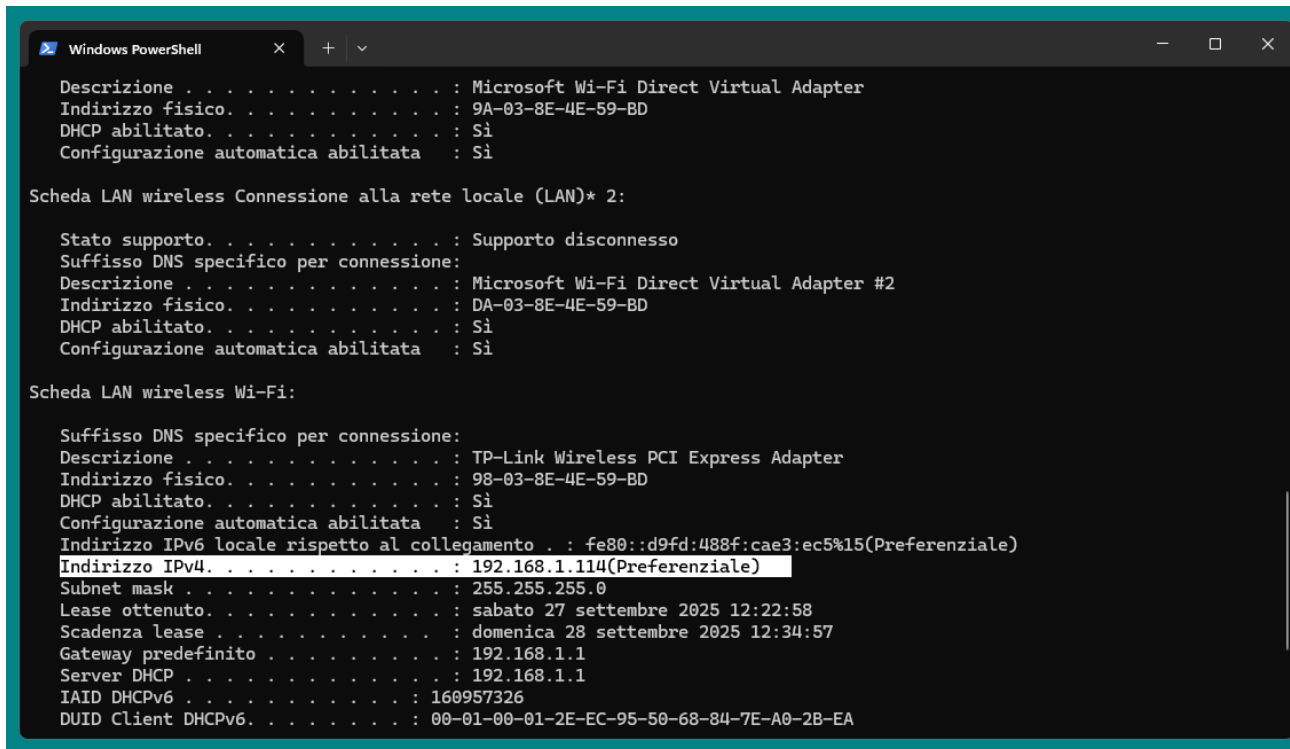


Intro

Ho innanzitutto verificato il mio ip di Windows



```
Windows PowerShell
Descrizione . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
Indirizzo fisico. . . . . : 9A-03-8E-4E-59-BD
DHCP abilitato. . . . . : Sì
Configurazione automatica abilitata : Sì

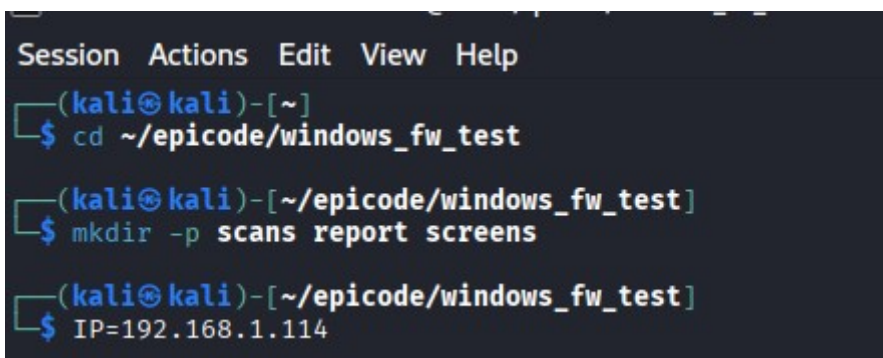
Scheda LAN wireless Connessione alla rete locale (LAN)* 2:

Stato supporto. . . . . : Supporto disconnesso
Suffisso DNS specifico per connessione:
Descrizione . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
Indirizzo fisico. . . . . : DA-03-8E-4E-59-BD
DHCP abilitato. . . . . : Sì
Configurazione automatica abilitata : Sì

Scheda LAN wireless Wi-Fi:

Suffisso DNS specifico per connessione:
Descrizione . . . . . : TP-Link Wireless PCI Express Adapter
Indirizzo fisico. . . . . : 98-03-8E-4E-59-BD
DHCP abilitato. . . . . : Sì
Configurazione automatica abilitata : Sì
Indirizzo IPv6 locale rispetto al collegamento . : fe80::d9fd:488f:cae3:ec5%15(Preferenziale)
Indirizzo IPv4. . . . . : 192.168.1.114(Preferenziale)
Subnet mask . . . . . : 255.255.255.0
Lease ottenuto. . . . . : sabato 27 settembre 2025 12:22:58
Scadenza lease . . . . . : domenica 28 settembre 2025 12:34:57
Gateway predefinito . . . . . : 192.168.1.1
Server DHCP . . . . . : 192.168.1.1
IAID DHCPv6 . . . . . : 160957326
DUID Client DHCPv6. . . . . : 00-01-00-01-2E-EC-95-50-68-84-7E-A0-2B-EA
```

Ho poi impostato una cartella in modo da eseguire il tutto da lì



```
Session Actions Edit View Help
(kali@kali)-[~]
$ cd ~/epicode/windows_fw_test

(kali@kali)-[~/epicode/windows_fw_test]
$ mkdir -p scans report screens

(kali@kali)-[~/epicode/windows_fw_test]
$ IP=192.168.1.114
```

Ero pienamente consapevole che il ping avrebbe potuto fallire, quindi ho deciso di verificare con ARP che fosse effettivamente raggiungibile. Nonostante non risponda ai ping, comportamento tipico con il firewall attivo, tramite ARP scan si è confermata la presenza dell'host nella LAN

