

# WIN7

## Esecuzione SYN scan sul target 192.168.60.102(Win7)

The screenshot shows a Kali Linux virtual machine interface. On the left, Wireshark is capturing traffic on the eth0 interface. The packet list shows two TCP SYN packets from 192.168.50.100 to 192.168.60.102 on port 80. The packet details for the first packet (No. 49) show the Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol layers. The packet bytes pane shows the raw data. On the right, a terminal window shows the execution of an Nmap SYN scan on 192.168.60.102. The output indicates that the host is up and lists several open ports: 135/tcp, 139/tcp, 445/tcp, 49152/tcp, 49153/tcp, 49154/tcp, 49155/tcp, and 49156/tcp.

```
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port == 80
No. Time Source Destination Protocol Length Info
49 7.774378895 192.168.50.100 192.168.60.102 TCP 58 46887 → 80 [SYN] Seq=0 Win
71 7.875338939 192.168.50.100 192.168.60.102 TCP 58 46889 → 80 [SYN] Seq=0 Win

Frame 49: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on eth0
Ethernet II, Src: PcsCompu_c7:e1:36 (08:00:27:c7:e1:36), Dst: 08:00:27:c7:e1:36
Internet Protocol Version 4, Src: 192.168.50.100, Dst: 192.168.60.102
Transmission Control Protocol, Src Port: 46887, Dst Port: 80

File Actions Edit View Help
root@kali: /home/kali
nmap -sS 192.168.60.102
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-17 11:55 EDT
Nmap scan report for 192.168.60.102
Host is up (0.0034s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
Nmap done: 1 IP address (1 host up) scanned in 11.04 seconds
root@kali: /home/kali
```

## Esecuzione UDP scan per 192.168.60.102(Win7)


The screenshot shows a Kali Linux virtual machine interface. On the left, Wireshark is capturing traffic on the eth0 interface. The packet list shows two TCP ACK packets from 192.168.50.100 to 192.168.60.102 on port 80. The packet details for the first packet (No. 45) show the Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol layers. The packet bytes pane shows the raw data. On the right, a terminal window shows the execution of an Nmap UDP scan on 192.168.60.102. The output indicates that the host is up and lists several open ports: 137/udp and 139/udp.

```
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port == 80
No. Time Source Destination Protocol Length Info
45 140.200275727 192.168.50.100 192.168.60.102 TCP 54 50696 → 80 [ACK] Seq=1 Ack=
53 145.648574363 192.168.50.100 192.168.60.102 TCP 54 63143 → 80 [ACK] Seq=1 Ack=

Frame 45: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on eth0
Ethernet II, Src: PcsCompu_c7:e1:36 (08:00:27:c7:e1:36), Dst: 08:00:27:c7:e1:36
Internet Protocol Version 4, Src: 192.168.50.100, Dst: 192.168.60.102
Transmission Control Protocol, Src Port: 50696, Dst Port: 80
Source Port: 50696
Destination Port: 80
[Stream index: 9]
[Conversation completeness: Incomplete (4)]

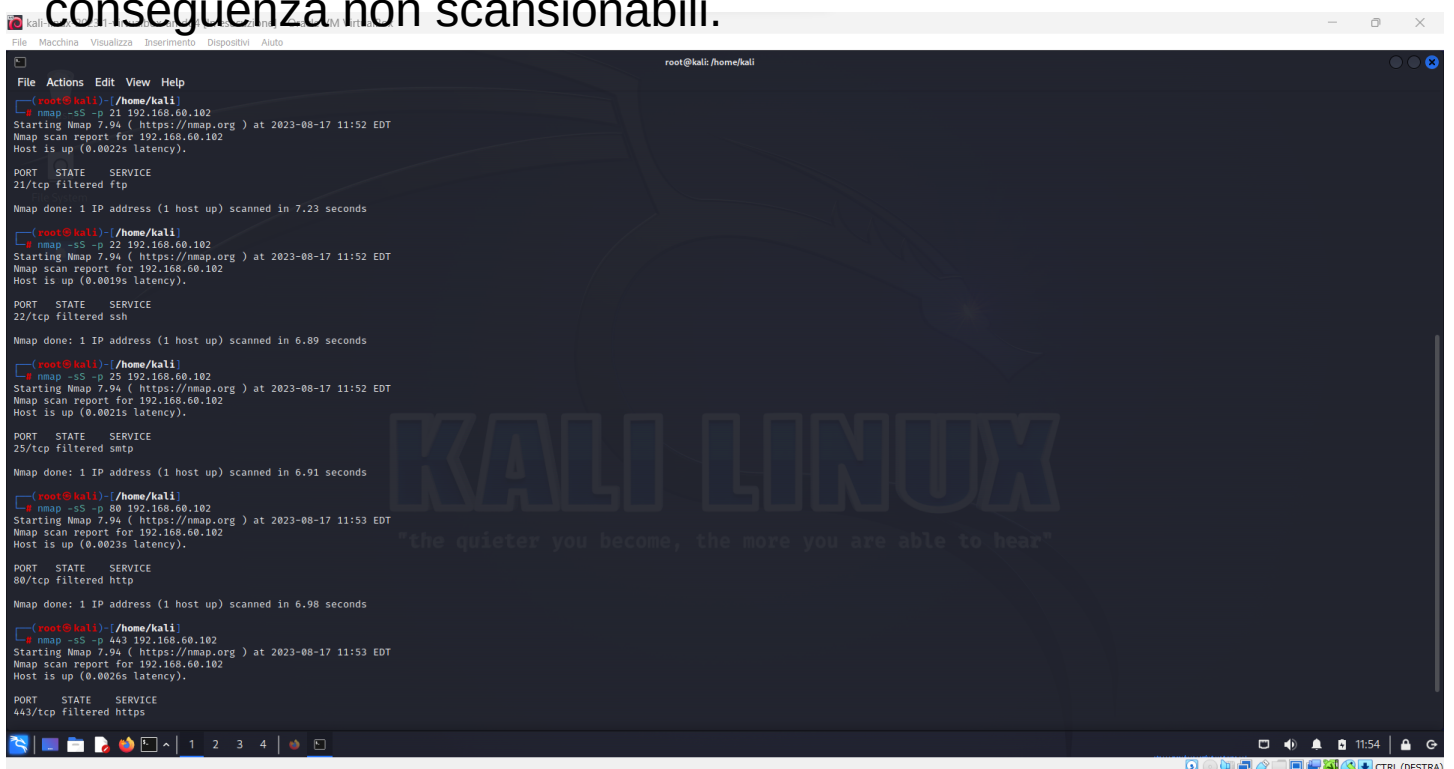
File Actions Edit View Help
root@kali: /home/kali
nmap -sU 192.168.60.102
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-17 11:38 EDT
Nmap scan report for 192.168.60.102
Host is up (0.0029s latency).
Not shown: 999 open/filtered udp ports (no-response)
PORT      STATE SERVICE
137/udp    open  netbios-ns
139/udp    open  netbios-ssn
Nmap done: 1 IP address (1 host up) scanned in 13.44 seconds
root@kali: /home/kali
```

