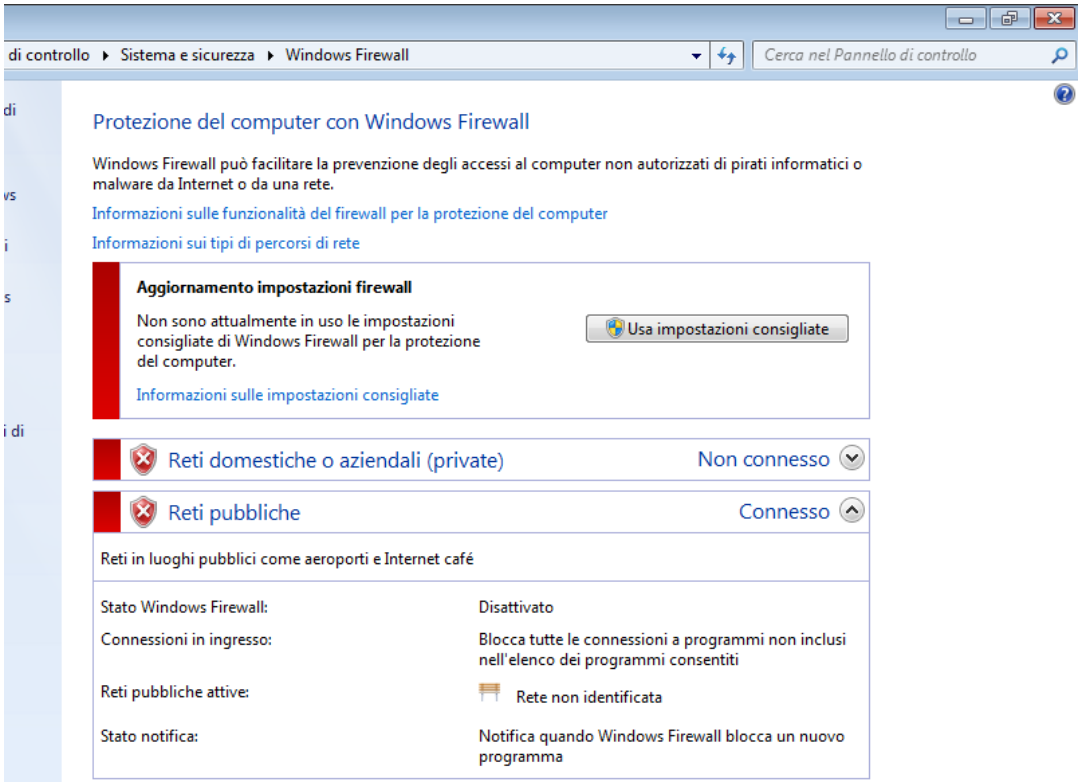
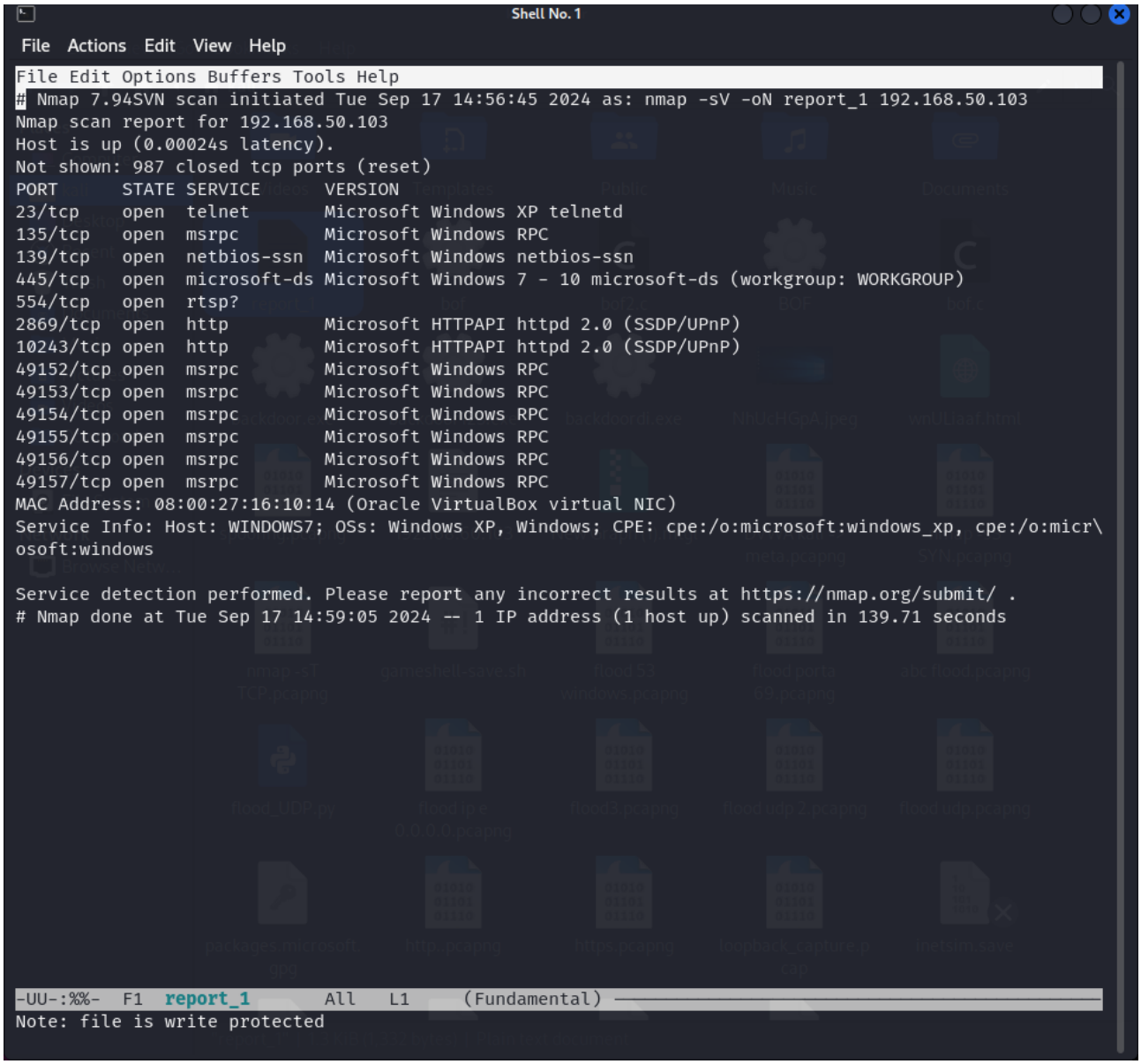
Scansione con Firewall disattivato



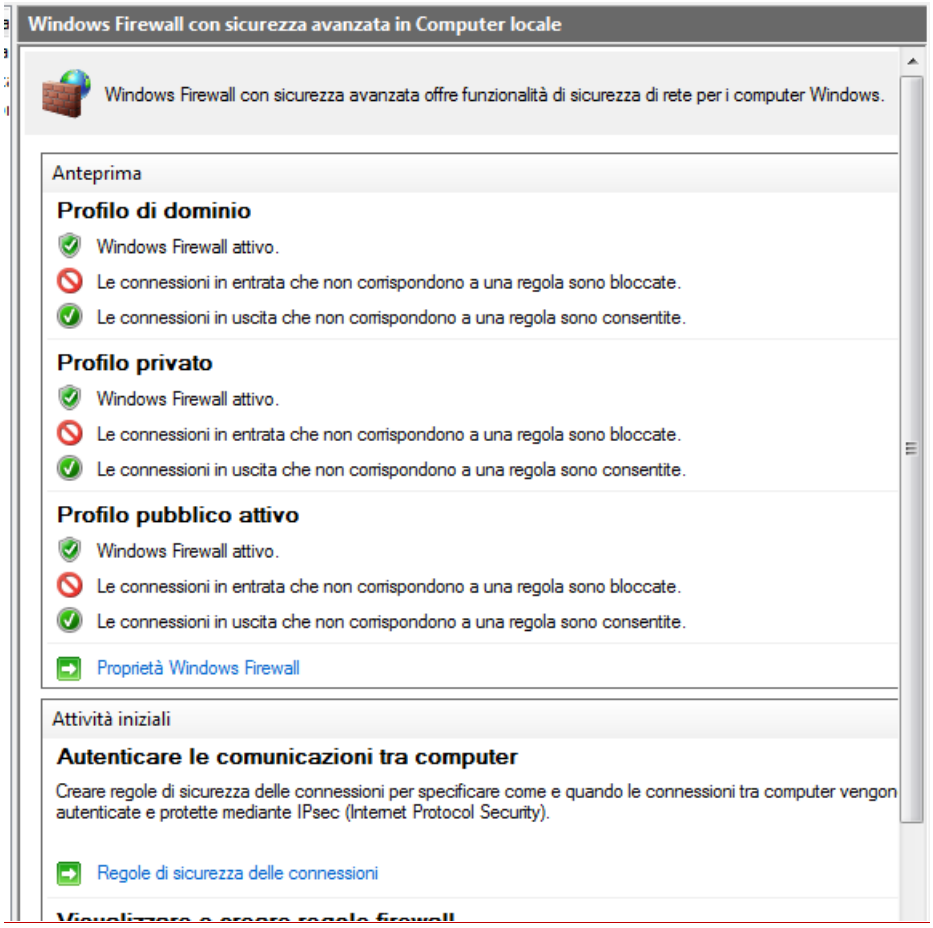

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.50.103 -oN report_1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-17 19:10 CEST
Nmap scan report for 192.168.50.103
Host is up (0.00054s latency).
Not shown: 987 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
23/tcp    open  telnet       Microsoft Windows XP telnetd
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)
554/tcp   open  rtsp?
2869/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
10243/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: WINDOWS7; OSs: Windows XP, Windows; CPE: cpe:/o:microsoft:windows_xp, cpe:/o:micro
soft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 140.31 seconds
```



