



Van Zwam Arjen

S9-L1 PRATICA



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 2. Effettuate una scansione con nmap sulla macchina target (utilizzate lo switch-sV, per la service detectione -o nomefile report 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.

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

CONFIG INDIRIZZI IP

Come da traccia, ho cambiato gli indirizzi IP delle due macchine, **Kali Linux** e **Windows XP**

```
(nejra@Nejra)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 192.168.240.100 netmask 255.255.255.0 broadcast 192.168.240.255
      inet6 fe80::a00:27ff:fe6:b28f prefixlen 64 scopeid 0x20<link>
        ether 08:00:27:c6:b2:8f txqueuelen 1000 (Ethernet)
          RX packets 0 bytes 0 (0.0 B)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 16 bytes 2424 (2.3 KiB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
      inet 127.0.0.1 netmask 255.0.0.0
      inet6 ::1 prefixlen 128 scopeid 0x10<host>
        loop txqueuelen 1000 (Local Loopback)
          RX packets 8 bytes 480 (480.0 B)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 8 bytes 480 (480.0 B)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
Microsoft Windows XP [Versione 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Nejra>ipconfig

Configurazione IP di Windows

Scheda Ethernet Connessione alla rete locale (LAN):
  Suffisso DNS specifico per connessione:
  Indirizzo IP . . . . . : 192.168.240.150
  Subnet mask . . . . . : 255.255.255.0
  Gateway predefinito . . . . . : 192.168.240.1

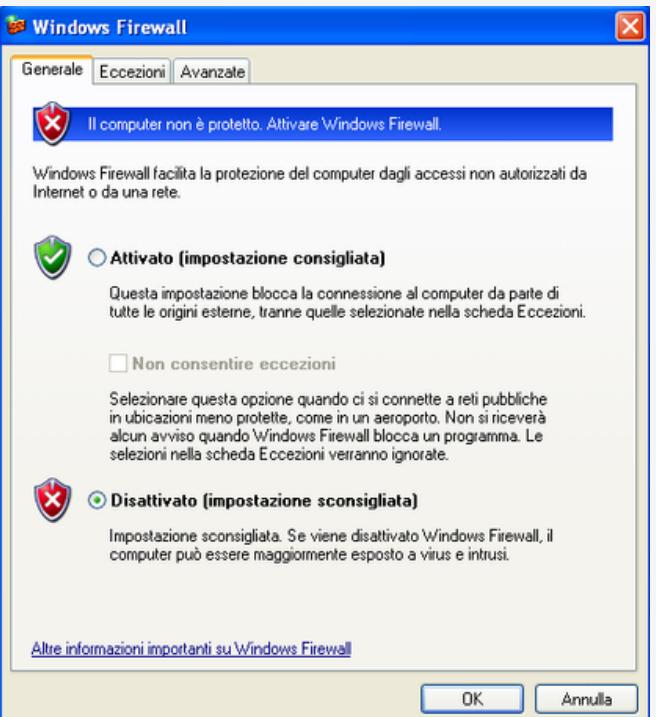
C:\Documents and Settings\Nejra>
```



NMAP SENZA FIREWALL

DISABILITARE FIREWALL

Innanzitutto ho controllato che i Firewall del Win XP fossero disabilitati come chiedeva la traccia.



NMAP -SV

Ho dunque startato NMAP tramite la shell di Kali

```
$ nmap -sV 192.168.240.150 -o report.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-22 14:13 CEST
Nmap scan report for 192.168.240.150
Host is up (0.00024s 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_xp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.66 seconds

# Nmap 7.94SVN scan initiated Mon Apr 22 14:13:58 2024 as: nmap -sV -o report.txt 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 (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_xp
10
11 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
12 # Nmap done at Mon Apr 22 14:14:19 2024 -- 1 IP address (1 host up) scanned in 20.66 seconds
```



