1. Scansione OS Fingerprint (nmap -O)

La scansione OS Fingerprint cerca di identificare il sistema operativo del target analizzando le risposte ai pacchetti inviati.

Risultati:

IP: 192.168.50.102

Sistema Operativo: Windows 7

2. Scansione SYN (nmap -sS)

Risultati sulla stessa rete (192.168.50.100):

```
PORT STATE SERVICE
 135/tcp open msrpc
 139/tcp open netbios-ssn
 445/tcp open microsoft-ds
 554/tcp open rtsp
 2869/tcp open icslap
 5357/tcp open wsdapi
 49152/tcp open unknown
 49153/tcp open unknown
 49154/tcp open unknown
 49155/tcp open unknown
 49156/tcp open unknown
```

Risultati su rete diversa (192.168.60.100):

```
 PORT STATE SERVICE
 135/tcp open msrpc
 139/tcp open netbios-ssn
 445/tcp open microsoft-ds
 554/tcp open rtsp
 2869/tcp open icslap
 5357/tcp open wsdapi
 49152/tcp open unknown
 49153/tcp open unknown
 49154/tcp open unknown
 49155/tcp open unknown
 49156/tcp open unknown
```

3. Scansione TCP Connect (nmap -sT)

Risultati sulla stessa rete (192.168.50.100):

```
PORT STATE SERVICE
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
554/tcp open rtsp
2869/tcp open icslap
5357/tcp open wsdapi
49152/tcp open unknown
49153/tcp open unknown
49154/tcp open unknown
49155/tcp open unknown
49156/tcp open unknown
```

Risultati su rete diversa (192.168.60.100):

```
PORT STATE SERVICE
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
554/tcp open rtsp
2869/tcp open icslap
5357/tcp open wsdapi
49152/tcp open unknown
49153/tcp open unknown
49154/tcp open unknown
49155/tcp open unknown
49156/tcp open unknown
```

4. Rilevazione delle Versioni (nmap -sV)

Risultati sulla stessa rete (192.168.50.100):

```
 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)
 554/tcp open rtsp Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
 2869/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
 5357/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
```

