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

nmap -O 192.168.60.103
Sistema Operativo: FreeBSD 11.x (97%) (Nota: OSSCAN può essere inaffidabile)
Porte Aperte:
53/tcp (domain)
80/tcp (http)
Tipo Dispositivo: Generale
Distanza di Rete: 1 hop

nmap -sV 192.168.60.103
Servizi:
53/tcp (Unbound)
80/tcp (nginx)
Sistema Operativo: FreeBSD 11.x (97%) (Nota: OSSCAN può essere inaffidabile)
MAC Address: Non fornito

nmap -sS 192.168.60.103
Porte Aperte:
53/tcp (domain)
80/tcp (http)

nmap -sT 192.168.60.103
Porte Aperte:
53/tcp (domain)
80/tcp (http)
Sistema Operativo: FreeBSD 11.x (97%) (Nota: OSSCAN può essere inaffidabile)
MAC Address: Non fornito

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

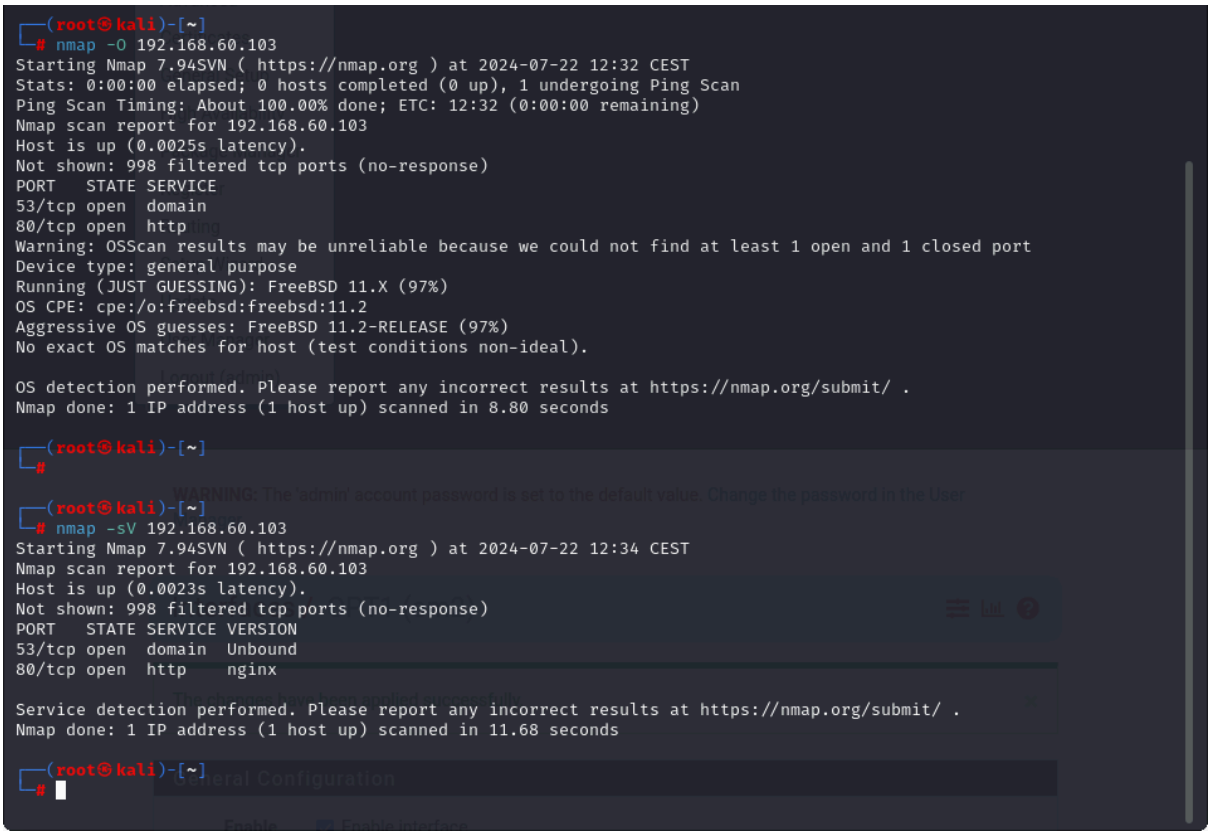
nmap -sS 192.168.50.103
Porte Aperte:
135/tcp (msrpc)
139/tcp (netbios-ssn)
445/tcp (microsoft-ds)
49152/tcp (unknown)
49153/tcp (unknown)
49154/tcp (unknown)
49155/tcp (unknown)
49156/tcp (unknown)
49157/tcp (unknown)

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)