NMAP SENZA FIREWALL

RISCONTRI

Come si può notare, abbiamo trovato tre **porte TCP** aperte: 135, 139 e 445. Dove potrebbero contenere **vulnerabilità**

File Azioni Modifica Visualizza Aiuto

```
└$ nmap -sV 192.168.240.150 -o report.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-22 14:13 CEST
Nmap scan report for 192.168.240.150
Host is up (0.00024s 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

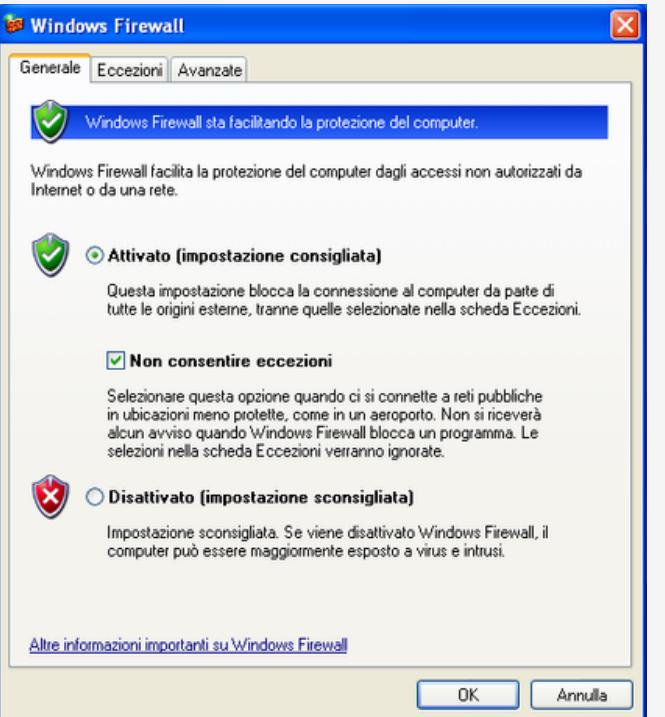
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.66 seconds
```



NMAP CON FIREWALL

ABILITARE FIREWALL

Questa volta, per confrontare i risultati, ho abilitato i Windows Firewall tramite il pannello di controllo dedicato



NMAP -SV

Ho dunque startato NMAP tramite la shell di Kali

```
(nejra@Nejra):[~]$ nmap -sV 192.168.240.150 -o report2.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-22 14:16 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 3.18 seconds

(nejra@Nejra):[~]$
```

Apri Salva : ○○×

```
report2.txt
```

```
1 # Nmap 7.94SVN scan initiated Mon Apr 22 14:16:28 2024 as: nmap -sV -o report2.txt 192.168.240.150
2 # Nmap done at Mon Apr 22 14:16:31 2024 -- 1 IP address (0 hosts up) scanned in 3.18 seconds
```



NMAP SENZA FIREWALL

RISCONTRI

Come si può notare, le porte trovate precedentemente aperte ora non lo sono più, o per lo meno, sono nascoste da eventuali scan da eventuali **attaccanti**

```
└─(nejra㉿Nejra)-[~]
└─$ nmap -sV 192.168.240.150 -o report2.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-22 14:16 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 3.18 seconds
```

CONCLUSIONI FINALI

Il firewall di Windows XP **non** supporta la visualizzazione delle porte aperte direttamente tramite l'interfaccia utente. Di default, **il firewall blocca** tutte le porte in entrata e **apre solo alcune porte** specifiche per alcune applicazioni di rete, ragion per cui il motivo per il quale con NMAP non si vedano le porte con Firewall attivo è che blocca il traffico di rete in base a regole predefinite o personalizzate. Quando una connessione o un pacchetto di rete arriva in un qualsiasi host, il firewall controlla le regole per determinare se dovrebbe essere **consentito o bloccato**.





Van Zwam Arjen

GRAZIE PER
L'ATTENZIONE

Arjen Van Zwam