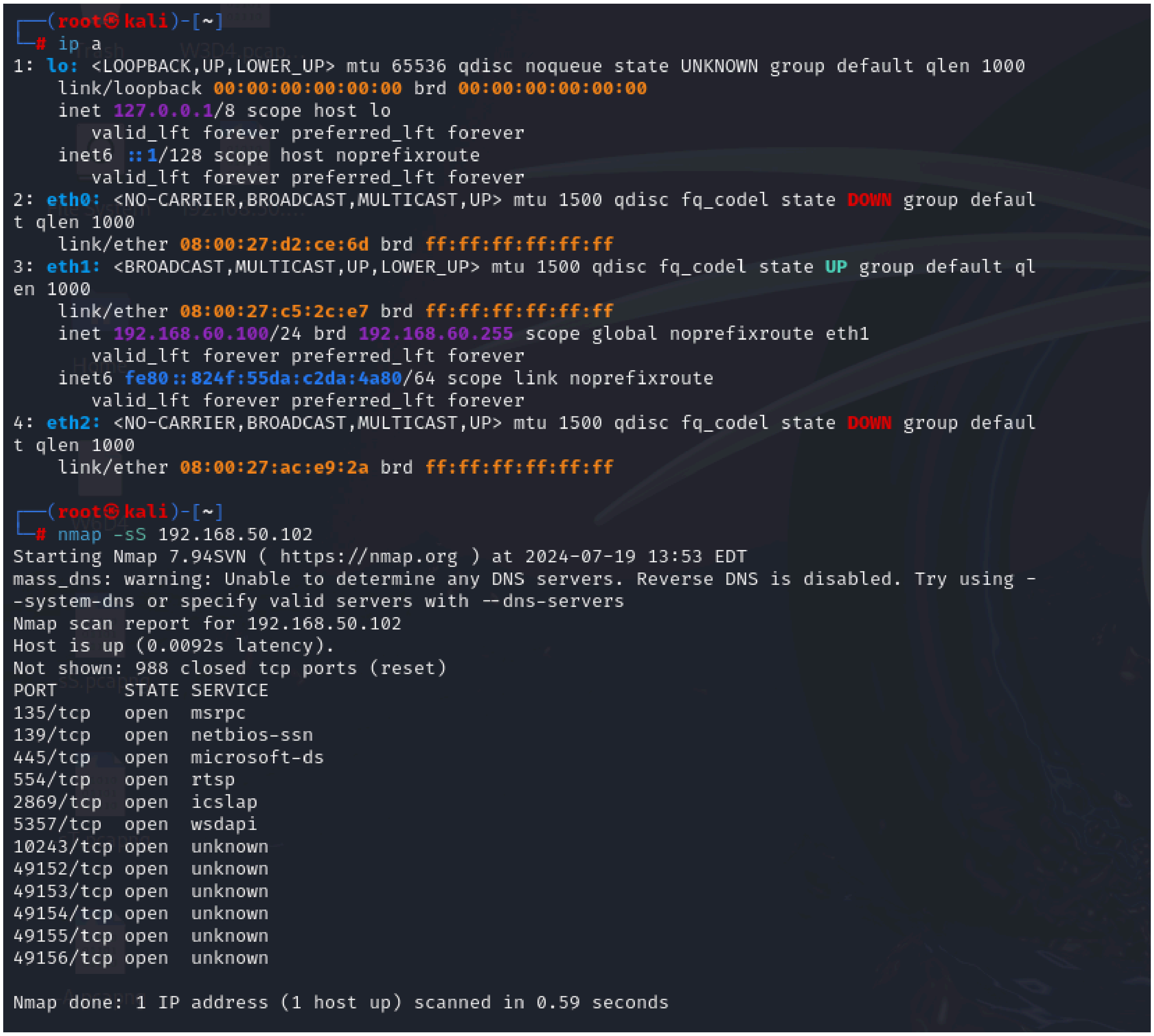
Risultati su rete diversa (192.168.60.100):

```
 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)
 554/tcp open rtsp Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
 2869/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
 5357/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
```

