

SCANSIONI NMAP CON FIREWALL DI WINDOWS XP SPENTO

```
(kali@kali)-[~]
$ nmap -sV 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-09 14:21 EDT
Nmap scan report for 192.168.240.150
Host is up (0.0022s latency).
Not shown: 997 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 Microsoft Windows XP microsoft-ds
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.68 seconds
```

```
(kali@kali)-[~]
$ nmap -sV 192.168.240.150 -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-09 14:22 EDT
Nmap scan report for 192.168.240.150
Host is up (0.0026s latency).
Not shown: 997 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 Microsoft Windows XP microsoft-ds
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.51 seconds
```

```
(kali@kali)-[~]
$ nmap -sV 192.168.240.150 -oN ciao
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-09 14:24 EDT
Stats: 0:00:02 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Nmap scan report for 192.168.240.150
Host is up (0.0026s latency).
Not shown: 997 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 Microsoft Windows XP microsoft-ds
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.41 seconds
```

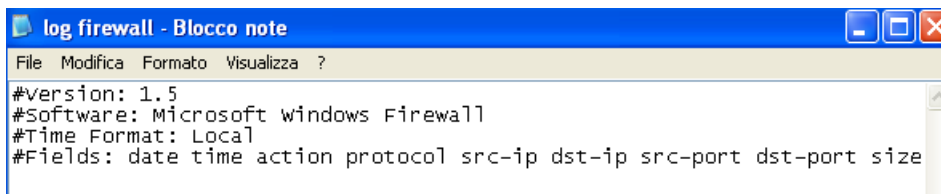
```
~/ciao - Mousepad
File Edit Search View Document Help
[Icons]
1 # Nmap 7.94SVN scan initiated Tue Apr 9 14:24:54 2024 as: nmap -sV -oN ciao 192.168.240.150
2 Nmap scan report for 192.168.240.150
3 Host is up (0.0026s latency).
4 Not shown: 997 closed tcp ports (conn-refused)
5 PORT      STATE SERVICE      VERSION
6 135/tcp   open  msrpc        Microsoft Windows RPC
7 139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
8 445/tcp   open  microsoft-ds Microsoft Windows XP microsoft-ds
9 Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp
10
11 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
12 # Nmap done at Tue Apr 9 14:25:14 2024 -- 1 IP address (1 host up) scanned in 20.41 seconds
13 |
```

SCANSIONI NMAP CON FIREWALL DI WINDOWS XP ATTIVO

```
(kali㉿kali)-[~]  
$ nmap -sV 192.168.1.60  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-09 14:30 EDT  
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 3.12 seconds
```

```
(kali㉿kali)-[~]  
$ nmap -sV 192.168.240.150 -Pn  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-09 14:31 EDT  
Nmap scan report for 192.168.240.150  
Host is up.  
All 1000 scanned ports on 192.168.240.150 are in ignored states.  
Not shown: 1000 filtered tcp ports (no-response)  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 215.31 seconds  
  
(kali㉿kali)-[~]
```

```
(kali㉿kali)-[~]  
$ nmap -sV 192.168.240.150 -oN ciao2  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-09 14:38 EDT  
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 3.20 seconds
```



The screenshot shows a Windows XP Notepad window titled "log firewall - Blocco note". The window contains the following text:

```
#Version: 1.5  
#Software: Microsoft windows Firewall  
#Time Format: Local  
#Fields: date time action protocol src-ip dst-ip src-port dst-port size
```

La differenza che si è potuta notare è che con il firewall spento la scansione ha rilevato 3 porte aperte, con il firewall acceso non ne ha rilevato nessuna. Nel caso del firewall chiuso abbiamo dovuto vedere i log direttamente da kali in quanto windows xp non crea un file di log se il firewall è spento.