

Consegna S9L1:

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 che abbiamo utilizzato 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 nomefile` 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.

3

Traccia:

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

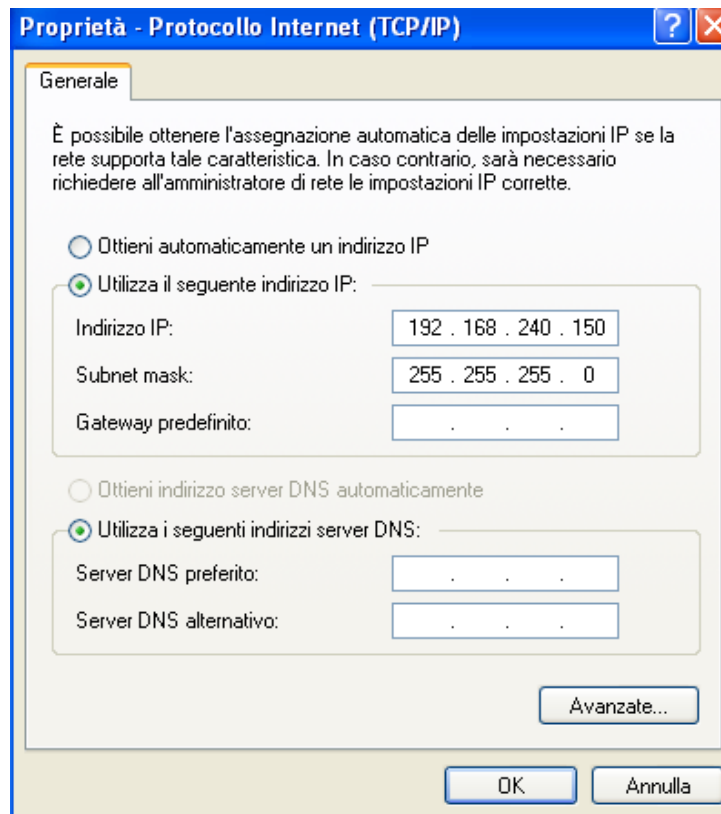
Requisiti:

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

Configurazione indirizzi IP Kali Linux e Windows XP:

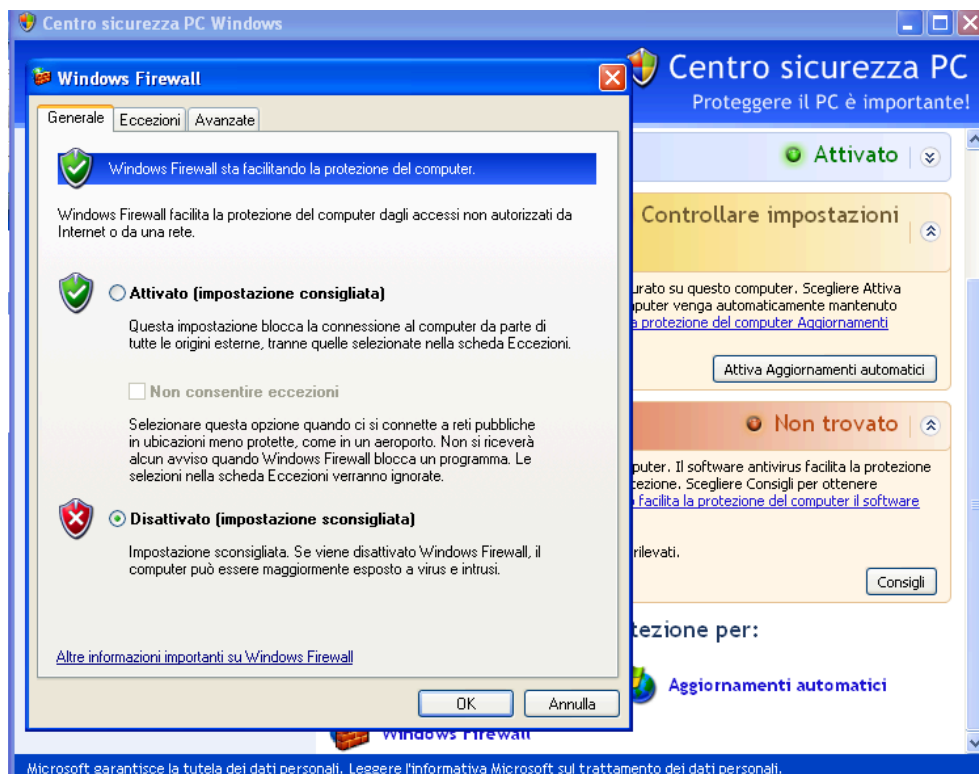
```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:b1:f1:9a brd ff:ff:ff:ff:ff:ff
    inet 192.168.240.100/24 brd 192.168.240.255 scope global noprefixroute eth0
        valid_lft forever preferred_lft forever
```



