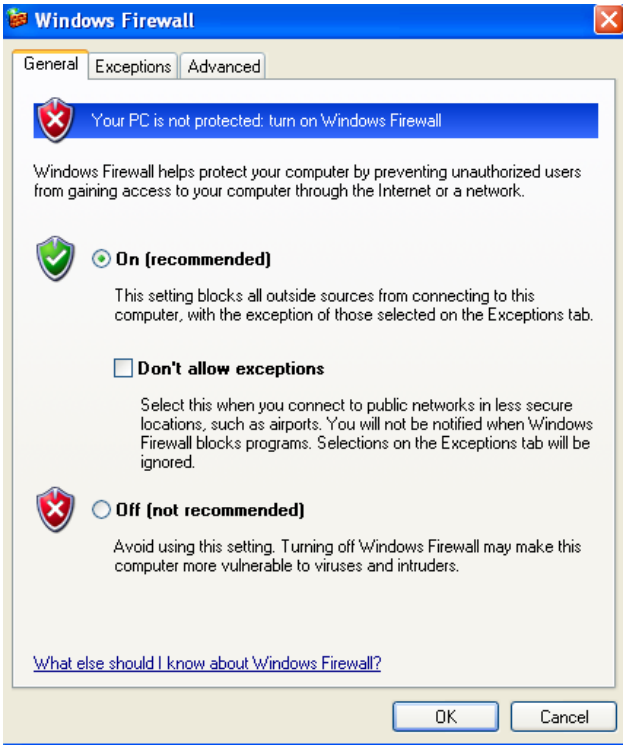
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.240.150 -o /home/kali/Desktop/eserciziofirewall
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-19 08:23 EST
Nmap scan report for 192.168.240.150
Host is up (0.00024s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE      VERSION
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: 08:00:27:07:EE:7C (Oracle VirtualBox virtual NIC)
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.47 seconds
```

~/Desktop/eserciziofirewall [Read Only] - Mousepad

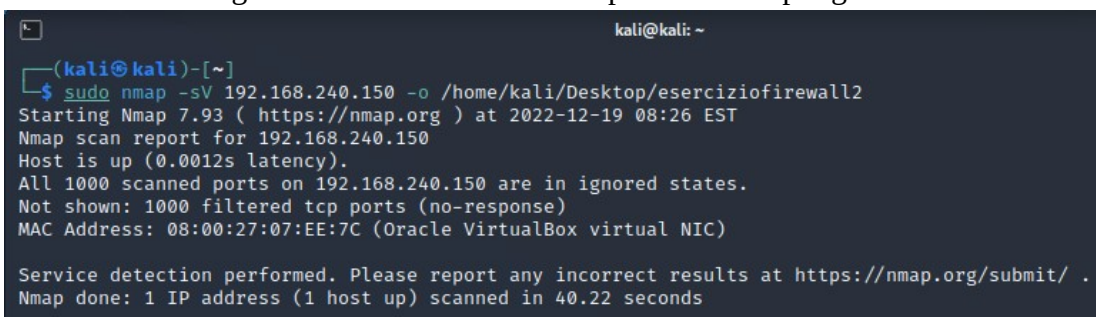
File Edit Search View Document Help

