

SCANNER NMAP FIREWALL SPENTO/ACCESO W11D4 BRUNI GABRIELE

## Protezione del PC con Windows Firewall

Windows Firewall contribuisce a impedire a pirati informatici o a malware di accedere al computer tramite una rete o Internet.

Aggiornamento impostazioni firewall

Non sono attualmente in uso le impostazioni consigliate di Windows Firewall per la protezione del computer.

[Informazioni sulle impostazioni consigliate](#)

Usa impostazioni consigliate


Reti private

Non connesso

Guest o reti pubbliche

Connesso

Reti in luoghi pubblici come aeroporti e Internet café

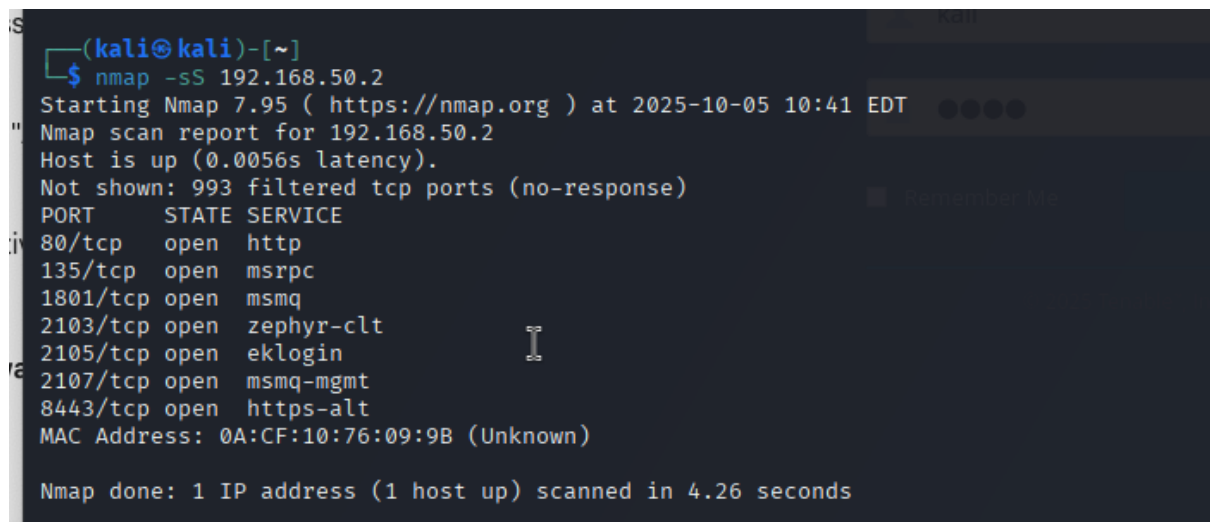
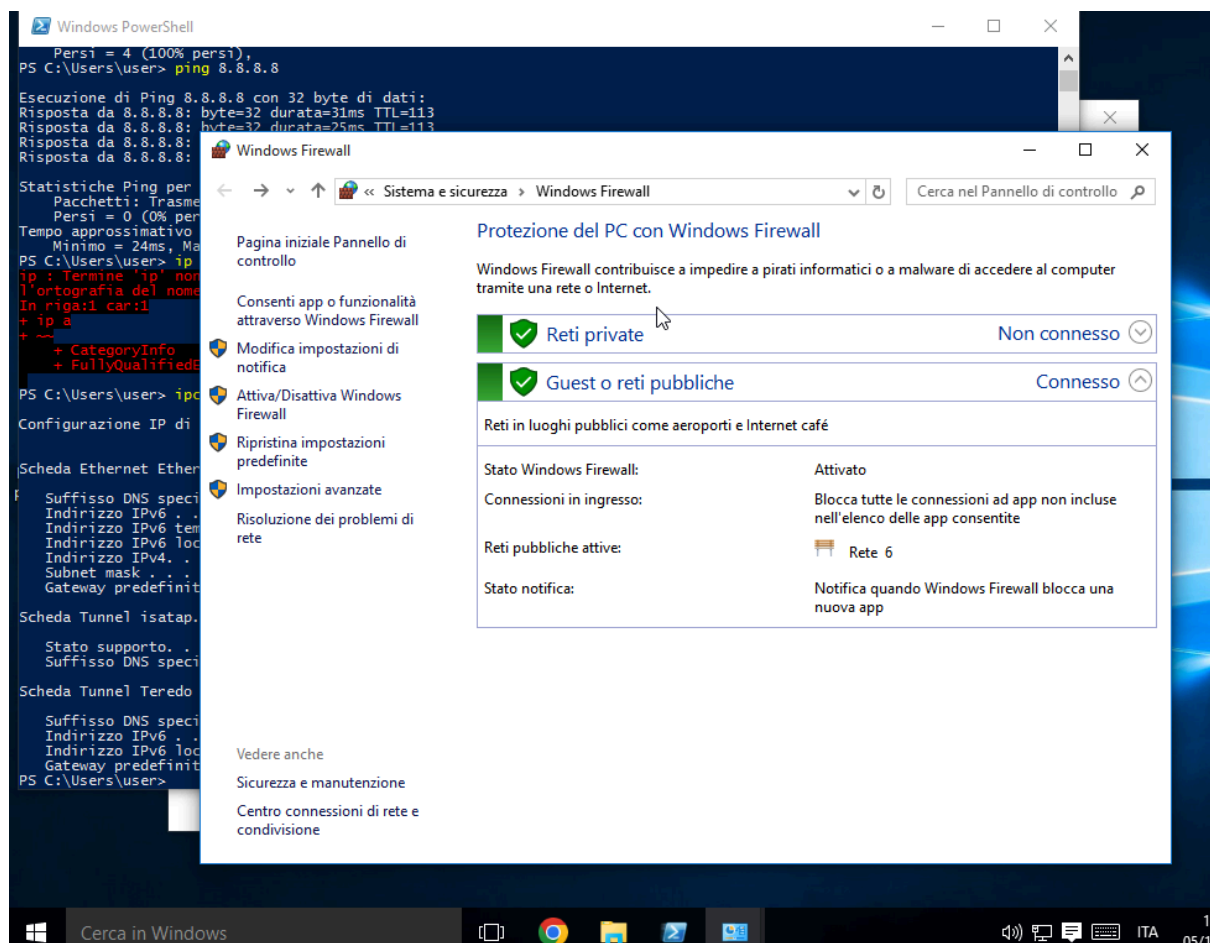
Stato Windows Firewall:	Disattivato
Connessioni in ingresso:	Blocca tutte le connessioni ad app non incluse nell'elenco delle app consentite
Reti pubbliche attive:	 Rete 6
Stato notifica:	Notifica quando Windows Firewall blocca una nuova app

```
(kali㉿kali)-[~]
$ nmap -sS 192.168.50.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-05 10:37 EDT
Nmap scan report for 192.168.50.2
Host is up (0.0012s latency).
Not shown: 982 closed tcp ports (reset)
PORT      STATE SERVICE
7/tcp     open  echo
9/tcp     open  discard
13/tcp    open  daytime
17/tcp    open  qotd
19/tcp    open  chargen
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1801/tcp  open  msmq
2103/tcp  open  zephyr-clt
2105/tcp  open  eklogin
2107/tcp  open  msmq-mgmt
3389/tcp  open  ms-wbt-server
5432/tcp  open  postgresql
8009/tcp  open  ajp13
8080/tcp  open  http-proxy
8443/tcp  open  https-alt
MAC Address: 0A:CF:10:76:09:9B (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.30 seconds

(kali㉿kali)-[~]
$
```