Ping di conferma tra le due macchine:

```
(kali@kali)-[~]  
$ ping 192.168.240.150 -c3  
PING 192.168.240.150 (192.168.240.150) 56(84) bytes of data.  
64 bytes from 192.168.240.150: icmp_seq=1 ttl=128 time=8.15 ms  
64 bytes from 192.168.240.150: icmp_seq=2 ttl=128 time=4.49 ms  
64 bytes from 192.168.240.150: icmp_seq=3 ttl=128 time=4.62 ms  
  
— 192.168.240.150 ping statistics —  
3 packets transmitted, 3 received, 0% packet loss, time 2006ms  
rtt min/avg/max/mdev = 4.494/5.755/8.149/1.693 ms
```

Disattivazione del firewall su Win XP:



Effettuiamo una scansione nmap per controllare quale porte siano aperte sull'indirizzo IP di Windows XP, tramite gli switch -sV e -o seguito da "ConsegnaXP" che sarebbe il nostro file di testo creato.

```
(kali㉿kali)-[~]
$ nmap -sV 192.168.240.150 -o ConsegnaXP.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-23 10:03 CEST
Nmap scan report for 192.168.240.150
Host is up (0.0053s latency).
Not shown: 997 closed tcp ports (conn-refused)
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
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 7.55 seconds
```

```
(kali㉿kali)-[~]
$ cat ConsegnaXP.txt
# Nmap 7.94SVN scan initiated Tue Jul 23 10:03:36 2024 as: nmap -sV -o ConsegnaXP.txt 192.168.240.150
Nmap scan report for 192.168.240.150
Host is up (0.0053s latency).
Not shown: 997 closed tcp ports (conn-refused)
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
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 at Tue Jul 23 10:03:43 2024 -- 1 IP address (1 host up) scanned in 7.55 seconds
```

Adesso riattiviamo il firewall su Windows ed effettuiamo un'altra scansione nmap, con la unica differenza che per vada con successo dobbiamo aggiungere il comando -Pn.

```
(kali㉿kali)-[~]
$ nmap -sV 192.168.240.150 -o Consegnafirewall.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-23 10:07 CEST
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 3.24 seconds

(kali㉿kali)-[~]
$ nmap -Pn -sV 192.168.240.150 -o Consegnafirewall.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-23 10:08 CEST
Nmap scan report for 192.168.240.150
Host is up (0.0030s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows XP microsoft-ds
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 12.84 seconds

(kali㉿kali)-[~]
$ cat Consegnafirewall.txt
# Nmap 7.94SVN scan initiated Tue Jul 23 10:08:29 2024 as: nmap -Pn -sV -o Consegnafirewall.txt 192.168.240.150
Nmap scan report for 192.168.240.150
Host is up (0.0030s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows XP microsoft-ds
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 at Tue Jul 23 10:08:42 2024 -- 1 IP address (1 host up) scanned in 12.84 seconds
```