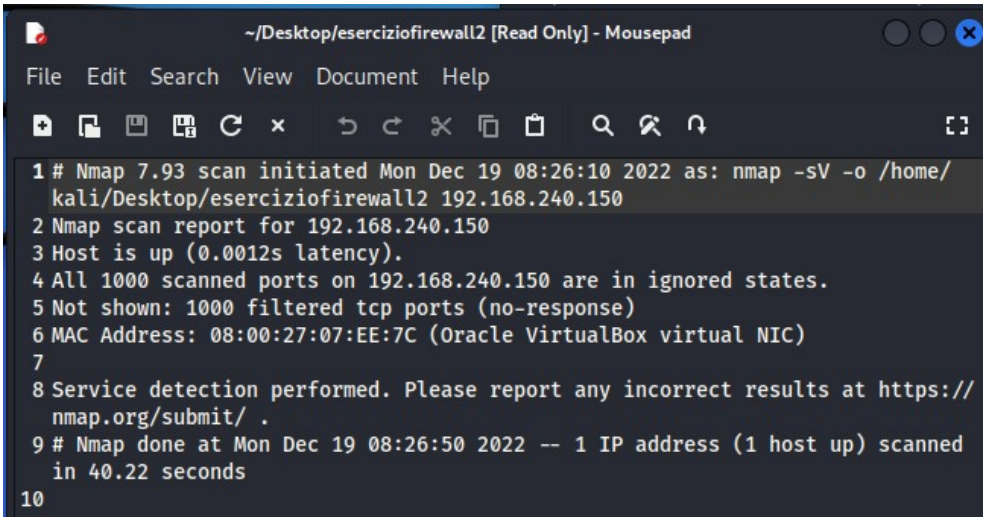
```
 1 # Nmap 7.93 scan initiated Mon Dec 19 08:23:30 2022 as: nmap -sV -o /home/
   kali/Desktop/eserciziofirewall 192.168.240.150
 2 Nmap scan report for 192.168.240.150
 3 Host is up (0.00024s latency).
 4 Not shown: 997 closed tcp ports (reset)
 5 PORT    STATE SERVICE      VERSION
 6 135/tcp open  msrpc        Microsoft Windows RPC
 7 139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
 8 445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
 9 MAC Address: 08:00:27:07:EE:7C (Oracle VirtualBox virtual NIC)
10 Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/
   o:microsoft:windows_xp
11
12 Service detection performed. Please report any incorrect results at https://
   nmap.org/submit/ .
13 # Nmap done at Mon Dec 19 08:23:51 2022 -- 1 IP address (1 host up) scanned
   in 21.47 seconds
14
```

A questo punto sono andato a riabilitare il Firewall di Windows XP:

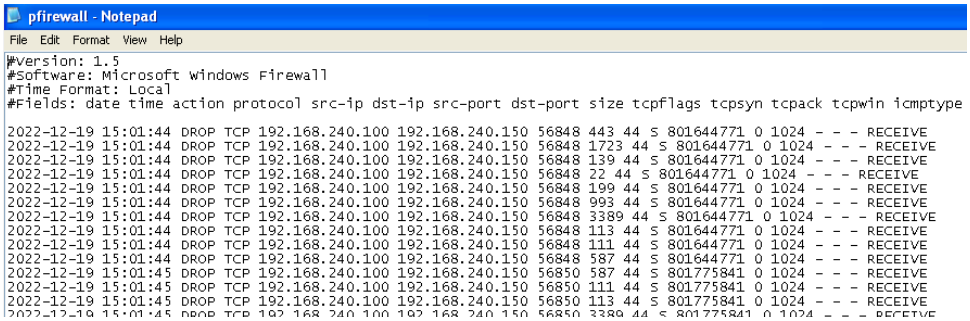


Ed ho nuovamente eseguito una scansione con Nmap usando sempre gli switch -sV e -o:





Mettendo a confronto le due scansioni possiamo vedere come nella prima, quella con il firewall abbassato, riusciamo a ottenere informazioni sulle porte aperte, i servizi che lavorano su di esse e anche la versione dei servizi. Nella scansione con il firewall alzato invece non riusciamo ad ottenere nessuna di queste informazioni. L'unica informazione che ci fornisce è che Nmap ha omesso di mettere in lista 1000 porte TCP poiché sono filtrate. Tramite il quesito bonus ho avuto conferma del fatto che le porte risultano filtrate: il Firewall droppa tutte le richiete TCP. Andando a cercare i log del Firewall, situati nel file di testo "pfirewall" nella cartella C://WINDOWS, possiamo vedere quanto segue:



```
#Version: 1.5
#Software: Microsoft Windows Firewall
#Time Format: Local
#Fields: date time action protocol src-ip dst-ip src-port dst-port size tcpflags tcpsyn tcpack tcpwin icmptype

2022-12-19 15:01:44 DROP TCP 192.168.240.100 192.168.240.150 56848 443 44 S 801644771 0 1024 - - - RECEIVE
2022-12-19 15:01:44 DROP TCP 192.168.240.100 192.168.240.150 56848 1723 44 S 801644771 0 1024 - - - RECEIVE
2022-12-19 15:01:44 DROP TCP 192.168.240.100 192.168.240.150 56848 139 44 S 801644771 0 1024 - - - RECEIVE
2022-12-19 15:01:44 DROP TCP 192.168.240.100 192.168.240.150 56848 22 44 S 801644771 0 1024 - - - RECEIVE
2022-12-19 15:01:44 DROP TCP 192.168.240.100 192.168.240.150 56848 199 44 S 801644771 0 1024 - - - RECEIVE
2022-12-19 15:01:44 DROP TCP 192.168.240.100 192.168.240.150 56848 993 44 S 801644771 0 1024 - - - RECEIVE
2022-12-19 15:01:44 DROP TCP 192.168.240.100 192.168.240.150 56848 3389 44 S 801644771 0 1024 - - - RECEIVE