# Esecuzione OS scan e Version scan sul target 192.168.60.102(Win7)



```
root@kali: /home/kali
nmap -O -sV 192.168.60.102
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-17 11:27 EDT
Stats: 0:01:11 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 75.00% done; ETC: 11:28 (0:00:20 remaining)
Nmap scan report for 192.168.60.102
Host is up (0.0024s latency).
Not shown: 992 filtered tcp ports (no-response)
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
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized|phone
Running: Microsoft Windows 7|Phone
OS CPE: cpe:/o:microsoft:windows.7 cpe:/o:microsoft:windows
OS details: Microsoft Windows Embedded Standard 7, Microsoft Windows Phone 7.5 or 8.0
Service Info: Host: WIN7; OS: Windows; CPE: cpe:/o:microsoft:windows
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 72.92 seconds
root@kali: /home/kali
```

Come possiamo notare sembra che windows sia protetto da un firewall che impedisce lo scan,effettuando dei test per singola porta si può verificare che alcune porte sono “filtered” e di conseguenza non scansionabili.



```
root@kali: /home/kali
nmap -sS -p 21 192.168.60.102
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-17 11:52 EDT
Nmap scan report for 192.168.60.102
Host is up (0.0022s latency).
PORT      STATE SERVICE
21/tcp    filtered ftp
Nmap done: 1 IP address (1 host up) scanned in 7.23 seconds
root@kali: /home/kali
nmap -sS -p 22 192.168.60.102
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-17 11:52 EDT
Nmap scan report for 192.168.60.102
Host is up (0.0019s latency).
PORT      STATE SERVICE
22/tcp    filtered ssh
Nmap done: 1 IP address (1 host up) scanned in 6.89 seconds
root@kali: /home/kali
nmap -sS -p 25 192.168.60.102
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-17 11:52 EDT
Nmap scan report for 192.168.60.102
Host is up (0.0021s latency).
PORT      STATE SERVICE
25/tcp    filtered smtp
Nmap done: 1 IP address (1 host up) scanned in 6.91 seconds
root@kali: /home/kali
nmap -sS -p 80 192.168.60.102
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-17 11:53 EDT
Nmap scan report for 192.168.60.102
Host is up (0.0023s latency).
PORT      STATE SERVICE
80/tcp    filtered http
Nmap done: 1 IP address (1 host up) scanned in 6.98 seconds
root@kali: /home/kali
nmap -sS -p 443 192.168.60.102
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-17 11:53 EDT
Nmap scan report for 192.168.60.102
Host is up (0.0026s latency).
PORT      STATE SERVICE
443/tcp   filtered https
```

Alcune soluzioni per “bypassare” un firewall con nmap possono essere:

- Eliminazione parallelismo attraverso il Timing(-T “0-1”).
- Mac Spoofing con nmap (--spooof-mac)
- FIN scan (dove possibile) (-sF)

Nmap mette a disposizione altri strumenti per il “Firewall Bypass”.