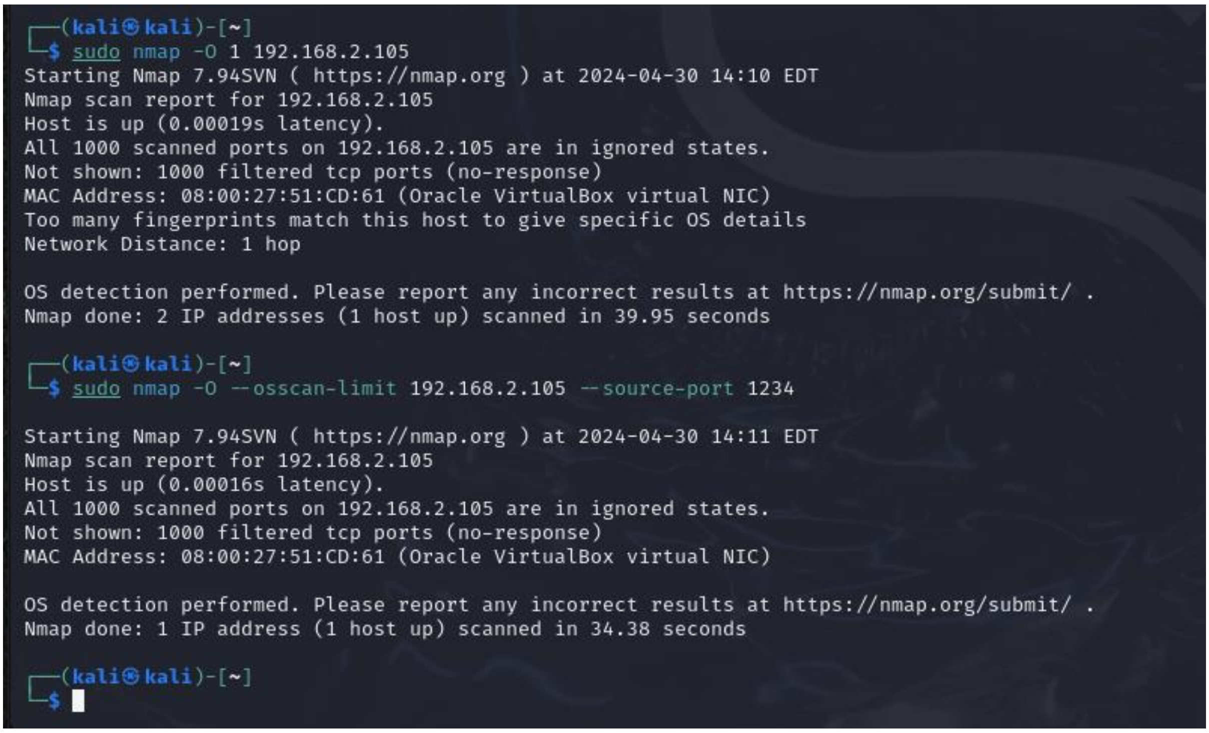
Scansione nmap Windows 7

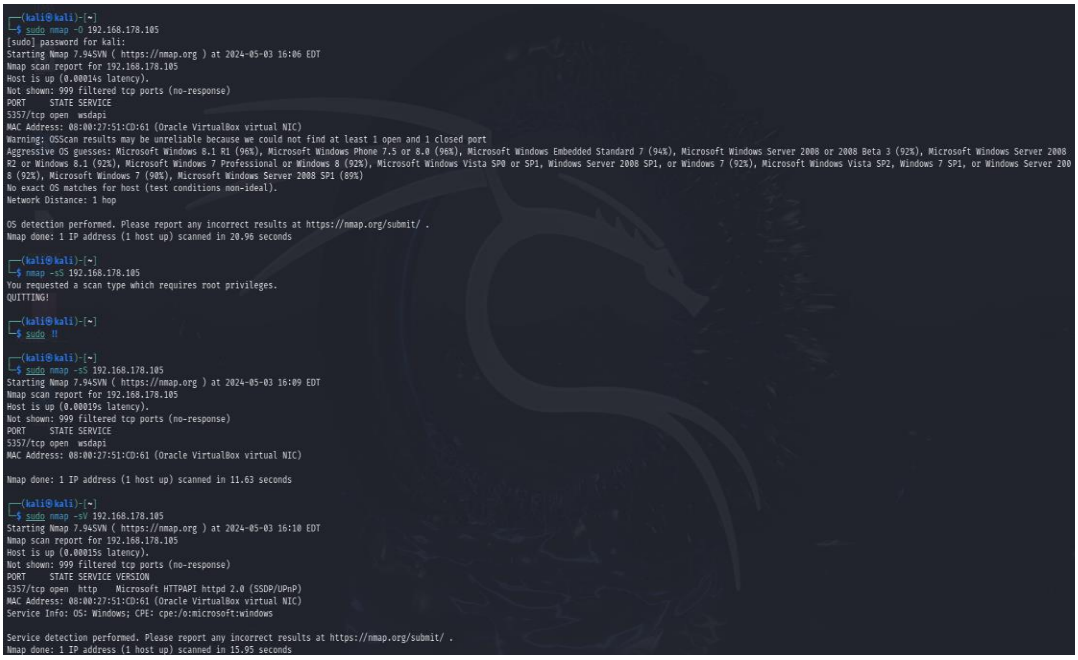
Non sono riuscito ad effettuare una scansione nmap senza modificare Windows, impostandolo su **rete domestica**. Opzioni provate: --osscan-limit, -Pn, -f (frammentazione pacchetti), -e (scheda di rete), -s (spoofing del MAC), -T0, -T1, porta sorgente 80 443.

Risultati originali (too many fingerprints)



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 1 192.168.2.105
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-30 14:10 EDT
Nmap scan report for 192.168.2.105
Host is up (0.00019s latency).
All 1000 scanned ports on 192.168.2.105 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:51:CD:61 (Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 2 IP addresses (1 host up) scanned in 39.95 seconds

┌──(kali㉿kali)-[~]
└─$ sudo nmap -O --osscan-limit 192.168.2.105 --source-port 1234

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-30 14:11 EDT
Nmap scan report for 192.168.2.105
Host is up (0.00016s latency).
All 1000 scanned ports on 192.168.2.105 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:51:CD:61 (Oracle VirtualBox virtual NIC)

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 34.38 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

Risultati Windows su rete domestica



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.178.105
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-03 16:06 EDT
Nmap scan report for 192.168.178.105
Host is up (0.00014s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE
5357/tcp open  wsdapi
MAC Address: 08:00:27:51:CD:61 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows 8.1 R1 (96%), Microsoft Windows Phone 7.5 or 8.0 (96%), Microsoft Windows Embedded Standard 7 (94%), Microsoft Windows Server 2008 or 2008 Beta 3 (92%), Microsoft Windows Server 2008
R2 or Windows 8.1 (92%), Microsoft Windows 7 Professional or Windows 8 (92%), Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (92%), Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 200
8 (92%), Microsoft Windows 7 (90%), Microsoft Windows Server 2008 SP1 (89%)
No exact OS matches for host (test conditions non-ideal).
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 20.96 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -sS 192.168.178.105
You requested a scan type which requires root privileges.
QUITTING!

┌──(kali㉿kali)-[~]
└─$ sudo !!

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.178.105
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-03 16:09 EDT
Nmap scan report for 192.168.178.105
Host is up (0.00019s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE
5357/tcp open  wsdapi
MAC Address: 08:00:27:51:CD:61 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 11.63 seconds

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.178.105
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-03 16:10 EDT
Nmap scan report for 192.168.178.105
Host is up (0.00015s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
5357/tcp open  http    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 08:00:27:51:CD:61 (Oracle VirtualBox virtual NIC)
Service Info: 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 15.95 seconds
```