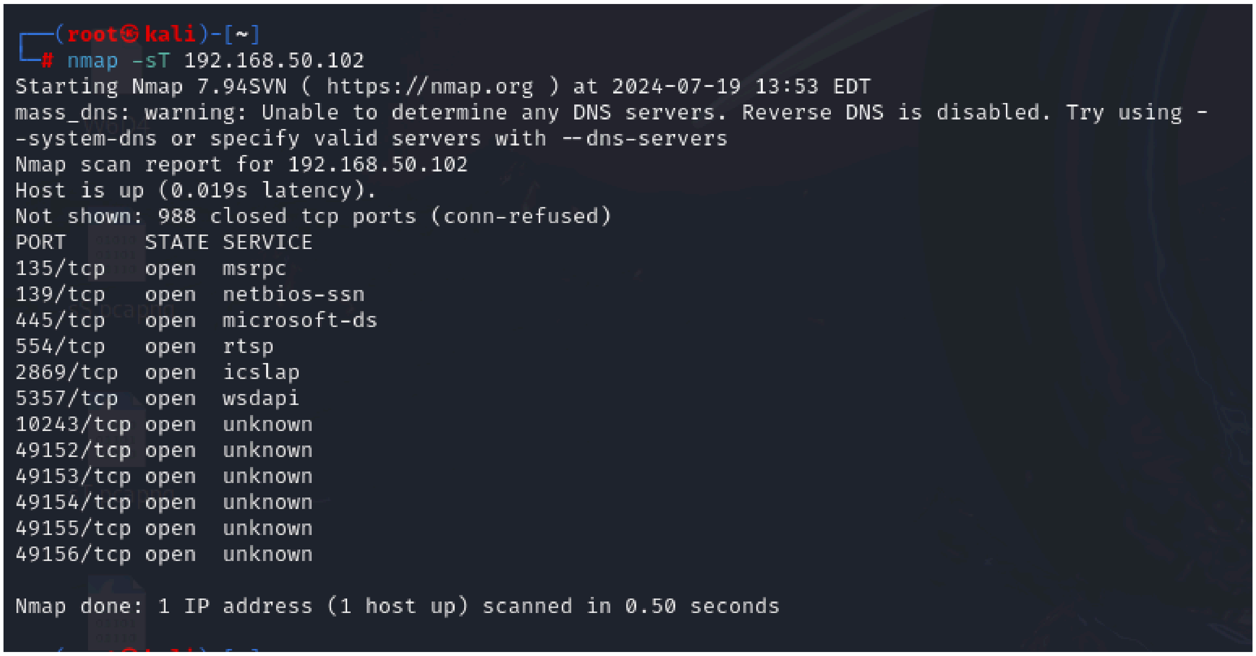
5. Conclusioni

Le scansioni effettuate su Windows 7 hanno mostrato che il sistema risponde in modo simile sia su rete locale che su rete diversa, indicando che le configurazioni di sicurezza e di rete non cambiano in base alla rete di origine. Non ci sono state differenze nei risultati delle scansioni tra la rete stessa e la rete diversa in quanto ho disattivato il firewall altrimenti non avrei visto nulla.

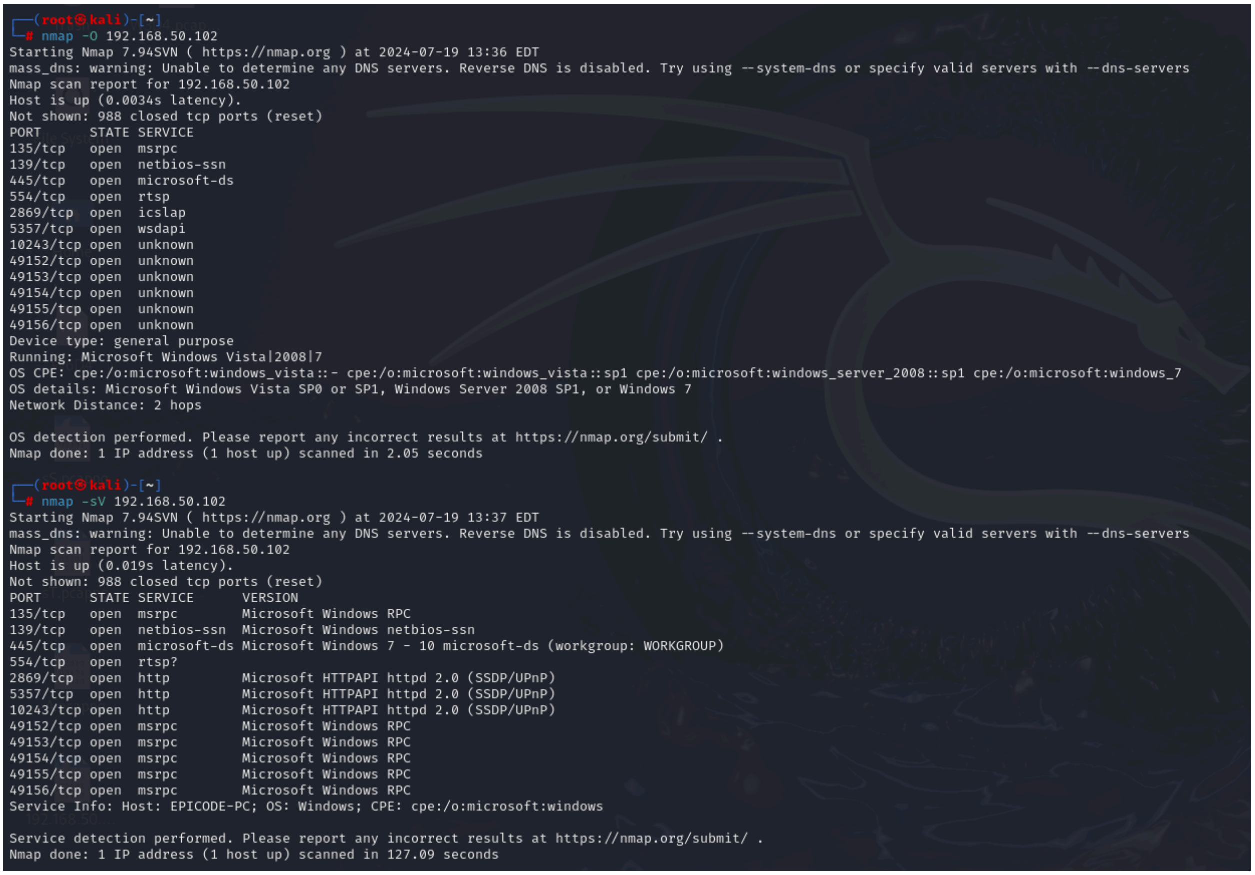
Di seguito gli screenshot.



```
┌──(root㉿kali)-[~]
└─# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state DOWN group defaul
t qlen 1000
    link/ether 08:00:27:d2:ce:6d brd ff:ff:ff:ff:ff:ff
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default ql
en 1000
    link/ether 08:00:27:c5:2c:e7 brd ff:ff:ff:ff:ff:ff
    inet 192.168.60.100/24 brd 192.168.60.255 scope global noprefixroute eth1
       valid_lft forever preferred_lft forever
    inet6 fe80::824f:55da:c2da:4a80/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
4: eth2: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state DOWN group defaul
t qlen 1000
    link/ether 08:00:27:ac:e9:2a brd ff:ff:ff:ff:ff:ff

┌──(root㉿kali)-[~]
└─# nmap -sS 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-19 13:53 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using -
-system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.50.102
Host is up (0.0092s latency).
Not shown: 988 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  icslap
5357/tcp  open  wsdapi
10243/tcp open  unknown
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 0.59 seconds
```

