

Security Operation: azioni preventive

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.

Sono andato a configurare gli indirizzi IP di entrambe le macchine ai seguenti indirizzi:

-Kali 192.168.240.100

-Windows XP 192.168.240.150

```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
GNU nano 6.4 /etc/network/interfaces  
# This file describes the network interfaces available on your system  
# and how to activate them. For more information, see interfaces(5).  
  
source /etc/network/interfaces.d/*  
  
# The loopback network interface  
auto lo  
iface lo inet loopback  
  
auto eth0  
iface eth0 inet static  
address 192.168.240.100  
netmask 255.255.255.0  
gateway 192.168.1.101
```

```
(kali@kali): ~  
$ ping 192.168.240.150  
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=2.01 ms  
64 bytes from 192.168.240.150: icmp_seq=2 ttl=128 time=2.79 ms  
64 bytes from 192.168.240.150: icmp_seq=3 ttl=128 time=3.46 ms  
64 bytes from 192.168.240.150: icmp_seq=4 ttl=128 time=3.63 ms  
64 bytes from 192.168.240.150: icmp_seq=5 ttl=128 time=3.70 ms  
^C  
--- 192.168.240.150 ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 4013ms  
rtt min/avg/max/mdev = 2.006/3.117/3.697/0.641 ms
```

Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☐ Obtain an IP address automatically

☒ Use the following IP address:

IP address: 192.168.240.150

Subnet mask: 255.255.255.0

Default gateway: 192.168.1.201

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server: . . .

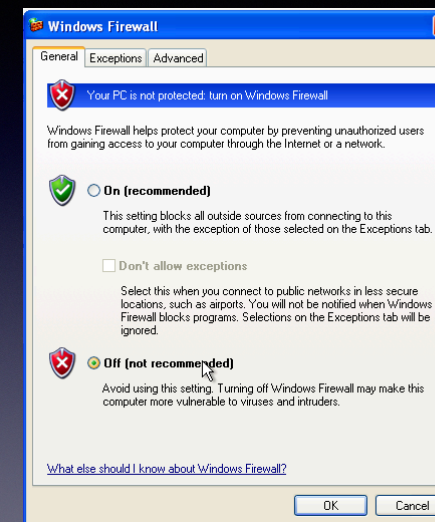
Alternate DNS server: . . .

Advanced

```
C:\Documents and Settings\Fabio\QOI>ping 192.168.240.100  
Pinging 192.168.240.100 with 32 bytes of data:  
Reply from 192.168.240.100: bytes=32 time=1ms TTL=64  
Reply from 192.168.240.100: bytes=32 time=2ms TTL=64  
Reply from 192.168.240.100: bytes=32 time=2ms TTL=64  
Reply from 192.168.240.100: bytes=32 time=1ms TTL=64  
Ping statistics for 192.168.240.100:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milliseconds:  
Minimum = 1ms, Maximum = 2ms, Average = 1ms  
C:\Documents and Settings\Fabio\QOI>
```

Fatto ciò sono andato a verificare lo stato del firewall su Windows, riscontrando che esso fosse disattivato.

Solo in questo modo la nostra macchina attaccante potrà effettuare una scansione con nmap come vedremo di seguito.



Infatti come risultato abbiamo ottenuto con comando “nmap -sV” la scansione porte e versione della macchina bersaglio.

In più ho creato un file (reportwindowsexp.txt) dove inserire il report della scansione appena effettuata, che ho associato con -o.