```
kali@kali: ~/epicode/windows_fw_test
Session Actions Edit View Help
PING 192.168.1.114 (192.168.1.114) 56(84) bytes of data.
— 192.168.1.114 ping statistics —
3 packets transmitted, 0 received, 100% packet loss, time 2240ms

(kali@kali)-[~/epicode/windows_fw_test]
$ sudo nmap -sn 192.168.1.0/24 -PR -oN scans/01_arp.txt
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-27 19:31 EDT
Stats: 0:00:01 elapsed; 0 hosts completed (0 up), 255 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 50.59% done; ETC: 19:31 (0:00:01 remaining)
Nmap scan report for 192.168.1.1
Host is up (0.0026s latency).
MAC Address: 28:3B:82:32:E3:E9 (D-Link International)
Nmap scan report for OPPO-A5-2020 (192.168.1.100)
Host is up (0.10s latency).
MAC Address: AA:35:81:89:E3:38 (Unknown)
Nmap scan report for FramaPC (192.168.1.114)
Host is up (0.00042s latency).
MAC Address: 98:03:8E:4E:59:BD (Unknown)
Nmap scan report for kali (192.168.1.126)
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.40 seconds

(kali@kali)-[~/epicode/windows_fw_test]
$
```

Ora che abbiamo verificato l'host, il prossimo passo è fare le scansioni con Firewall ON .

OS FINGERPRINT (FIREWALL ON)

```
(kali㉿kali)-[~/epicode/windows_fw_test]
$ sudo nmap -O -oN scans/02_os_fw_on.nmap $IP
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-27 19:35 EDT
Nmap scan report for Framapc (192.168.1.114)
Host is up (0.00077s latency).
All 1000 scanned ports on Framapc (192.168.1.114) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 98:03:8E:4E:59:BD (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

L'host è stato rilevato come attivo, ma tutte le 1000 porte TCP risultano filtrate. Questo comportamento è coerente con il firewall di Windows che blocca le connessioni in ingresso. A causa della mancanza di risposte utili, Nmap non è stato in grado di identificare il sistema operativo.

SYN SCAN (FIREWALL ON)

```
(kali㉿kali)-[~/epicode/windows_fw_test]
$ sudo nmap -sS -p- -T4 -sV -oN scans/03_syn_fw_on.nmap $IP

Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-27 19:38 EDT
Nmap scan report for Framapc (192.168.1.114)
Host is up (0.00092s latency).
Not shown: 65534 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
7680/tcp  open  pando-pub?
MAC Address: 98:03:8E:4E:59:BD (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 173.80 seconds
```

Come visibile dall'immagine, il firewall filtra la quasi totalità delle connessioni, consentendo l'accesso solo a pochissimi servizi.

TCP CONNECT SCAN (FIREWALL ON)

```
(kali㉿kali)-[~/epicode/windows_fw_test]
$ nmap -sT -p- -T3 -sV -oN scans/04_tcp_fw_on.nmap $IP

Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-27 19:44 EDT
Nmap scan report for Framapc (192.168.1.114)
Host is up (0.0024s latency).
Not shown: 65534 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
7680/tcp  open  pando-pub?
MAC Address: 98:03:8E:4E:59:BD (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 161.93 seconds

(kali㉿kali)-[~/epicode/windows_fw_test]
$
```

Come si può vedere, il risultato è pressappoco identico a quello precedente: entrambe individuano una sola porta accessibile.

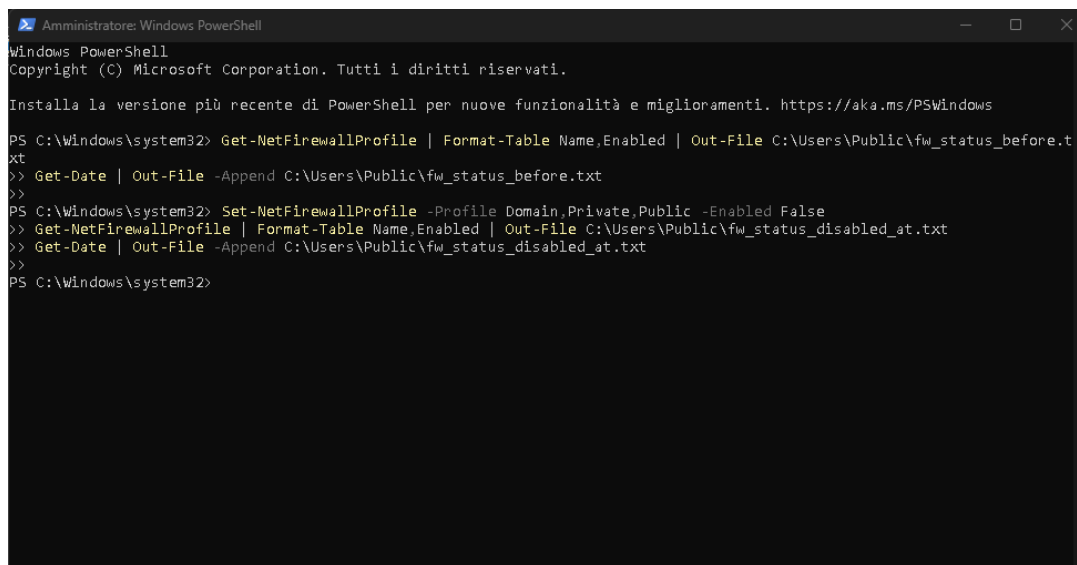
CONSIDERAZIONI FINALI:

OS fingerprint = fallito, tutto filtrato.

SYN = 1 porta aperta (7680/tcp).

TCP connect = conferma stessa porta aperta.

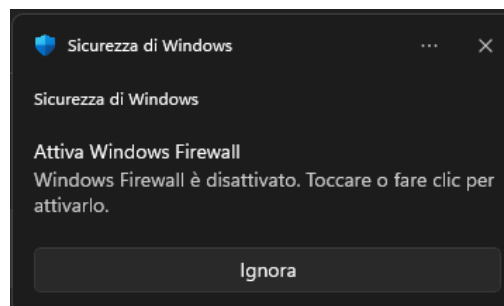
Prima di procedere ai medesimi comandi, ho disattivato i Firewall tramite la Shell Windows (eseguita come amministratore) e mi sono assicurato della riuscita dell'operazione.



```
Amministratore: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. Tutti i diritti riservati.