FIREWALL ACCESO



## Analisi dei Problemi e Differenze Concettuali (Nmap vs. Firewall)

L'analisi comparativa dei due screenshot (Firewall OFF e Firewall ON/Ripristinato) evidenzia un problema tecnico nella configurazione del target Windows, ma permette comunque di **evidenziare chiaramente la differenza teorica** che Nmap cerca.

## Fallimento del Blocco del Traffico

Il problema principale rilevato è l'**assenza di filtraggio** (*filtering*) da parte del Windows Firewall.

- **Il Dato Reale:** In tutte le scansioni SYN (-sS), le porte critiche (come 80, 445 e 3389) sono rimaste nello stato **open** (aperte).
- **Cosa Significa:** Un firewall di default è un filtro *stateful* (che tiene traccia delle connessioni). Se fosse stato configurato correttamente, avrebbe dovuto **scartare** i pacchetti SYN in entrata non richiesti.
  - **Risposta Attesa (Firewall funzionante):** La porta risulterebbe **filtered** (filtrata), perché il firewall scarta il pacchetto SYN di Nmap e non risponde.
  - **Risposta Ottenuta (Firewall non funzionante):** La porta risponde con SYN/ACK come se non ci fosse nessun filtro, confermando lo stato **open**.

Questo indica che, nonostante l'attivazione e il ripristino, le regole di eccezione che permettono l'accesso a questi servizi sono rimaste attive, **vanificando la funzione protettiva del firewall**.