ESERCIZIO W11D1 PRATICA 2

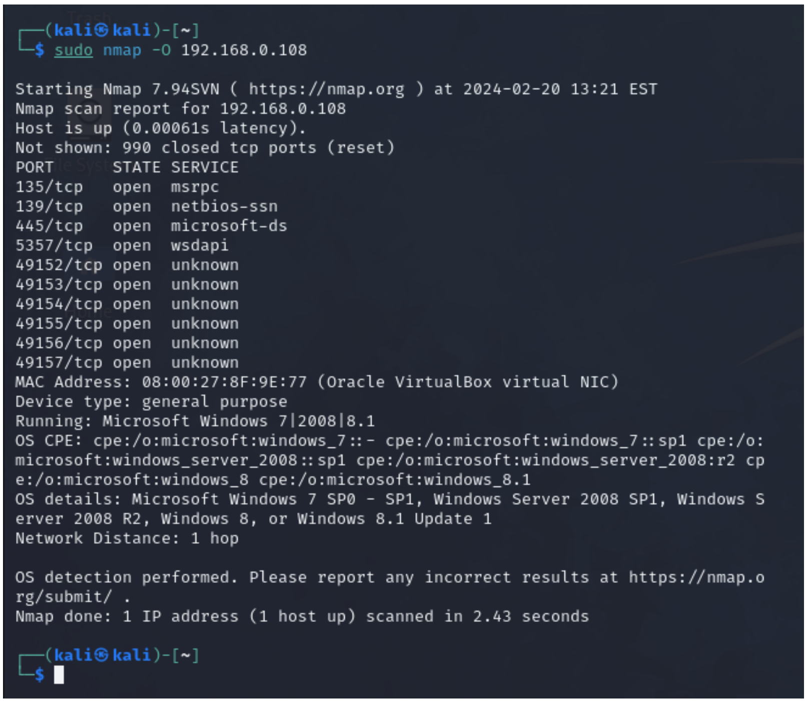
Traccia: Tecniche di scansione con Nmap Si richiede allo studente di effettuare le seguenti scansioni sul target Windows 7:

OS fingerprint

Syn Scan

Version detection

SCANSIONE OS-FINGERPRINT:



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.0.108

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-20 13:21 EST
Nmap scan report for 192.168.0.108
Host is up (0.00061s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsdapi
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: 08:00:27:8F:9E:77 (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 cp
e:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows S
erver 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.o
rg/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.43 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

Ecco il report della scansione dell'OS Fingerprint eseguita sul target Windows 7 con l'indirizzo IP 192.168.0.108:

IP del Sistema Operativo: 192.168.0.108

Porte Aperte:

135/tcp - msrpc

139/tcp - netbios-ssn

445/tcp - microsoft-ds

5357/tcp - wsdapi

49152/tcp - unknown

49153/tcp - unknown

49154/tcp - unknown

49155/tcp - unknown

49156/tcp - unknown

49157/tcp - unknown

Descrizione dei Servizi:

msrpc: Microsoft Remote Procedure Call (RPC)

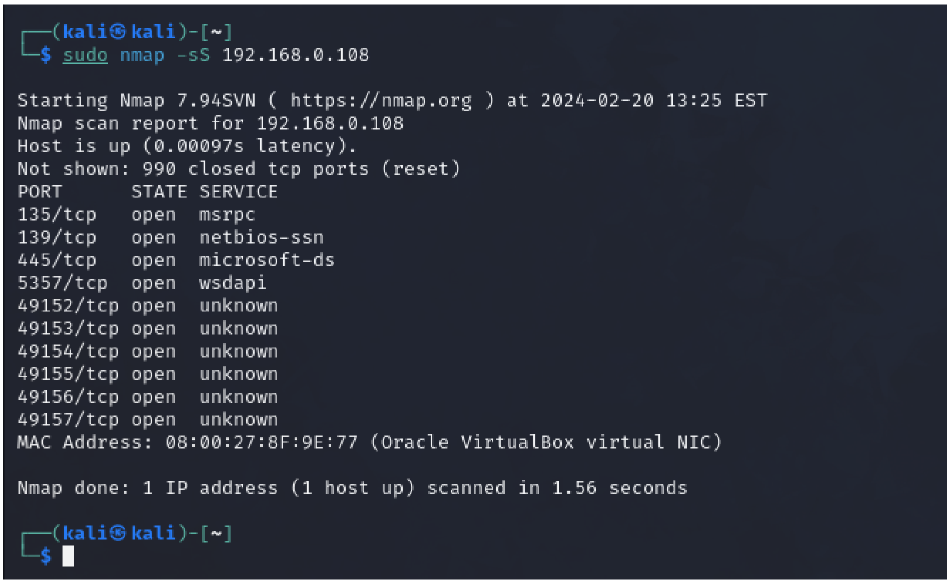
netbios-ssn: NetBIOS Session Service

microsoft-ds: Microsoft Directory Services (SMB)

wsdapi: Web Services for Devices API

Sistema Operativo Identificato: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, o Windows 8.1 Update 1