Con il Firewall disabilitato, tutte le porte di rete aperte sui servizi attivi sulla macchina Windows erano direttamente visibili e accessibili da Nmap. Questa esposizione mette la macchina a rischio di attacchi, poiché gli aggressori possono sfruttare questi servizi non protetti.

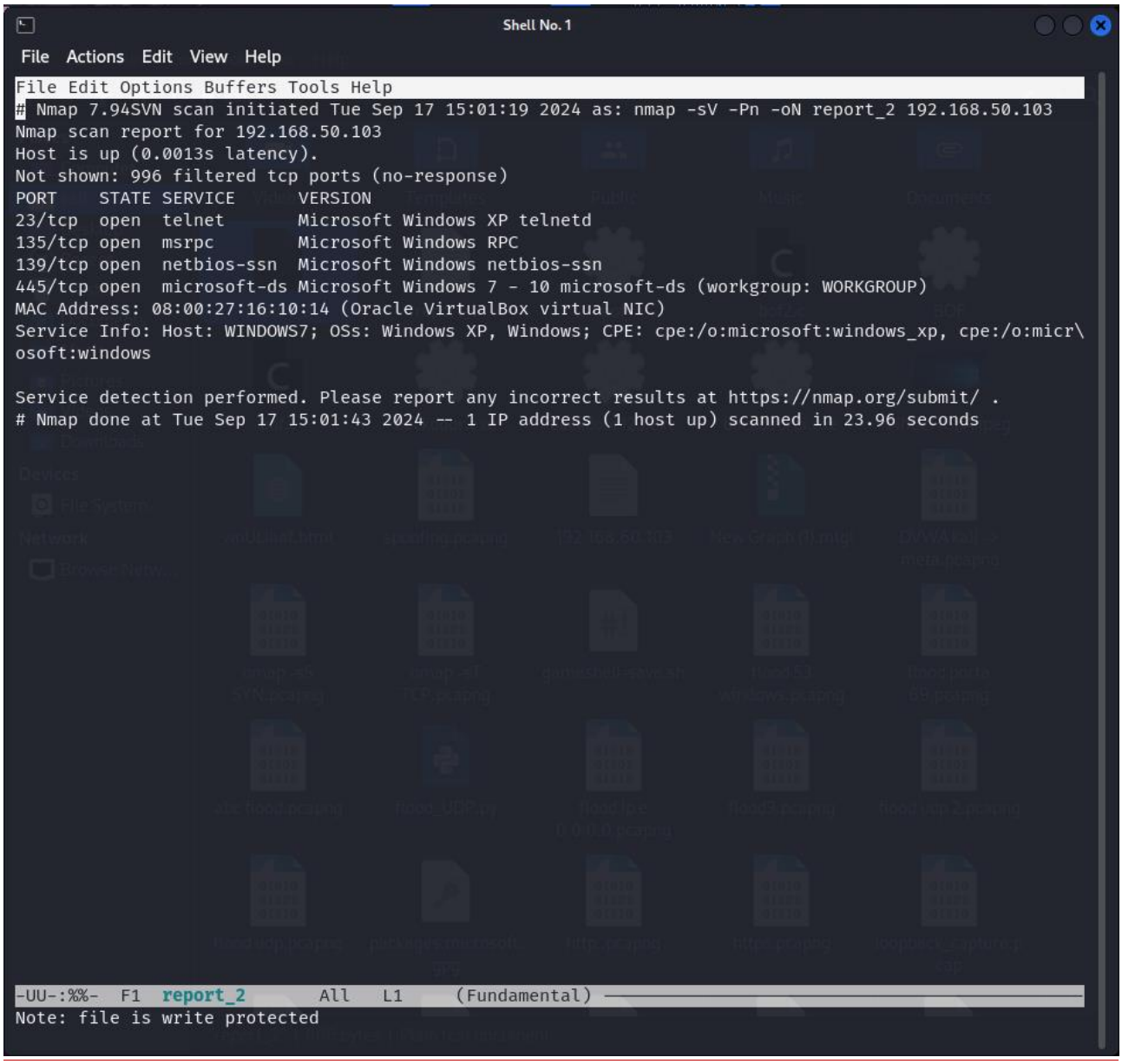
Scansione con Firewall attivato e ping bloccato




```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.50.103 -oN report_4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-17 19:06 CEST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.11 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.50.103 -oN report_5 -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-17 19:07 CEST
Nmap scan report for 192.168.50.103
Host is up (0.00094s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT    STATE SERVICE      VERSION
