

## M4,W2,D1

L'attività mira a verificare sperimentalmente l'efficacia delle azioni preventive di sicurezza, analizzando come l'attivazione del Firewall modifichi la visibilità dei servizi di rete dall'esterno. Lo scopo è confrontare i risultati di due scansioni per comprendere la riduzione del rischio ottenuta filtrando il traffico in ingresso

### 1. NMAP CON FIREWALL ATTIVATO

The screenshot shows the Windows Firewall settings window. It has two main sections: 'Impostazioni di rete privata' and 'Impostazioni di rete pubblica'. Both sections have the 'Attiva Windows Firewall' radio button selected. Under 'Reti private', there are three checkboxes: 'Blocca tutte le connessioni in ingresso, incluse quelle nell'elenco delle app consentite' (unchecked), 'Notifica quando Windows Firewall blocca una nuova app' (checked), and 'Disattiva Windows Firewall (scelta non consigliata)' (unchecked). Under 'Reti pubbliche', similar options are present. On the right side, there's a summary section titled 'Protezione del PC con Windows Firewall' which shows 'Windows Firewall contribuisce a impedire a pirati informatici o a malware di accedere al computer tramite una rete o Internet'. It lists 'Reti private' as 'Non connesso' and 'Guest o reti pubbliche' as 'Connesso'. Below this, it details the state of the firewall ('Attivato'), incoming connections ('Blocca tutte le connessioni ad app non incluse nell'elenco delle app consentite'), active public networks ('Rete non identificata', 'Rete 7'), and notification settings ('Notifica quando Windows Firewall blocca una nuova app').

```
(kali㉿kali)-[~]
$ nmap -sV -oN report_firewall_on.txt 192.168.56.106
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-09 06:51 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Stats: 0:00:52 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 28.57% done; ETC: 06:54 (0:01:50 remaining)
Nmap scan report for 192.168.56.106
Host is up (0.00047s 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?
2103/tcp  open  msrpc       Microsoft Windows RPC
2105/tcp  open  msrpc       Microsoft Windows RPC
2107/tcp  open  msrpc       Microsoft Windows RPC
8443/tcp  open  ssl/https-alt
MAC Address: 08:00:27:19:B6:C8 (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 85.44 seconds
```

Con il firewall attivo, la scansione rivela un sistema parzialmente blindato ma con alcune eccezioni significative. Nmap riporta che ben 993 porte sono in stato "filtered", confermando che il firewall sta bloccando silenziosamente la maggior parte del traffico. Tuttavia, oltre al classico server web Microsoft IIS sulla porta 80 e ai servizi RPC sulla porta 135, emergono altre porte aperte inaspettate. È visibile la porta 1801 (msmq), legata al Microsoft Message Queuing, e diverse porte dinamiche per RPC come la 2103, 2105 e 2107. Un dettaglio cruciale è la presenza della porta 8443 aperta, che indica un servizio SSL/HTTPS alternativo in ascolto. Questo dimostra che, nonostante il firewall, diversi canali di comunicazione rimangono esposti e potenzialmente sfruttabili se non necessari.

## 2. NMAP CON FIREWALL DISATTIVATO

The screenshot shows the Windows Firewall settings. Under 'Impostazioni di rete privata', 'Attiva Windows Firewall' is selected. Under 'Impostazioni di rete pubblica', 'Disattiva Windows Firewall (scelta non consigliata)' is selected. On the right, the 'Protezione del PC con Windows Firewall' section shows that both 'Reti private' and 'Guest o reti pubbliche' are set to 'Non connesso'. A note states that Windows Firewall is not currently active.

```
(kali㉿kali)-[~]
$ nmap -sV -oN report_firewall_off.txt 192.168.56.106

Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-09 07:08 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.106
Host is up (0.0018s 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
up: 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: 08:00:27:19:B6:C8 (PCS Systemtechnik/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 161.40 seconds
```

Senza il firewall, la superficie d'attacco espone una vasta gamma di servizi che trasformano la macchina in un bersaglio facile. Le porte precedentemente filtrate appaiono ora come "closed" (982 porte), indicando che il sistema risponde attivamente a qualsiasi stimolo esterno. È particolarmente critica la presenza di servizi ormai obsoleti come echo (7), discard (9), daytime (13), qotd (17) e chargen (19), spesso abusati dagli attaccanti. Ancor più rischiosa è l'esposizione diretta dei servizi di condivisione Windows, ovvero NetBIOS (139) e SMB (445), che rappresentano storicamente i vettori principali per la diffusione di ransomware e permettono l'enumerazione di utenti e cartelle. A peggiorare il quadro contribuisce la porta 3389 (Remote Desktop), che invita a tentativi di brute-force sulla password per ottenere il controllo remoto totale del sistema, mentre l'accesso libero al database PostgreSQL (5432) e al server Apache Tomcat (porte 8080 e 8009) espone l'ambiente a furti di dati e vulnerabilità web specifiche, offrendo diverse strade per un'intrusione completa.

### 3. CONCLUSIONE

```
(kali㉿kali)-[~]
$ ls
ciao.py          hydra.restore      Public
Desktop          Music              report_firewall_off.txt
Documents        my_shell.php     report_firewall_on.txt
dos              nano.5662.save   shell.php
Downloads        nano.8461.save   Socket_test
FdeKwdHV.jpeg    Net-DNS-1.53   Templates
gameshell        Net-DNS-1.53.tar.gz uff.py
gameshell.1      password_db.txt users.txt.bk
gameshell-save.sh Pictures          utenti.txt
gameshell.sh     Prova             Videos
hash_dvwa.txt    prova.py         windows

(kali㉿kali)-[~]
$ cat report_firewall_off.txt
# Nmap 7.95 scan initiated Mon Feb  9 07:08:56 2026 as: /usr/lib/nmap/nmap
--privileged -sV -oN report_firewall_off.txt 192.168.56.106
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disa
```

L'esercizio si conclude con la verifica del salvataggio dei dati: come evidenziato nell'ultimo screenshot, il comando ls mostra la presenza dei file di output report\_firewall\_off.txt e report\_firewall\_on.txt nella directory di lavoro , mentre l'ispezione con cat conferma che l'intera scansione è stata registrata correttamente. Dal confronto dei report emerge un cambiamento radicale della sicurezza: si passa da un sistema "silenzioso" con 993 porte filtrate che ignorano le connessioni a un host completamente esposto che risponde attivamente su tutte le porte (982 porte closed). Senza il filtro del firewall, servizi critici come SMB, RDP e database, prima nascosti o protetti, diventano immediatamente accessibili, dimostrando empiricamente come l'attivazione del firewall sia determinante per ridurre la superficie d'attacco.