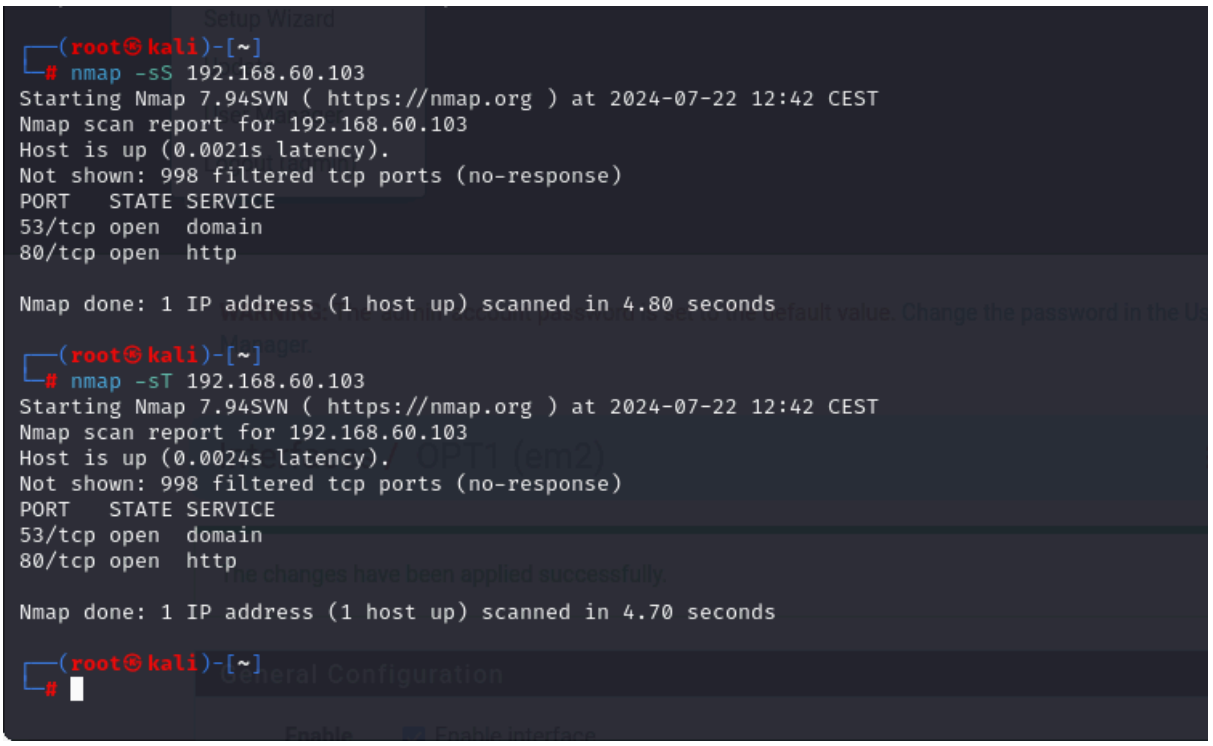
nmap -sV 192.168.50.103
Servizi:
135/tcp (Microsoft Windows RPC)
139/tcp (Microsoft Windows netbios-ssn)
445/tcp (Microsoft Windows 7 - 10 microsoft-ds)
49152/tcp (Microsoft Windows RPC)
49153/tcp (Microsoft Windows RPC)
49154/tcp (Microsoft Windows RPC)
49155/tcp (Microsoft Windows RPC)
49156/tcp (Microsoft 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)

Osservazioni finali:
192.168.50.103: IP che rappresenta un sistema Windows (versioni 7, 2008, 8.1) con diverse porte RPC aperte (135, 49152-49157), NetBIOS (139) e Microsoft-DS (445). Il dispositivo è una macchina virtuale gestita da Oracle VirtualBox, come indicato dal MAC Address. La scansione su questa rete mostra un alto grado di dettaglio e affidabilità, dato che si trova sulla stessa rete dell'attaccante.
192.168.60.103: IP che, anche se appartiene allo stesso sistema operativo precedentemente scansionato, suggerisce un sistema operativo FreeBSD a causa dell'elevata affidabilità della rilevazione OS. Sono aperte solo le porte 53 (DNS) e 80 (HTTP), con i servizi DNS gestiti da Unbound e HTTP da Nginx. Le informazioni sono meno dettagliate e potrebbero non essere completamente affidabili, probabilmente a causa della rete che è diversa da quella dell’attaccante.
Quindi, in conclusione, nel mio specifico caso, le principali differenze nelle scansioni sono influenzate dalla rete in cui si trova il target al momento: con l'IP 192.168.50.103 (nella stessa rete dell'attaccante) vengono fornite informazioni più dettagliate e precise; con l'IP 192.168.60.103 (su una rete diversa) i risultati sono meno affidabili e più limitati.

Scansioni di Kali su Windows con macchine poste su reti diverse



```
┌──(root㉿kali)-[~]
└─# nmap -O 192.168.60.103
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 12:32 CEST
Stats: 0:00:00 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Ping Scan Timing: About 100.00% done; ETC: 12:32 (0:00:00 remaining)
Nmap scan report for 192.168.60.103
Host is up (0.0025s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE
53/tcp open  domain
80/tcp open  http
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): FreeBSD 11.X (97%)
OS CPE: cpe:/o:freebsd:freebsd:11.2
Aggressive OS guesses: FreeBSD 11.2-RELEASE (97%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.80 seconds

┌──(root㉿kali)-[~]
└─#

┌──(root㉿kali)-[~]
└─# nmap -sV 192.168.60.103
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 12:34 CEST
Nmap scan report for 192.168.60.103
Host is up (0.0023s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
53/tcp open  domain  Unbound
80/tcp open  http    nginx

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.68 seconds

┌──(root㉿kali)-[~]
└─#
```



```
┌──(root㉿kali)-[~]
└─# nmap -sS 192.168.60.103
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 12:42 CEST
Nmap scan report for 192.168.60.103
Host is up (0.0021s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE
53/tcp open  domain
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 4.80 seconds

┌──(root㉿kali)-[~]
└─# nmap -sT 192.168.60.103
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 12:42 CEST
Nmap scan report for 192.168.60.103
Host is up (0.0024s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE
53/tcp open  domain
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 4.70 seconds

┌──(root㉿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
```