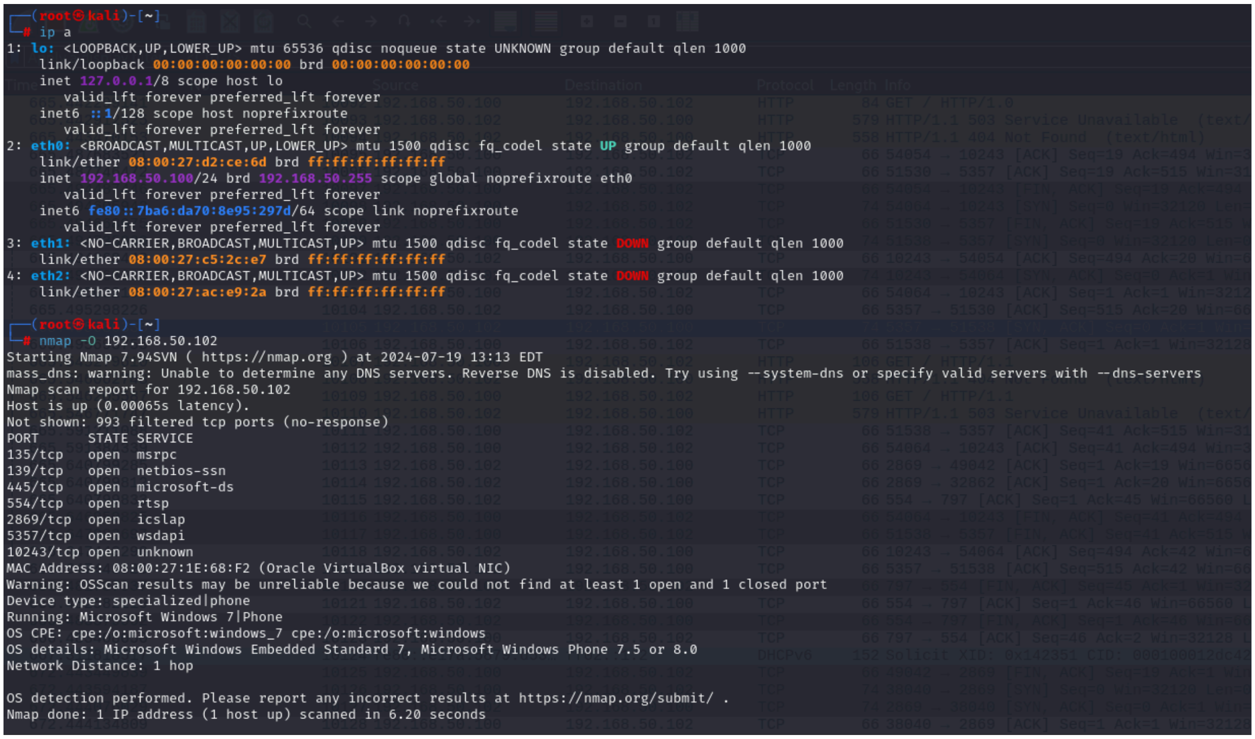


```
┌──(root㉿kali)-[~]
└─# nmap -sT 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-19 13:53 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using -
-system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.50.102
Host is up (0.019s latency).
Not shown: 988 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  icslap
5357/tcp  open  wsdapi
10243/tcp open  unknown
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 0.50 seconds
```