2022-12-19 15:01:44 DROP TCP 192.168.240.100 192.168.240.150 56848 113 44 S 801644771 0 1024 - - - RECEIVE
2022-12-19 15:01:44 DROP TCP 192.168.240.100 192.168.240.150 56848 111 44 S 801644771 0 1024 - - - RECEIVE
2022-12-19 15:01:44 DROP TCP 192.168.240.100 192.168.240.150 56848 587 44 S 801644771 0 1024 - - - RECEIVE
2022-12-19 15:01:45 DROP TCP 192.168.240.100 192.168.240.150 56850 587 44 S 801775841 0 1024 - - - RECEIVE
2022-12-19 15:01:45 DROP TCP 192.168.240.100 192.168.240.150 56850 111 44 S 801775841 0 1024 - - - RECEIVE
2022-12-19 15:01:45 DROP TCP 192.168.240.100 192.168.240.150 56850 113 44 S 801775841 0 1024 - - - RECEIVE
2022-12-19 15:01:45 DROP TCP 192.168.240.100 192.168.240.150 56850 3389 44 S 801775841 0 1024 - - - RECEIVE
```

Per data e orario, il file ci indica il tipo d'azione sostenuta dal Firewall, in questo caso "drop, il tipo di protocollo adottato, TCP, l'IP sorgente, che corrisponde a quello della macchina Kali, l'IP destinatario, che corrisponde a quello di Windows XP, la porta sorgente, la porta destinataria e tutta una serie di ulteriori informazioni. Facendo una scansione con il Firewall abbassato in questo file non viene aggiunta alcuna informazione.

Sono anche andato ad ispezionare i log di sistema tramite l'applicazione Event Viewer ma non ho trovato alcuna traccia delle scansioni effettuate con Nmap, sia con il Firewall alzato che abbassato, avendole effettuate intorno alle 16:15:

System 362 event(s)

Type	Date	Time	Source	Category	Event	User	Computer
Error	19/12/2022	16.02.02	W32Time	None	29	N/A	WXP
Error	19/12/2022	16.02.02	W32Time	None	17	N/A	WXP
Information	19/12/2022	15.47.02	Service Control Manager	None	7036	N/A	WXP
Information	19/12/2022	15.47.02	Service Control Manager	None	7035	Administrator	WXP
Information	19/12/2022	15.47.02	Service Control Manager	None	7036	N/A	WXP
Information	19/12/2022	15.47.02	Service Control Manager	None	7036	N/A	WXP
Information	19/12/2022	15.47.02	Service Control Manager	None	7035	SYSTEM	WXP
Information	19/12/2022	15.47.02	Service Control Manager	None	7036	N/A	WXP
Information	19/12/2022	15.47.02	Service Control Manager	None	7035	SYSTEM	WXP
Information	19/12/2022	15.47.02	Service Control Manager	None	7036	N/A	WXP
Information	19/12/2022	15.47.02	Service Control Manager	None	7035	SYSTEM	WXP
Information	19/12/2022	15.47.02	Service Control Manager	None	7036	N/A	WXP
Information	19/12/2022	15.47.02	Service Control Manager	None	7035	SYSTEM	WXP
Information	19/12/2022	15.47.02	Service Control Manager	None	7036	N/A	WXP
Information	19/12/2022	15.47.02	Service Control Manager	None	7035	SYSTEM	WXP
Error	19/12/2022	15.47.01	W32Time	None	29	N/A	WXP
Error	19/12/2022	15.47.01	W32Time	None	17	N/A	WXP
Error	19/12/2022	15.46.58	W32Time	None	29	N/A	WXP