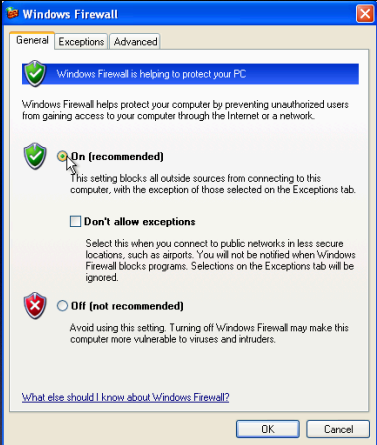
```
(kali@kali)~$ nmap -sV 192.168.240.150 -o reportwindowsexp.txt
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-19 13:58 CET
Nmap scan report for 192.168.240.150
Host is up (0.0028s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE        VERSION
135/tcp   open  msrpc          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 20.56 seconds
```

```
File Modifica Cerca Visualizza Documento Aiuto
1 # Nmap 7.93 scan initiated Mon Dec 19 13:58:26 2022 as: nmap -sV -o reportwindowsexp.txt 192.168.240.150
2 Nmap scan report for 192.168.240.150
3 Host is up (0.0028s latency).
4 Not shown: 997 closed tcp ports (conn-refused)
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 Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp
10
11 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
12 # Nmap done at Mon Dec 19 13:58:47 2022 -- 1 IP address (1 host up) scanned in 20.56 seconds
13
```

Ma adesso proviamo ad effettuare una scansione con firewall attivo e come risultato otteniamo l'esatto opposto, ovvero vi è comunicazione fra le macchine ma non è possibile effettuare alcuna scansione.

```
(kali@kali)-[~]
$ ping 192.168.240.150
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=5.02 ms
64 bytes from 192.168.240.150: icmp_seq=2 ttl=128 time=2.97 ms
64 bytes from 192.168.240.150: icmp_seq=3 ttl=128 time=2.64 ms
64 bytes from 192.168.240.150: icmp_seq=4 ttl=128 time=1.22 ms
64 bytes from 192.168.240.150: icmp_seq=5 ttl=128 time=2.71 ms
^C
--- 192.168.240.150 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4014ms
rtt min/avg/max/mdev = 1.217/2.911/5.018/1.218 ms
```

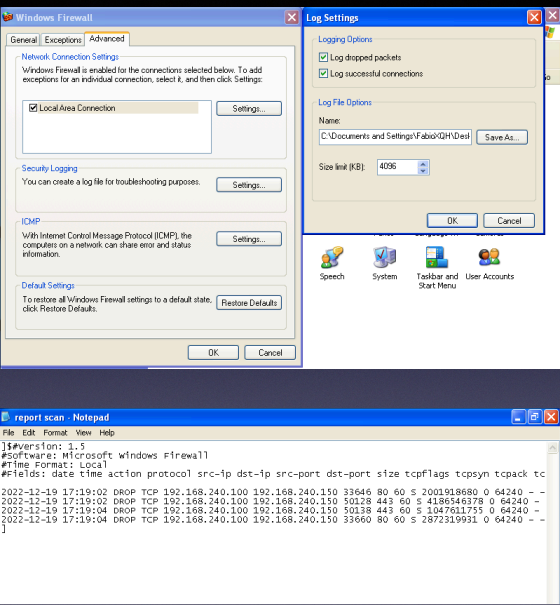


```
(kali@kali)-[~]
$ nmap -sV 192.168.240.150 -o reportwindowsxp.txt
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-19 14:10 CET
Note: Host seems down. If it is really up, but blocking our ping probes,
try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.18 seconds
```

```
~/reportwindowsxp.txt - Mousepad
File Modifica Cerca Visualizza Documento Aiuto

1 # Nmap 7.92 scan initiated Mon Dec 19 14:10:52 2022 as: nmap -sV -o
reportwindowsxp.txt 192.168.240.150
2 # Nmap done at Mon Dec 19 14:10:55 2022 -- 1 IP address (0 hosts up) scanned
in 3.18 seconds
3 |
```

Una cosa in più che sono andato a configurare nelle opzioni avanzate del firewall, sono i log dei pacchetti in uscita e le connessioni con eventuali macchine. Ricevendo un report di tentativo di invio pacchetti tcp da macchina attaccante Kali, bloccati dal firewall.



Conclusioni:

Come abbiamo visto nella lezione teorica di oggi, possiamo dedurre che il firewall gioca un ruolo fondamentale per la sicurezza dei dati all'interno di un sistema informatico.

Pertanto occorre prestare la massima attenzione e assicurarsi di tenere sempre attivo il firewall onde evitare che qualche malintenzionato possa andare ad effettuare azioni malevole nella nostra rete.