Installa la versione piú recente di PowerShell per nuove funzionalità e miglioramenti. https://aka.ms/PSWindows

PS C:\Windows\system32> Get-NetFirewallProfile | Format-Table Name,Enabled | Out-File C:\Users\Public\fw_status_before.txt
>> Get-Date | Out-File -Append C:\Users\Public\fw_status_before.txt
>>
PS C:\Windows\system32> Set-NetFirewallProfile -Profile Domain,Private,Public -Enabled False
>> Get-NetFirewallProfile | Format-Table Name,Enabled | Out-File C:\Users\Public\fw_status_disabled_at.txt
>> Get-Date | Out-File -Append C:\Users\Public\fw_status_disabled_at.txt
>>
PS C:\Windows\system32>
```



OS FINGERPRINT (FIREWALL OFF)

```
(kali㉿kali)-[~/epicode/windows_fw_test]
└─$ sudo nmap -O -oN scans/02_os_fw_off.nmap $IP

[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-27 19:59 EDT
Nmap scan report for Framapc (192.168.1.114)
Host is up (0.0012s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 98:03:8E:4E:59:BD (Unknown)
Aggressive OS guesses: Microsoft Windows 10 1703 or Windows 11 21H2 (99%), Microsoft Windows 11 21H2 (98%), Microsoft Windows 10 1703 (97%), Microsoft Windows 10 1507 - 1607 (97%), Microsoft Windows Server 2022 (96%), Microsoft Windows 10 1511 (95%), Microsoft Windows 10 (94%), Microsoft Windows Longhorn (94%), Microsoft Windows 10 1511 - 1607 (94%), Microsoft Windows Vista SP2 or Windows 7 or Windows Server 2008 R2 or Windows 8.1 (94%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.44 seconds

(kali㉿kali)-[~/epicode/windows_fw_test]
```

Ecco la prova di come il firewall spento cambi tutto: Nmap ha potuto eseguire fingerprinting OS molto più accurato, indicando come possibili sistemi Windows 10 (varie build), Windows 11 o Windows Server 2022, con alte probabilità di affidabilità.

SYN SCAN (FIREWALL OFF)

```
(kali㉿kali)-[~/epicode/windows_fw_test]
└─$ sudo nmap -sS -p- -T4 -sV -oN scans/03_syn_fw_off.nmap $IP
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-27 20:02 EDT
Nmap scan report for Framapc (192.168.1.114)
Host is up (0.00022s latency).
Not shown: 65524 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?
5040/tcp   open  unknown
7680/tcp   open  pando-pub?
49664/tcp  open  msrpc            Microsoft Windows RPC
49665/tcp  open  msrpc            Microsoft Windows RPC
49666/tcp  open  msrpc            Microsoft Windows RPC
49667/tcp  open  msrpc            Microsoft Windows RPC
49668/tcp  open  msrpc            Microsoft Windows RPC
49687/tcp  open  msrpc            Microsoft Windows RPC
MAC Address: 98:03:8E:4E:59:BD (Unknown)
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 113.75 seconds

(kali㉿kali)-[~/epicode/windows_fw_test]
└─$
```

Anche qui c'è la dimostrazione che il firewall di Windows blocca la maggior parte del traffico in entrata, impedendo la rilevazione di servizi. Con il firewall disabilitato, Nmap è in grado di identificare numerosi servizi Microsoft, in particolare RPC e SMB.

TCP CONNECT SCAN (FIREWALL OFF)

```
(kali@kali)-[~/epicode/windows_fw_test]
$ nmap -sT -p- -T3 -sV -oN scans/04_tcp_fw_off.nmap $IP

Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-27 20:06 EDT
Nmap scan report for Framapc (192.168.1.114)
Host is up (0.0017s latency).
Not shown: 65524 closed tcp ports (conn-refused)
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?
5040/tcp   open  unknown
7680/tcp   open  pando-pub?
49664/tcp  open  msrpc          Microsoft Windows RPC
49665/tcp  open  msrpc          Microsoft Windows RPC
49666/tcp  open  msrpc          Microsoft Windows RPC
49667/tcp  open  msrpc          Microsoft Windows RPC
49668/tcp  open  msrpc          Microsoft Windows RPC
49687/tcp  open  msrpc          Microsoft Windows RPC
MAC Address: 98:03:8E:4E:59:BD (Unknown)
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 118.27 seconds

(kali@kali)-[~/epicode/windows_fw_test]
$
```

Anche qui possiamo dire che con firewall attivo, quasi tutte le porte risultavano filtrate (solo la 7680 era rilevabile). Con firewall disattivo, compaiono i servizi core di Windows (RPC, SMB, NetBIOS) e diverse porte dinamiche associate a Microsoft RPC.