SCANSIONE SYN-SCAN:



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.0.108

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-20 13:25 EST
Nmap scan report for 192.168.0.108
Host is up (0.00097s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsdapi
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: 08:00:27:8F:9E:77 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.56 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

Ecco il report della scansione Syn Scan eseguita sul target Windows 7 con l'indirizzo IP 192.168.0.108:

IP del Sistema Operativo: 192.168.0.108

Porte Aperte:

135/tcp - msrpc

139/tcp - netbios-ssn

445/tcp - microsoft-ds

5357/tcp - wsdapi

49152/tcp - unknown

49153/tcp - unknown

49154/tcp - unknown

49155/tcp - unknown

49156/tcp - unknown

49157/tcp - unknown

Descrizione dei Servizi:

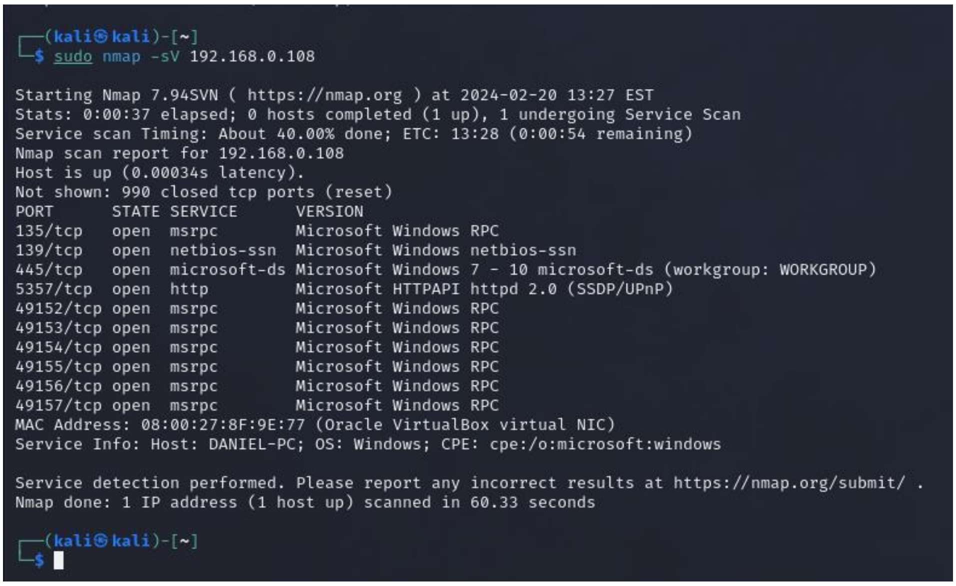
msrpc: Microsoft Remote Procedure Call (RPC)

netbios-ssn: NetBIOS Session Service

microsoft-ds: Microsoft Directory Services (SMB)

wsdapi: Web Services for Devices API

SCANSIONE VERSION DETECTION:



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.0.108

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-20 13:27 EST
Stats: 0:00:37 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 40.00% done; ETC: 13:28 (0:00:54 remaining)
Nmap scan report for 192.168.0.108
Host is up (0.00034s latency).
Not shown: 990 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)
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
49157/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:8F:9E:77 (Oracle VirtualBox virtual NIC)
Service Info: Host: DANIEL-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 60.33 seconds

┌──(kali㉿kali)-[~]
└─$ █
```

Ecco il report della scansione di rilevamento delle versioni eseguita sul target Windows 7 con l'indirizzo IP 192.168.0.108:

IP del Sistema Operativo: 192.168.0.108

Porte Aperte:

135/tcp - msrpc

139/tcp - netbios-ssn

445/tcp - microsoft-ds

5357/tcp - http (Microsoft HTTPAPI httpd 2.0 - SSDP/UPnP)

49152/tcp - msrpc

49153/tcp - msrpc

49154/tcp - msrpc

49155/tcp - msrpc

49156/tcp - msrpc

49157/tcp - msrpc

Servizi in Ascolto con Versione:

msrpc: Microsoft Windows RPC

netbios-ssn: Microsoft Windows netbios-ssn

microsoft-ds: Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)

http (5357/tcp): Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

Informazioni aggiuntive:

Host: DANIEL-PC

Sistema Operativo: Windows