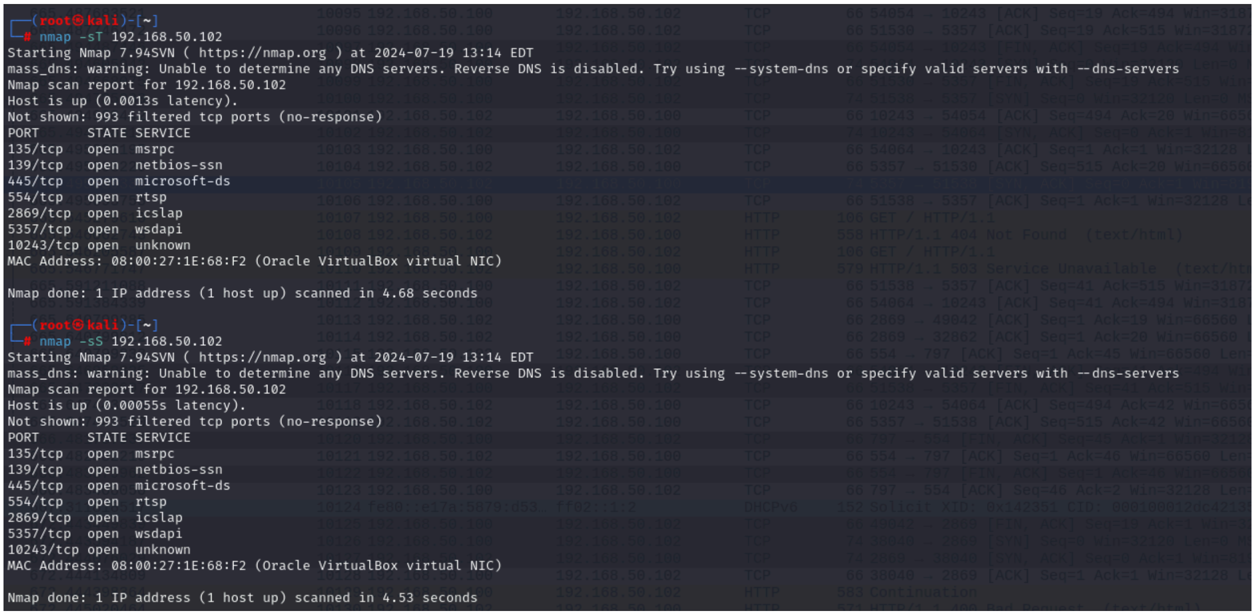


```
┌──(root㉿kali)-[~]
└─# nmap -O 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-19 13:36 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.50.102
Host is up (0.0034s latency).
Not shown: 988 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  icslap
5357/tcp  open  wsdapi
10243/tcp open  unknown
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
Device type: general purpose
Running: Microsoft Windows Vista|2008|7
OS CPE: cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_7
OS details: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7
Network Distance: 2 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.05 seconds

┌──(root㉿kali)-[~]
└─# nmap -sV 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-19 13:37 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.50.102
Host is up (0.019s latency).
Not shown: 988 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)
554/tcp   open  rtsp?
2869/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/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
Service Info: Host: EPICODE-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 127.09 seconds
```

