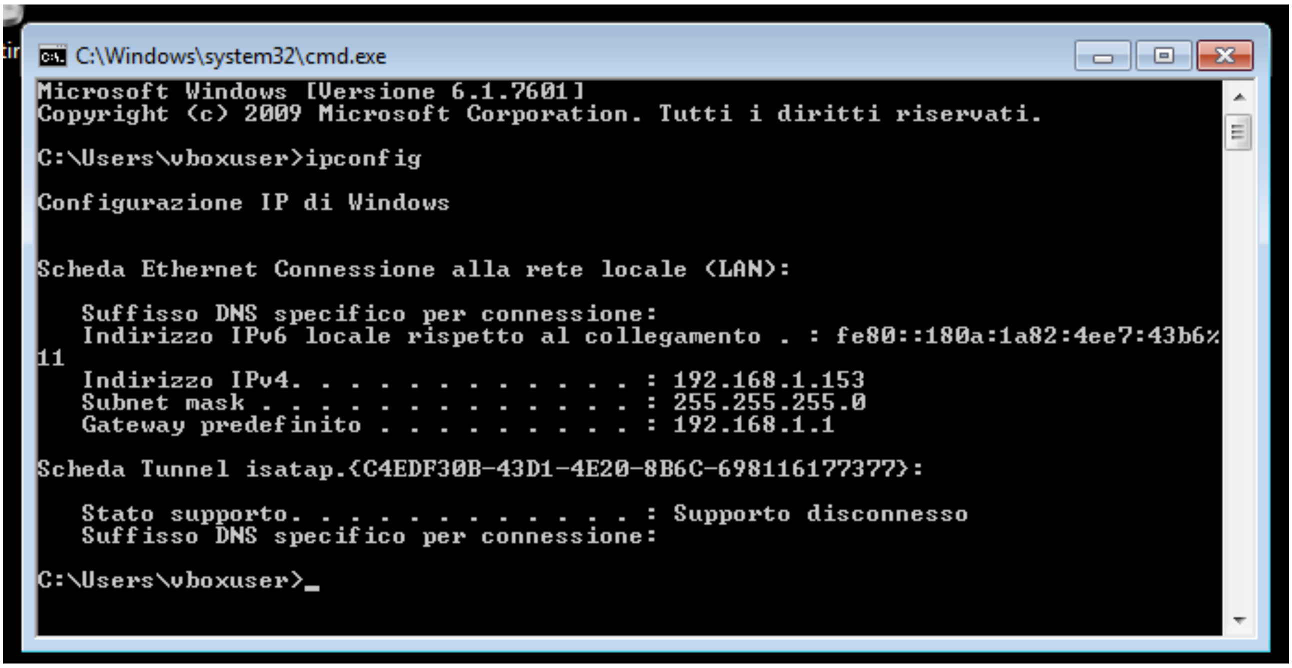
Marco Bagnaschi
m.bagnaschi@icloud.com

Traccia:

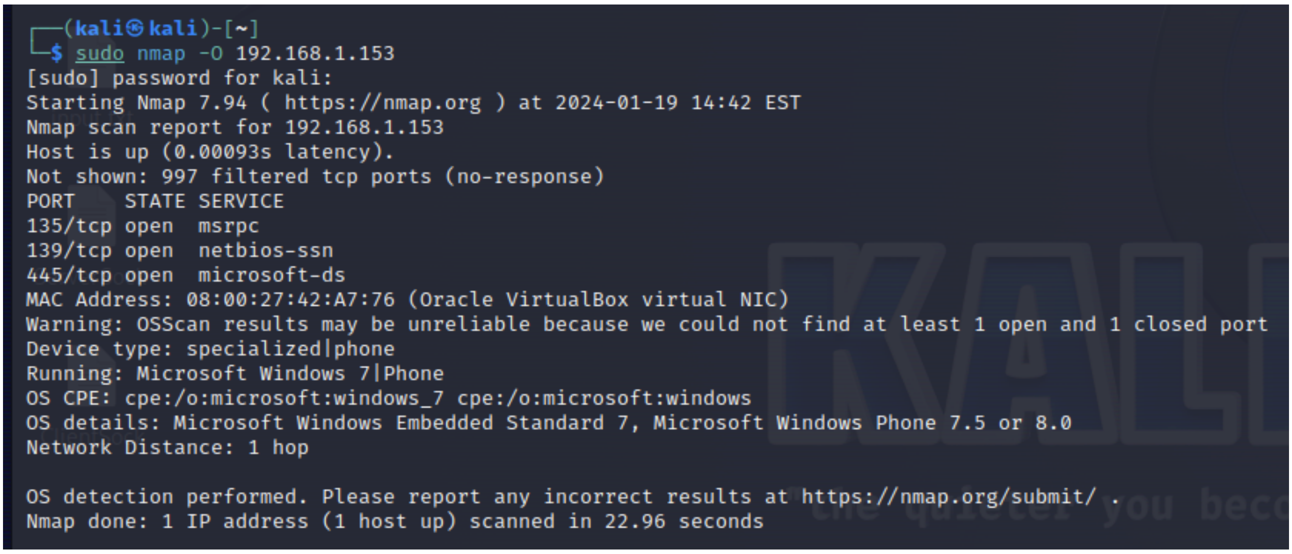
Tecniche di scansione con Nmap
Si richiede allo studente di effettuare le seguenti scansioni sul target Windows 7:
OS fingerprint
Syn Scan
Version detection

Svolgimento:



```
Microsoft Windows [Versione 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Tutti i diritti riservati.

C:\Users\vboxuser>ipconfig

Configurazione IP di Windows


Scheda Ethernet Connessione alla rete locale (LAN):

   Suffisso DNS specifico per connessione:
   Indirizzo IPv6 locale rispetto al collegamento . : fe80::180a:1a82:4ee7:43b6%
11
   Indirizzo IPv4. . . . . . . . . . . . : 192.168.1.153
   Subnet mask . . . . . . . . . . . . . : 255.255.255.0
   Gateway predefinito . . . . . . . . . : 192.168.1.1

Scheda Tunnel isatap.{C4EDF30B-43D1-4E20-8B6C-698116177377}:

   Stato supporto. . . . . . . . . . . . : Supporto disconnesso
   Suffisso DNS specifico per connessione:

C:\Users\vboxuser>_
```

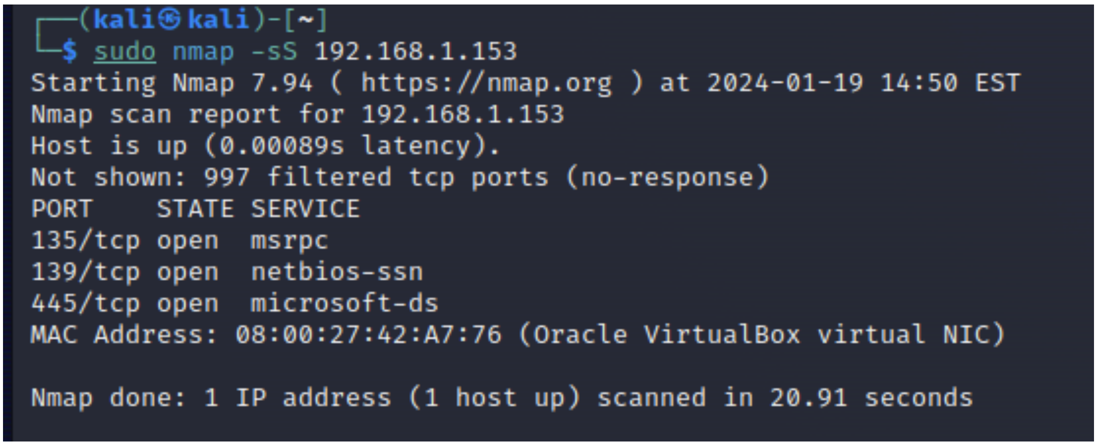
Scansione con “nmap -O” sul target Windows 7 “192.168.1.153”



