

ESERCITAZIONE W18D1(1)

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.

3

Scansione di nmap ,(senza firewall) sulla macchina Windows XP

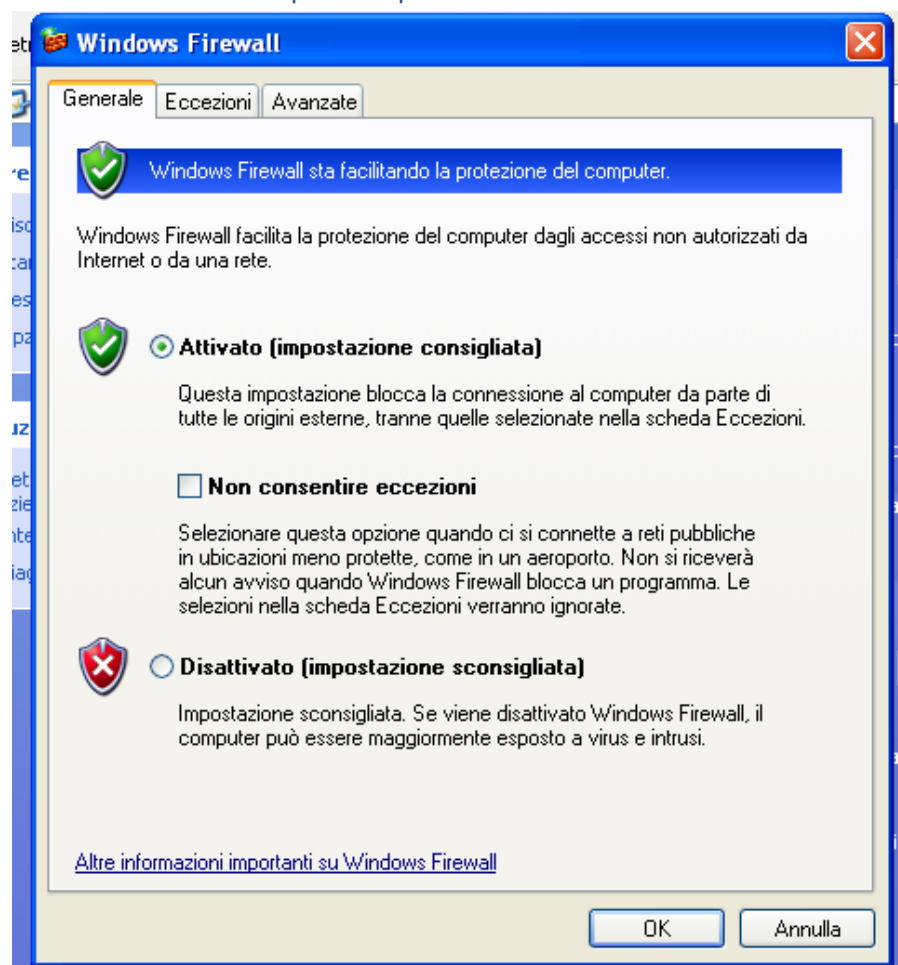
```
(kali㉿kali)-[~]
$ sudo nmap -sV -o nomefilereport 192.168.11.113
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-09 13:25 EDT
Nmap scan report for 192.168.11.113
Host is up (0.00011s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Microsoft Windows XP microsoft-ds
MAC Address: 08:00:27:20:5F:06 (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 20.87 seconds

(kali㉿kali)-[~]
$
```

Dalla scansione possiamo vedere che ci sono 3 servizi in ascolto sulle porte TCP

Attivo il firewall per la prossima scansione



Scansione nmap su Windows XP (con firewall attivo)

```
(kali@kali)-[~]
$ sudo nmap -sV -o nomefilereport2 192.168.11.113
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-09 13:28 EDT
Nmap scan report for 192.168.11.113
Host is up (0.00030s latency).
All 1000 scanned ports on 192.168.11.113 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:20:5F:06 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 38.00 seconds
```

Da questa scansione possiamo vedere che grazie al firewall tutte le porte sono filtrate, quindi bloccandone l'accesso