Analisi Windows Firewall tramite scansioni Nmap

1. Obiettivo dell'esercizio

L'obiettivo dell'esercizio è analizzare l'impatto del **Windows Firewall** sulla superficie di attacco di un sistema Windows, confrontando i risultati di due scansioni **Nmap con service detection (-sV)**:

- una con firewall **disattivato**
- una con firewall **attivato**

---

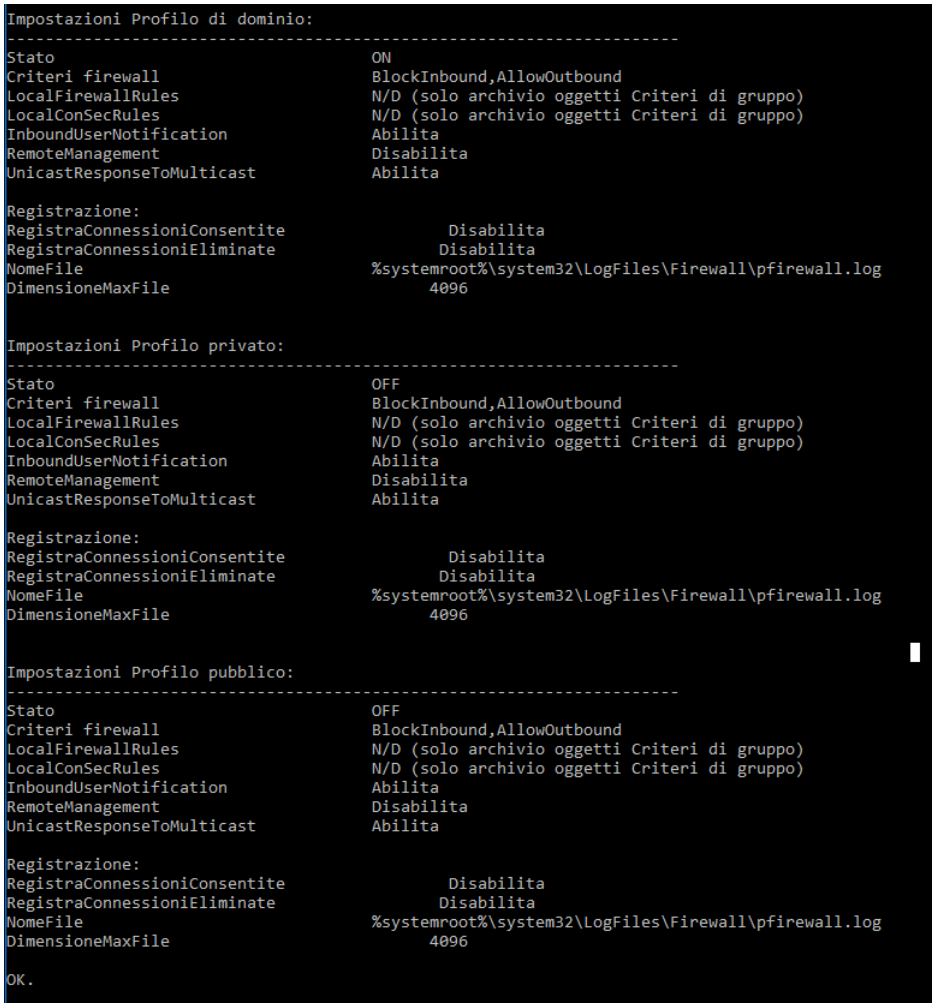
2. Ambiente di test

- **Attacker**: Kali Linux
- **Target**: Windows (in esecuzione su VirtualBox)
- **IP target**: 192.168.50.102
- **Tool utilizzato**: Nmap 7.95
- **Opzione Nmap**: -sV (service version detection)

---

3. Verifica stato iniziale del Windows Firewall

Prima di eseguire la scansione, è stato verificato lo stato del firewall tramite comando netsh.



Dall'output risulta che:

- Profilo **Privato**: OFF
- Profilo **Pubblico**: OFF

Il sistema risultava quindi esposto alle connessioni in ingresso.

---

4. Scansione Nmap con Windows Firewall disattivato

Con il firewall disattivato è stata eseguita la seguente scansione:

sudo nmap -sV -oN scan_fw_off.txt 192.168.50.102

```
┌──(pireddone㉿kali)-[~]
└─$ sudo nmap -sV -oN scan_fw_off.txt 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-04 14:25 CET
Nmap scan report for 192.168.50.102
Host is up (0.00040s latency).
Not shown: 982 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
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  msmq?
2103/tcp open  msrpc         Microsoft Windows RPC
2105/tcp open  msrpc         Microsoft Windows RPC
2107/tcp open  msrpc         Microsoft Windows RPC
3389/tcp open  ms-wbt-server Microsoft Terminal Services
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: 08:00:27:34:48:36 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: DESKTOP-9K1O4BT; 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 170.93 seconds
```

Risultato

La scansione ha evidenziato numerose porte **open**, tra cui:

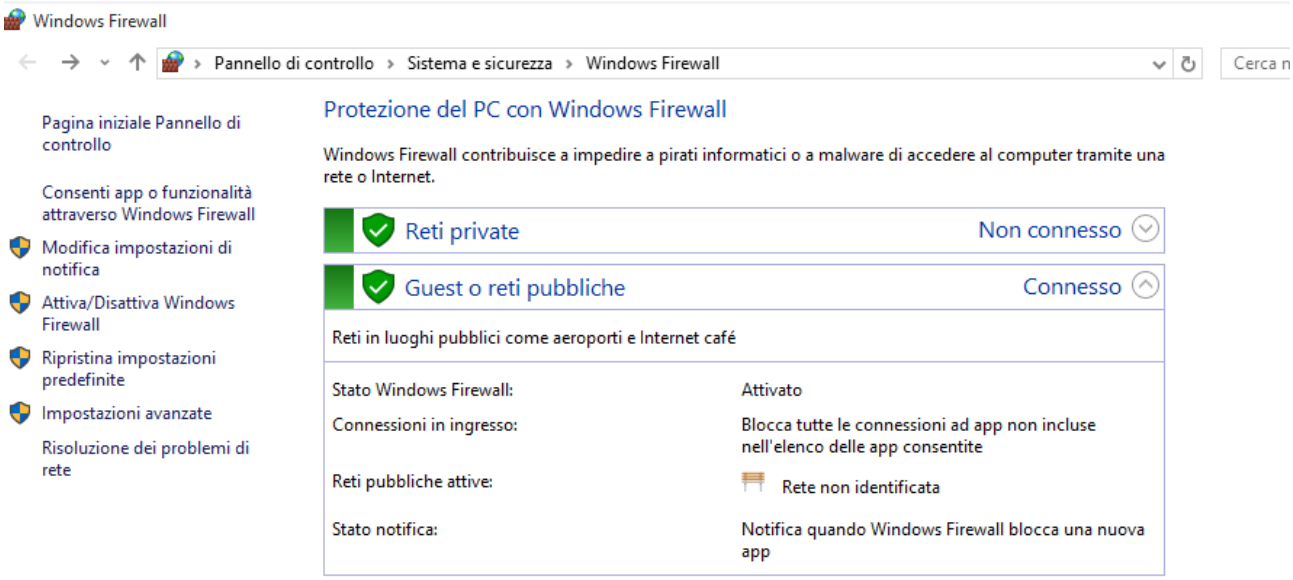
- 80/tcp – HTTP (Microsoft IIS 10.0)
- 135/tcp – MSRPC
- 139/tcp – NetBIOS
- 445/tcp – SMB
- 3389/tcp – RDP
- 8080/tcp – Apache Tomcat
- 8443/tcp – HTTPS

Grazie all'opzione -sV, Nmap è riuscito a identificare correttamente i servizi e le versioni in esecuzione.

---

5. Attivazione del Windows Firewall

Successivamente è stato attivato il Windows Firewall tramite interfaccia grafica, abilitandolo per il profilo di rete pubblico e bloccando le connessioni in ingresso non autorizzate.



---

6. Scansione Nmap con Windows Firewall attivo

Dopo l'attivazione del firewall, è stata ripetuta la scansione Nmap con le stesse opzioni:

sudo nmap -sV -oN scan_fw_on.txt 192.168.50.102

```
┌──(pireddone㉿kali)-[~]
└─$ sudo nmap -sV -oN scan_fw_on.txt 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-04 14:33 CET
Nmap scan report for 192.168.50.102
Host is up (0.00083s latency).
Not shown: 992 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?
2103/tcp open  msrpc         Microsoft Windows RPC
2105/tcp open  msrpc         Microsoft Windows RPC
2107/tcp open  msrpc         Microsoft Windows RPC
3389/tcp open  ms-wbt-server Microsoft Terminal Services
8443/tcp open  ssl/https-alt
MAC Address: 08:00:27:34:48:36 (PCS Systemtechnik/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 92.65 seconds
```

Risultato

In questo scenario:

- **992 porte TCP risultano filtered**
- solo poche porte risultano ancora accessibili
- la capacità di Nmap di identificare servizi e versioni è fortemente ridotta

La presenza di porte “filtered” indica che il firewall sta bloccando o ignorando le richieste in ingresso.

---

7. Confronto e analisi dei risultati

Il confronto tra le due scansioni mostra chiaramente l’efficacia del Windows Firewall nel ridurre la superficie di attacco del sistema.

- Con firewall **disattivato**:
    - ampia esposizione dei servizi
    - elevata capacità di enumerazione da parte di Nmap
- Con firewall **attivato**:
    - traffico in ingresso filtrato
    - drastica riduzione delle informazioni disponibili a un potenziale attaccante

---

8. Conclusione

L’esercizio dimostra come l’attivazione del Windows Firewall influisca direttamente sulla visibilità dei servizi di rete. Il firewall rappresenta una misura di sicurezza fondamentale per limitare l’esposizione del sistema e ridurre le possibilità di enumerazione e attacco da parte di un attore malevolo.