CPTP0524 – W18D1

Security Operation: Azioni Preventive

Traccia:
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)

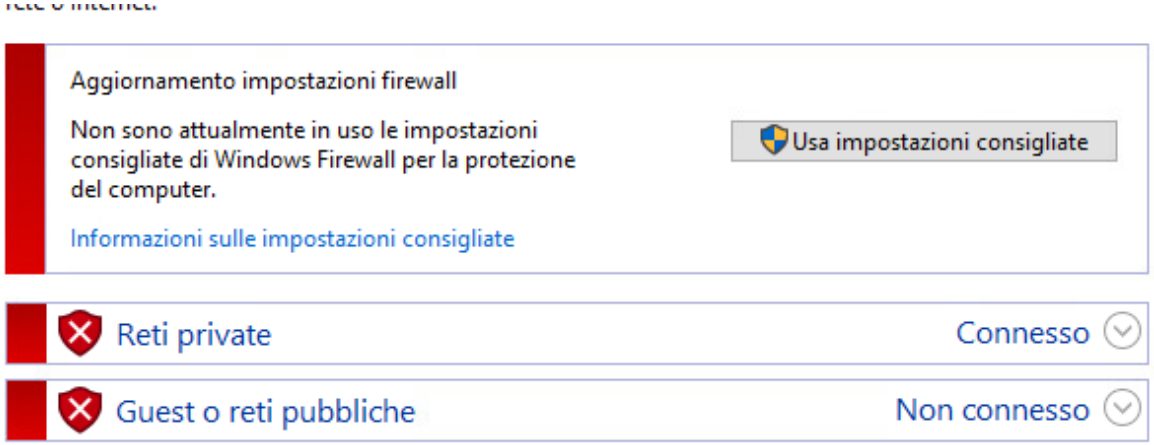
3. Abilitare il Firewall sulla macchina Windows

4. Effettuate una seconda scansione con nmap, utilizzando ancora una volta lo switch –sV.

5. Trovare le eventuali differenze e motivarle.

SVOLGIMENTO

1. Assicuratevi che il Firewall sia disattivato sulla macchina Windows



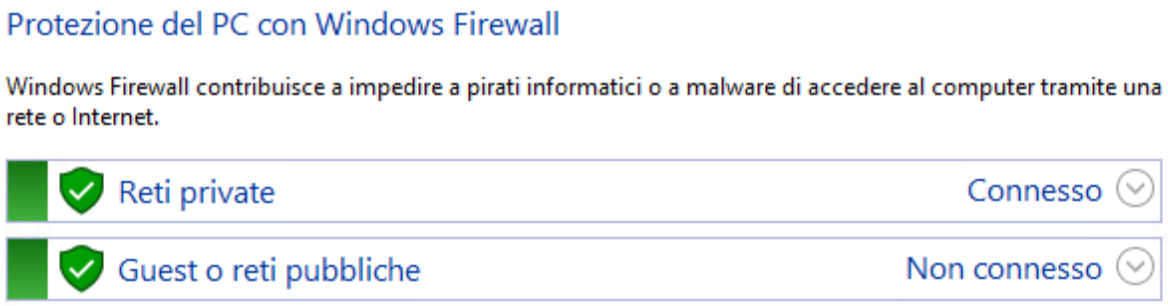
2. Effettuate una scansione con nmap sulla macchina target (utilizzate lo switch –sV, per la service detection e -o nomefilereport per salvare in un file l'output)

```
❯ nmap -sV -vvv 192.168.50.102 -o nofirewall
```

```
Nmap scan report for epi-win10.epicode (192.168.50.102)
Host is up, received arp-response (0.000099s latency).
Scanned at 2025-03-17 21:28:59 CET for 159s
Not shown: 981 closed tcp ports (reset)
PORT     STATE SERVICE       REASON          VERSION
7/tcp    open  echo          syn-ack ttl 128
9/tcp    open  discard?      syn-ack ttl 128
13/tcp   open  daytime       syn-ack ttl 128 Microsoft Windows International daytime
17/tcp   open  qotd          syn-ack ttl 128 Windows qotd (English)
19/tcp   open  chargen       syn-ack ttl 128
80/tcp   open  http          syn-ack ttl 128 Microsoft IIS httpd 10.0
135/tcp  open  msrpc         syn-ack ttl 128 Microsoft Windows RPC
139/tcp  open  netbios-ssn   syn-ack ttl 128 Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds  syn-ack ttl 128 Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
1801/tcp open  msmq?         syn-ack ttl 128
2103/tcp open  msrpc         syn-ack ttl 128 Microsoft Windows RPC
2105/tcp open  msrpc         syn-ack ttl 128 Microsoft Windows RPC
2107/tcp open  msrpc         syn-ack ttl 128 Microsoft Windows RPC
3389/tcp open  ms-wbt-server syn-ack ttl 128 Microsoft Terminal Services
5357/tcp open  http          syn-ack ttl 128 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5432/tcp open  postgresql?   syn-ack ttl 128
8009/tcp open  ajp13         syn-ack ttl 128 Apache Jserv (Protocol v1.3)
8080/tcp open  http          syn-ack ttl 128 Apache Tomcat/Coyote JSP engine 1.1
8443/tcp open  ssl/https-alt syn-ack ttl 128
MAC Address: 00:0C:29:32:E2:74 (VMware)
Service Info: Host: DESKTOP-9K1O4BT; OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 158.93 seconds
           Raw packets sent: 1066 (46.888KB) | Rcvd: 1001 (40.104KB)
```

3. Abilitare il Firewall sulla macchina Windows



4. Effettuate una seconda scansione con nmap, utilizzando ancora una volta lo switch –sV.

```
❯ nmap -sV -vvv 192.168.50.102 -o firewall
```

```
Nmap scan report for epi-win10.epicode (192.168.50.102)
Host is up, received arp-response (0.00022s latency).
Scanned at 2025-03-17 21:33:50 CET for 81s
Not shown: 989 filtered tcp ports (no-response)
PORT     STATE SERVICE       REASON          VERSION
80/tcp   open  http          syn-ack ttl 128 Microsoft IIS httpd 10.0
135/tcp  open  msrpc         syn-ack ttl 128 Microsoft Windows RPC
139/tcp  open  netbios-ssn   syn-ack ttl 128 Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds  syn-ack ttl 128 Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
1801/tcp open  msmq?         syn-ack ttl 128
2103/tcp open  msrpc         syn-ack ttl 128 Microsoft Windows RPC
2105/tcp open  msrpc         syn-ack ttl 128 Microsoft Windows RPC
2107/tcp open  msrpc         syn-ack ttl 128 Microsoft Windows RPC
3389/tcp open  ms-wbt-server syn-ack ttl 128 Microsoft Terminal Services
5357/tcp open  http          syn-ack ttl 128 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
8443/tcp open  ssl/https-alt syn-ack ttl 128
MAC Address: 00:0C:29:32:E2:74 (VMware)
Service Info: Host: DESKTOP-9K1O4BT; OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 81.20 seconds
           Raw packets sent: 1990 (87.544KB) | Rcvd: 12 (512B)
```

5. Trovare le eventuali differenze e motivarle.

Si può notare che i tempi di scansione variano, per esempio la scansione con firewall dura meno tempo ma mostra meno risultati in quantità di porte, a differenza della scansione senza firewalle che impiega piu tempo e trova più servizi.

Francesco Rinaldi