23/tcp  open  telnet       Microsoft Windows XP telnetd
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)
Service Info: Host: WINDOWS7; OSs: Windows XP, Windows; CPE: cpe:/o:microsoft:windows_xp, cpe:/o:micro
soft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 31.31 seconds
```



Quando il Firewall è abilitato, blocca tutte le porte non essenziali, rendendo invisibili o inaccessibili le porte non protette dall'esterno. La riduzione nel numero di porte rilevate dimostra che il Firewall sta svolgendo il suo compito di prevenire il traffico esterno non autorizzato, limitando così i servizi esposti.

Differenze tra i report:

Nel primo report, con il Firewall disabilitato, Nmap ha rilevato un numero significativo di porte aperte, tra cui diversi servizi come HTTP sulla porta 2869/tcp e diverse porte associate a MSRPC, comprese le porte da 49152 a 49157. Questo indica che la macchina era molto esposta e vulnerabile, mostrando un totale di 18 porte aperte e accessibili dall'esterno.

Nel secondo report, invece, con il Firewall attivato e il traffico ICMP bloccato, Nmap ha rilevato solo 4 porte aperte: il servizio Telnet sulla porta 23/tcp, MSRPC sulla porta 135/tcp, NetBIOS-SSN sulla porta 139/tcp e Microsoft-DS sulla porta 445/tcp. Il Firewall ha filtrato tutte le altre porte e ha impedito l'accesso agli altri servizi che erano stati rilevati nella prima scansione.

Questo dimostra chiaramente l'efficacia del Firewall nel proteggere la macchina, riducendo drasticamente la superficie di attacco e limitando la visibilità dei servizi attivi. Il confronto tra i due report mette in evidenza come l'attivazione del Firewall riduca il numero di porte esposte, proteggendo così la rete da potenziali attacchi esterni.