

## Traccia:

Le azioni preventive mirano a ridurre la possibilità di attacchi provenienti dall'esterno. Abbiamo visto che a livello di rete, possiamo configurare Firewall e regole per fare in modo che un determinato traffico, potenzialmente dannoso, venga bloccato.

La macchina Windows, 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 detection e `-o` nomefilereport per salvare in un file l'output)
3. Abilitare il Firewall sulla macchina Windows
4. Effettuate una seconda scansione con nmap, utilizzando ancora una volta lo switch `-sV`.
5. Trovare le eventuali differenze e motivarle

Eseguiamo il comando "sudo arp-scan -l" per individuare l'indirizzo IP della macchina Windows e facciamo una scansione sulle porte e i servizi attivi salvando il risultato in un file (WindowsScan) in output `-o` così da poter mettere a confronto questa scansione iniziale con quella che faremo dopo aver abilitato il Firewall.

```
C:\home\kali> sudo arp-scan -l
[sudo] password for kali:
Interface: eth0, type: EN10MB, MAC: 08:00:27:1e:36:4a, IPv4: 192.168.11.111
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.11.60 08:00:27:40:42:2c (Unknown)

1 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.586 seconds (98.99 hosts/sec). 1 responded

C:\home\kali> sudo nmap -sV -o WindowsScan 192.168.11.60
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-05 12:34 EST
Nmap scan report for 192.168.11.60
Host is up (0.0086s latency).
Not shown: 982 closed tcp ports (reset)
PORT      STATE SERVICE
7/tcp     open  echo
9/tcp     open  discard?
13/tcp    open  daytime      Microsoft Windows International daytime
17/tcp    open  qotd         Windows qotd (English)
19/tcp    open  chargen
80/tcp    open  http         Microsoft IIS httpd 10.0
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
1801/tcp  open  mssql?       Microsoft Windows RPC
2103/tcp  open  msrpc        Microsoft Windows RPC
2105/tcp  open  msrpc        Microsoft Windows RPC
2107/tcp  open  msrpc        Microsoft Windows RPC
3389/tcp  open  ssl/ms-wbt-server?
5432/tcp  open  postgresql?
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8080/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
8443/tcp  open  ssl/https-alt
MAC Address: 08:00:27:40:42:2C (Oracle VirtualBox virtual NIC)
Service Info: Host: DESKTOP-9K104BT; OS: Windows; CPE: cpe:/o:microsoft:windows

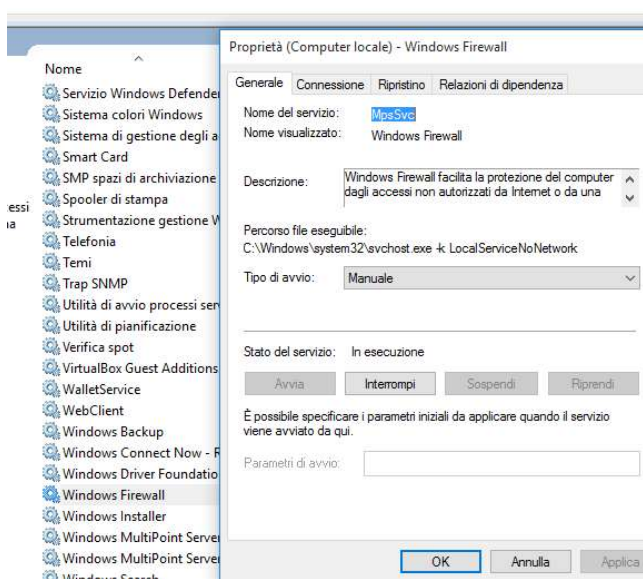
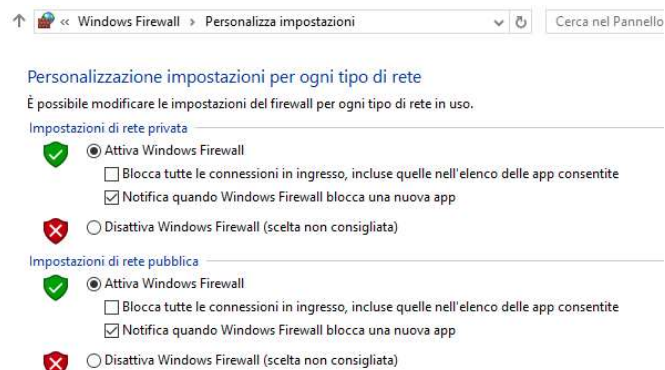
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 184.36 seconds
```

Abilitiamo il firewall seguendo i seguenti passaggi

Attivazione Windows Firewall:

- Andare in Servizi
- Cercare il servizio Windows Firewall
- Impostare il tipo di avvio in Manuale
- Applica

- Avvia
- Abilitare il firewall da Pannello di controllo\Tutti gli elementi del Pannello di controllo\Windows Firewall\Personalizza impostazioni.



Ora che abbiamo abilitato il firewall possiamo procedere con la scansione.

Come possiamo vedere la scansione ci mostra meno porte rispetto a prima inoltre le porte mostrate sembrano essere filtrate, non avendo dato risposta alle richieste dello scanner. Il Firewall che abbiamo abilitato quindi sta bloccando l'accesso alle porte.

```
C:\home\kali> sudo nmap -sV -o WindowsScan2 192.168.11.60
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-05 12:55 EST
Nmap scan report for 192.168.11.60
Host is up (0.0045s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT      STATE SERVICE        VERSION
80/tcp    open  http           Microsoft IIS httpd 10.0
135/tcp   open  msrpc          Microsoft Windows RPC
1801/tcp  open  msmq?         Microsoft Windows RPC
2103/tcp  open  msrpc          Microsoft Windows RPC
2105/tcp  open  msrpc          Microsoft Windows RPC
2107/tcp  open  msrpc          Microsoft Windows RPC
3443/tcp  open  ssl/https-alt
MAC Address: 08:00:27:40:42:2C (Oracle VirtualBox virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 108.81 seconds
```