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.1.153
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 14:42 EST
Nmap scan report for 192.168.1.153
Host is up (0.00093s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 08:00:27:42:A7:76 (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 22.96 seconds
```

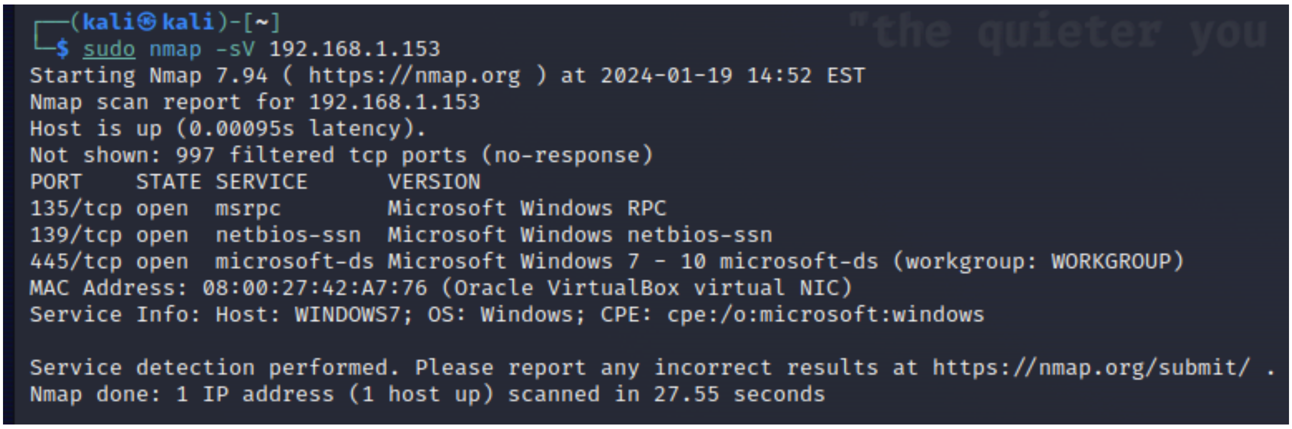
Abbiamo in questo caso un riscontro positivo sul S.O. della macchina target

Scansione con “nmap -sS” sul target Windows 7 “192.168.1.153”



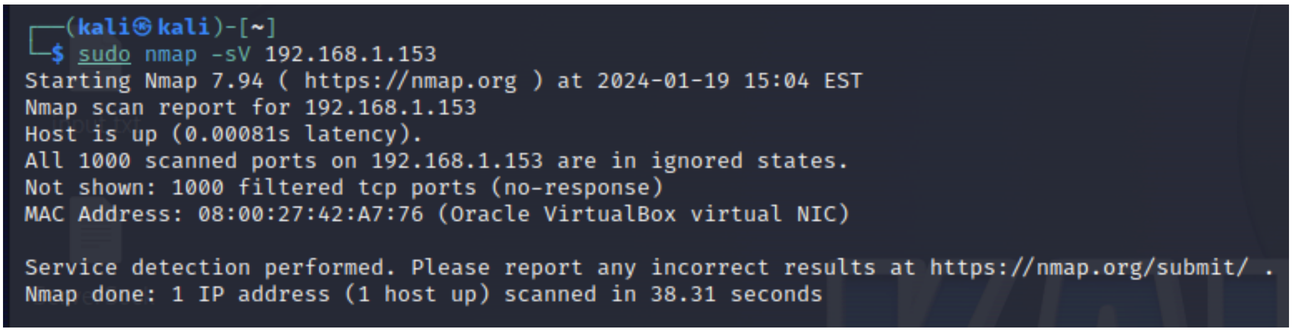
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.1.153
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 14:50 EST
Nmap scan report for 192.168.1.153
Host is up (0.00089s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 08:00:27:42:A7:76 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 20.91 seconds
```

Scansione con “nmap -sV” sul target Windows 7 “192.168.1.153”



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.1.153
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 14:52 EST
Nmap scan report for 192.168.1.153
Host is up (0.00095s latency).
Not shown: 997 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)
MAC Address: 08:00:27:42:A7:76 (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 27.55 seconds
```

Dopo aver disabilitato la regola creata per consentire le connessioni in ingresso proviamo ad eseguire nuovamente la scansione con il Version ma come vediamo non va a buon fine



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.1.153
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 15:04 EST
Nmap scan report for 192.168.1.153
Host is up (0.00081s latency).
All 1000 scanned ports on 192.168.1.153 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:42:A7:76 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 38.31 seconds
```