Indirizzo IP: 192.168.60.103 (Attaccante e target sono posti su reti distinte)

nmap -O 192.168.60.103
Sistema Operativo: Microsoft Windows 7/2008
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
49157/tcp open unknown
Tipo dispositivo: Generale
Distanza Network: 2 Hop

nmap -sV 192.168.60.103
Porte Aperte e Versioni Attive
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

nmap -sS 192.168.60.103
Porte Aperte
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
49157/tcp open unknown

nmap -sT 192.168.60.103
Porte Aperte
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
49157/tcp open unknown

Indirizzo IP: 192.168.50.103 (Target e attaccante sono posti sulla stessa rete)

nmap -O 192.168.50.103
Sistema Operativo: Microsoft Windows 7/2008/8.1
Porte Aperte:
135/tcp (msrpc)
139/tcp (netbios-ssn)

445/tcp (microsoft-ds)
49152/tcp (unknown)
49153/tcp (unknown)
49154/tcp (unknown)
49155/tcp (unknown)
49156/tcp (unknown)
49157/tcp (unknown)
Tipo Dispositivo: Generale
Distanza di Rete: 1 hop

nmap -sS 192.168.50.103
Porte Aperte:
135/tcp (msrpc)
139/tcp (netbios-ssn)
445/tcp (microsoft-ds)
49152/tcp (unknown)
49153/tcp (unknown)
49154/tcp (unknown)
49155/tcp (unknown)
49156/tcp (unknown)
49157/tcp (unknown)

nmap -sT 192.168.50.103
Porte Aperte:
135/tcp (msrpc)
139/tcp (netbios-ssn)
445/tcp (microsoft-ds)
49152/tcp (unknown)
49153/tcp (unknown)
49154/tcp (unknown)
49155/tcp (unknown)
49156/tcp (unknown)
49157/tcp (unknown)

nmap -sV 192.168.50.103
Servizi:
135/tcp (Microsoft Windows RPC)
139/tcp (Microsoft Windows netbios-ssn)
445/tcp (Microsoft Windows 7 - 10 microsoft-ds)
49152/tcp (Microsoft Windows RPC)
49153/tcp (Microsoft Windows RPC)
49154/tcp (Microsoft Windows RPC)
49155/tcp (Microsoft Windows RPC)
49156/tcp (Microsoft Windows RPC)
49157/tcp (Microsoft Windows RPC)
Sistema Operativo: Microsoft Windows 7/2008/8.1
MAC Address: 08:00:27:16:10:14 (Oracle VirtualBox virtual NIC)

Differenze principali tra le scansioni

Le scansioni Nmap effettuate su reti diverse e uguali hanno rivelato differenze significative nella quantità e precisione delle informazioni raccolte, influenzate dalla distanza tra l'attaccante e il target.

Quando il target era su una rete diversa (192.168.60.103), la distanza di rete era di 2 hop, indicando due passaggi di rete tra l'attaccante e il target. Questa distanza può introdurre latenza e potenziali filtri intermedi che potrebbero alterare i risultati della scansione. Al contrario, quando il target era sulla stessa rete (192.168.50.103), la distanza di rete era di 1 hop, indicando che attaccante e target erano sulla stessa subnet. Questa vicinanza riduce la latenza e le interferenze, permettendo una scansione più diretta e accurata.