Eseguendo un nuovo nmap, pero questa volta con lo switch -O, riusciamo ad ottenere informazioni sul sistema windows, anche se il firewall è attivo. Le informazioni le ritroviamo in "OS CPE:"

```
(kali㉿kali)-[~]
$ sudo nmap -Pn -O 192.168.240.150 -o Consegnafirewall2.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-23 10:13 CEST
Nmap scan report for 192.168.240.150
Host is up (0.0032s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 08:00:27:5C:8D:1C (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|specialized
Running (JUST GUESSING): Microsoft Windows XP|2003|2008|2000 (96%), General Dynamics embedded (89%)
OS CPE: cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_server_2003::sp1 cpe:/o:microsoft:windows_serv
er_2003::sp2 cpe:/o:microsoft:windows_server_2008::sp2 cpe:/o:microsoft:windows_2000::sp4
Aggressive OS guesses: Microsoft Windows XP SP3 (96%), Microsoft Windows XP (94%), Microsoft Windows Server 2003
SP1 or SP2 (94%), Microsoft Windows Server 2008 Enterprise SP2 (93%), Microsoft Windows Server 2003 SP2 (93%),
Microsoft Windows XP SP2 or SP3 (93%), Microsoft Windows 2000 SP4 (93%), Microsoft Windows XP SP2 or Windows Ser
ver 2003 (92%), Microsoft Windows 2000 SP4 or Windows XP SP2 or SP3 (90%), Microsoft Windows 2003 SP2 (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.70 seconds
```

Tramite Wireshark analizziamo il traffico di rete, per notare le trasmissioni che facciamo con nmap, e possiamo notare che molte di queste non avvengono con successo, lo possiamo notare nello screen in basso evidenziato in rosso

Wireshark interface showing network traffic on *eth0. The packet list displays various protocols and their details. The following table represents the data visible in the packet list:

No.	Time	Source	Destination	Protocol	Length	Info
2144	117.034161145	zte_09:67:e8	Broadcast	ARP	60	Who has 192.168.1.178? Tell 192.168.1.1
2145	117.103119581	192.168.1.129	192.168.1.255	UDP	77	43752 → 15600 Len=35
2146	118.114777132	192.168.240.100	192.168.240.150	TCP	74	[TCP Port numbers reused] 33440 → 139 [SYN] Seq=0
2147	118.117165394	192.168.240.150	192.168.240.100	TCP	78	139 → 33440 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0
2148	118.117211883	192.168.240.100	192.168.240.150	TCP	54	33440 → 139 [RST] Seq=1 Win=0 Len=0
2149	118.216907175	192.168.240.100	192.168.240.150	TCP	74	[TCP Port numbers reused] 33441 → 139 [SYN] Seq=0
2150	118.219620431	192.168.240.150	192.168.240.100	TCP	78	139 → 33441 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0
2151	118.219676613	192.168.240.100	192.168.240.150	TCP	54	33441 → 139 [RST] Seq=1 Win=0 Len=0
2152	118.317599879	192.168.240.100	192.168.240.150	TCP	74	[TCP Port numbers reused] 33442 → 139 [SYN] Seq=0
2153	118.321169543	192.168.240.150	192.168.240.100	TCP	74	139 → 33442 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0
2154	118.321230307	192.168.240.100	192.168.240.150	TCP	54	33442 → 139 [RST] Seq=1 Win=0 Len=0
2155	118.418885537	192.168.240.100	192.168.240.150	TCP	70	[TCP Port numbers reused] 33443 → 139 [SYN] Seq=0
2156	118.423352587	192.168.240.150	192.168.240.100	TCP	78	139 → 33443 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0
2157	118.423407240	192.168.240.100	192.168.240.150	TCP	54	33443 → 139 [RST] Seq=1 Win=0 Len=0
2158	118.520706221	192.168.240.100	192.168.240.150	TCP	74	[TCP Port numbers reused] 33444 → 139 [SYN] Seq=0
2159	118.525007928	192.168.240.150	192.168.240.100	TCP	78	139 → 33444 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0
2160	118.525079625	192.168.240.100	192.168.240.150	TCP	54	33444 → 139 [RST] Seq=1 Win=0 Len=0
2161	118.621092082	192.168.240.100	192.168.240.150	TCP	70	[TCP Port numbers reused] 33445 → 139 [SYN] Seq=0
2162	118.624027179	192.168.240.150	192.168.240.100	TCP	74	139 → 33445 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0
2163	118.624345973	192.168.240.100	192.168.240.150	TCP	54	33445 → 139 [RST] Seq=1 Win=0 Len=0
2164	118.648581539	192.168.240.100	192.168.240.150	ICMP	162	Echo (ping) request id=0xe7bc, seq=295/9985, ttl=

Con questo possiamo notare quanto sia importante impostare il firewall attivo, che aiuta notevolmente la protezione del pc, che nonostante abbia porte aperte ci nega l'entrata.