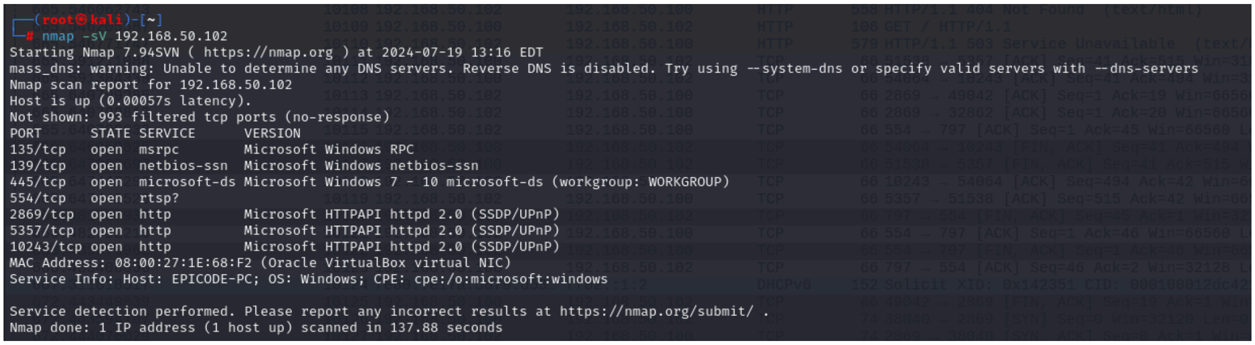
Stessa rete



```
┌──(root㉿kali)-[~]
└─# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:d2:ce:6d brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.100/24 brd 192.168.50.255 scope global noprefixroute eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::7ba6:da70:8e95:297d/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: eth1: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state DOWN group default qlen 1000
    link/ether 08:00:27:c5:2c:e7 brd ff:ff:ff:ff:ff:ff
4: eth2: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state DOWN group default qlen 1000
    link/ether 08:00:27:ac:e9:2a brd ff:ff:ff:ff:ff:ff

┌──(root㉿kali)-[~]
└─# nmap -O 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-19 13:13 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.50.102
Host is up (0.00065s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  icslap
5357/tcp  open  wsdapi
10243/tcp open  unknown
MAC Address: 08:00:27:1E:68:F2 (Oracle VirtualBox virtual NIC)
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
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.20 seconds
```



```
┌──(root㉿kali)-[~]
└─# nmap -sT 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-19 13:14 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.50.102
Host is up (0.0013s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  icslap
5357/tcp  open  wsdapi
10243/tcp open  unknown
MAC Address: 08:00:27:1E:68:F2 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 4.68 seconds

┌──(root㉿kali)-[~]
└─# nmap -sS 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-19 13:14 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.50.102
Host is up (0.00055s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  icslap
5357/tcp  open  wsdapi
10243/tcp open  unknown
MAC Address: 08:00:27:1E:68:F2 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 4.53 seconds
```



```
┌──(root㉿kali)-[~]
└─# nmap -sV 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-19 13:16 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.50.102
Host is up (0.00057s latency).
Not shown: 993 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)
554/tcp   open  rtsp?
2869/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
10243/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 08:00:27:1E:68:F2 (Oracle VirtualBox virtual NIC)
Service Info: Host: EPICODE-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 137.88 seconds
```