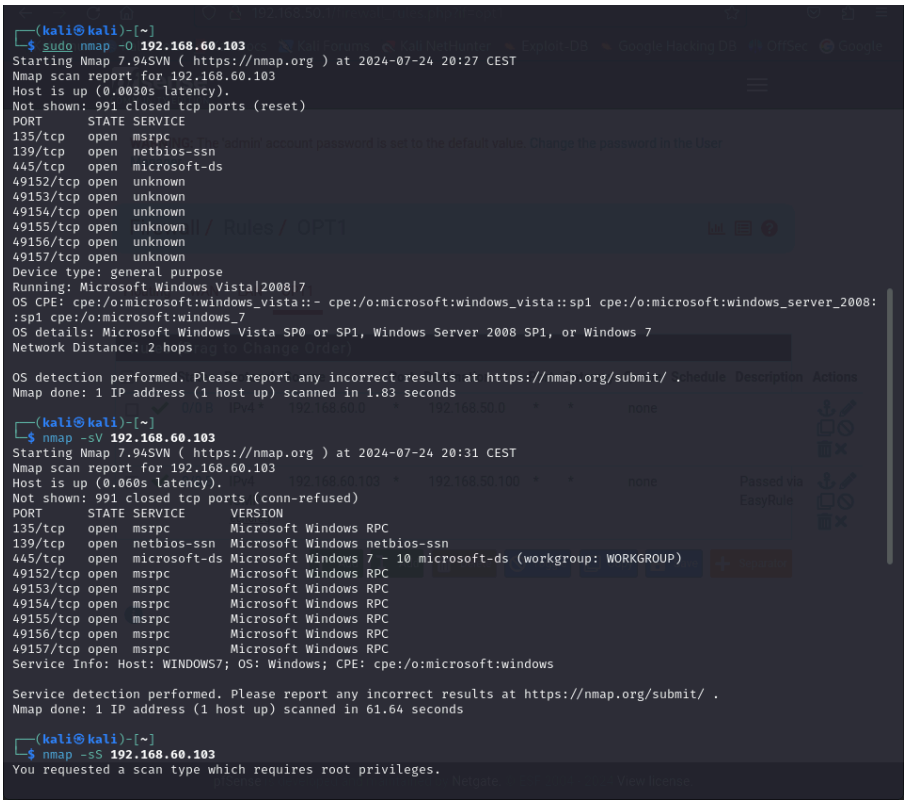
Nel caso della rete diversa, il sistema operativo rilevato è stato Microsoft Windows 7/2008. Nonostante la distanza aggiuntiva,

Nmap è riuscito a identificare il sistema operativo con un buon grado di precisione. Invece, sulla stessa rete, il sistema operativo rilevato è stato Microsoft Windows 7/2008/8.1. La vicinanza ha permesso a Nmap di ottenere informazioni leggermente più dettagliate, includendo una versione aggiuntiva (8.1).

Le porte aperte rilevate sono state le stesse in entrambe le situazioni (135, 139, 445, 49152-49157), indicando che la visibilità delle porte non è stata influenzata dalla distanza di rete. Inoltre, i servizi rilevati e le loro versioni erano identici, suggerendo che Nmap è stato in grado di identificare correttamente i servizi attivi su queste porte indipendentemente dalla distanza.

L'indirizzo MAC è stato rilevato solo quando il target e l'attaccante erano sulla stessa rete. Questo è prevedibile, poiché gli indirizzi MAC non vengono trasmessi oltre il primo hop di rete.

