

## Scansione con firewall disattivato

```
kali@kali: ~  
File Actions Edit View Help  
└─$ sudo nmap -sS -sV -p- -T5 -v 192.168.1.103  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-18 14:23 EDT  
NSE: Loaded 46 scripts for scanning.  
Initiating ARP Ping Scan at 14:23  
Scanning 192.168.1.103 [1 port]  
Completed ARP Ping Scan at 14:23, 0.07s elapsed (1 total hosts)  
Initiating Parallel DNS resolution of 1 host. at 14:23  
Completed Parallel DNS resolution of 1 host. at 14:23, 13.01s elapsed  
Initiating SYN Stealth Scan at 14:23  
Scanning 192.168.1.103 [65535 ports]  
Discovered open port 135/tcp on 192.168.1.103  
Discovered open port 139/tcp on 192.168.1.103  
Discovered open port 445/tcp on 192.168.1.103  
Discovered open port 49157/tcp on 192.168.1.103  
Discovered open port 49153/tcp on 192.168.1.103  
Discovered open port 49152/tcp on 192.168.1.103  
Discovered open port 49155/tcp on 192.168.1.103  
Discovered open port 49154/tcp on 192.168.1.103  
Discovered open port 49156/tcp on 192.168.1.103  
Completed SYN Stealth Scan at 14:24, 29.84s elapsed (65535 total ports)  
Initiating Service scan at 14:24  
Scanning 9 services on 192.168.1.103  
Service scan Timing: About 44.44% done; ETC: 14:26 (0:01:08 remaining)  
Completed Service scan at 14:25, 58.83s elapsed (9 services on 1 host)  
NSE: Script scanning 192.168.1.103.  
Initiating NSE at 14:25  
Completed NSE at 14:25, 0.03s elapsed  
Initiating NSE at 14:25  
Completed NSE at 14:25, 0.01s elapsed  
Nmap scan report for 192.168.1.103  
Host is up (0.00062s latency).  
Not shown: 65526 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     Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)  
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  
MAC Address: 08:00:27:FE:D6:96 (Oracle VirtualBox virtual NIC)  
Service Info: Host: WINDOWS-7; OS: Windows; CPE: cpe:/o:microsoft:windows  
  
Read data files from: /usr/bin/./share/nmap  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 102.12 seconds  
Raw packets sent: 66089 (2.908MB) | Rcvd: 65537 (2.622MB)
```

Scansione con firewall attivato

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ sudo nmap -sS -sV -p- -T5 -v 192.168.1.103  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-18 14:35 EDT  
NSE: Loaded 46 scripts for scanning.  
Initiating ARP Ping Scan at 14:35  
Scanning 192.168.1.103 [1 port]  
Completed ARP Ping Scan at 14:35, 0.06s elapsed (1 total hosts)  
Initiating Parallel DNS resolution of 1 host. at 14:35  
Completed Parallel DNS resolution of 1 host. at 14:35, 13.02s elapsed  
Initiating SYN Stealth Scan at 14:35  
Scanning 192.168.1.103 [65535 ports]  
SYN Stealth Scan Timing: About 4.43% done; ETC: 14:47 (0:11:08 remaining)  
SYN Stealth Scan Timing: About 8.87% done; ETC: 14:46 (0:10:27 remaining)  
SYN Stealth Scan Timing: About 13.33% done; ETC: 14:46 (0:09:52 remaining)  
SYN Stealth Scan Timing: About 18.22% done; ETC: 14:46 (0:09:17 remaining)  
SYN Stealth Scan Timing: About 23.10% done; ETC: 14:46 (0:08:43 remaining)  
SYN Stealth Scan Timing: About 28.01% done; ETC: 14:46 (0:08:08 remaining)  
SYN Stealth Scan Timing: About 33.36% done; ETC: 14:46 (0:07:32 remaining)  
SYN Stealth Scan Timing: About 38.26% done; ETC: 14:46 (0:06:58 remaining)  
SYN Stealth Scan Timing: About 43.86% done; ETC: 14:46 (0:06:21 remaining)  
SYN Stealth Scan Timing: About 49.09% done; ETC: 14:46 (0:05:46 remaining)  
SYN Stealth Scan Timing: About 54.36% done; ETC: 14:46 (0:05:11 remaining)  
SYN Stealth Scan Timing: About 59.63% done; ETC: 14:46 (0:04:35 remaining)  
SYN Stealth Scan Timing: About 64.98% done; ETC: 14:46 (0:03:58 remaining)  
SYN Stealth Scan Timing: About 70.09% done; ETC: 14:46 (0:03:24 remaining)  
SYN Stealth Scan Timing: About 75.26% done; ETC: 14:46 (0:02:49 remaining)  
SYN Stealth Scan Timing: About 80.56% done; ETC: 14:46 (0:02:13 remaining)  
SYN Stealth Scan Timing: About 85.85% done; ETC: 14:46 (0:01:37 remaining)  
SYN Stealth Scan Timing: About 90.98% done; ETC: 14:46 (0:01:02 remaining)  
Completed SYN Stealth Scan at 14:46, 684.22s elapsed (65535 total ports)  
Initiating Service scan at 14:46  
NSE: Script scanning 192.168.1.103.  
Initiating NSE at 14:46  
Completed NSE at 14:46, 0.00s elapsed  
Initiating NSE at 14:46  
Completed NSE at 14:46, 0.00s elapsed  
Nmap scan report for 192.168.1.103  
Host is up (0.0013s latency).  
All 65535 scanned ports on 192.168.1.103 are in ignored states.  
Not shown: 65535 filtered tcp ports (no-response)  
MAC Address: 08:00:27:FE:D6:96 (Oracle VirtualBox virtual NIC)  
  
Read data files from: /usr/bin/./share/nmap  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 697.66 seconds  
Raw packets sent: 131071 (5.767MB) | Rcvd: 1 (28B)  
  
(kali@kali)-[~]  
$
```

Come si evince dalle 2 scansioni il firewall di windows fa in modo che il sistema non risponda alle richieste di nmap e non permette l'individuazione di quali porte siano aperte e di conseguenza quali servizi siano attivi sull'host oggetto di scansione.