Scansioni di Kali su Windows con macchine poste su reti diverse



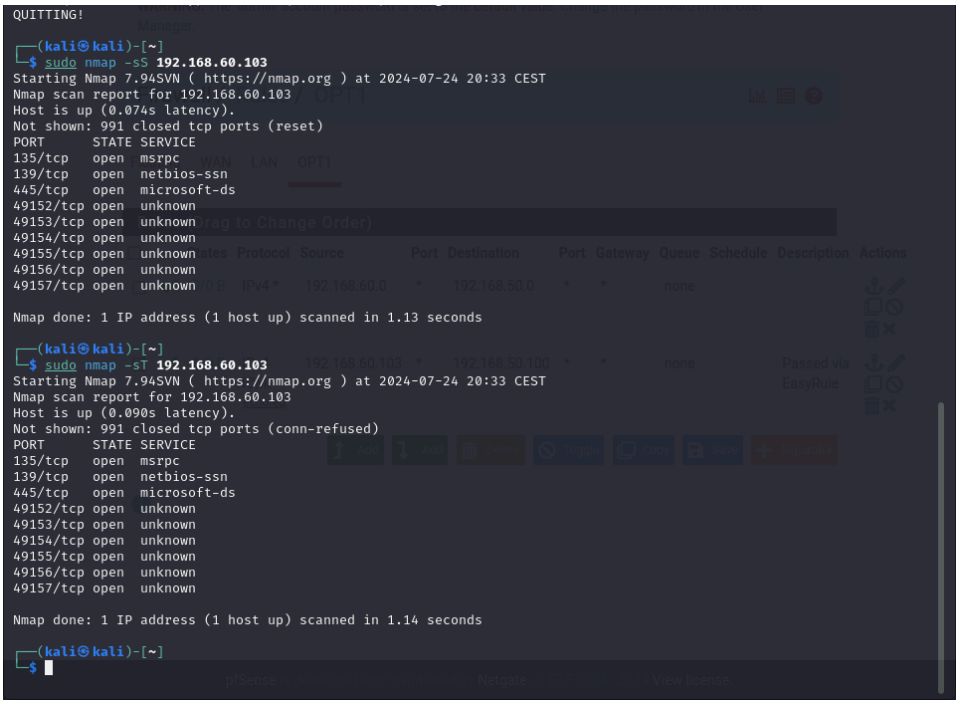
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.60.103
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-24 20:27 CEST
Nmap scan report for 192.168.60.103
Host is up (0.0030s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
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
49157/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 1.83 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.60.103
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-24 20:31 CEST
Nmap scan report for 192.168.60.103
Host is up (0.060s latency).
Not shown: 991 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 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
Service Info: Host: WINDOWS7; 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 61.64 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -sS 192.168.60.103
You requested a scan type which requires root privileges.
```



```
QUITTING!

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.60.103
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-24 20:33 CEST
Nmap scan report for 192.168.60.103
Host is up (0.074s latency).
Not shown: 991 closed tcp ports (reset)
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
49157/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 1.13 seconds

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT 192.168.60.103
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-24 20:33 CEST
Nmap scan report for 192.168.60.103
Host is up (0.090s latency).
Not shown: 991 closed tcp ports (conn-refused)
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
49157/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 1.14 seconds

┌──(kali㉿kali)-[~]
└─$
```

Scansioni su Windows con macchine poste sulla stessa rete

```
┌──(root㉿kali)-[~]
└─# nmap -O 192.168.50.103
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 12:48 CEST
Nmap scan report for 192.168.50.103
Host is up (0.0014s latency).
Not shown: 991 closed tcp ports (reset)
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
49157/tcp open  unknown
MAC Address: 08:00:27:16:10:14 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe
:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8
.1 Update 1
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 15.55 seconds

┌──(root㉿kali)-[~]
└─# nmap -sS 192.168.50.103
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 12:49 CEST
Nmap scan report for 192.168.50.103
Host is up (0.0014s latency).
Not shown: 991 closed tcp ports (reset)
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
49157/tcp open  unknown
MAC Address: 08:00:27:16:10:14 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.58 seconds
```

```
┌──(root㉿kali)-[~]
└─# nmap -sT 192.168.50.103
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 12:49 CEST
Nmap scan report for 192.168.50.103
Host is up (0.00074s latency).
Not shown: 991 closed tcp ports (conn-refused)
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
49157/tcp open  unknown
MAC Address: 08:00:27:16:10:14 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.62 seconds

┌──(root㉿kali)-[~]
└─# nmap -sV 192.168.50.103
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 12:50 CEST
Nmap scan report for 192.168.50.103
Host is up (0.00091s latency).
Not shown: 991 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: 08:00:27:16:10:14 (Oracle VirtualBox virtual NIC)
Service Info: Host: WINDOWS7; 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 74.60 seconds
```