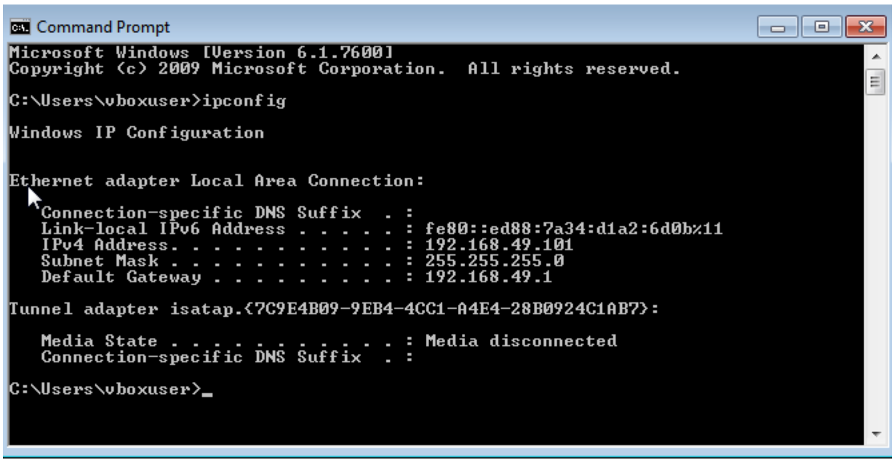
Esercitazione 7 Modulo 3 – Alessio Russo

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

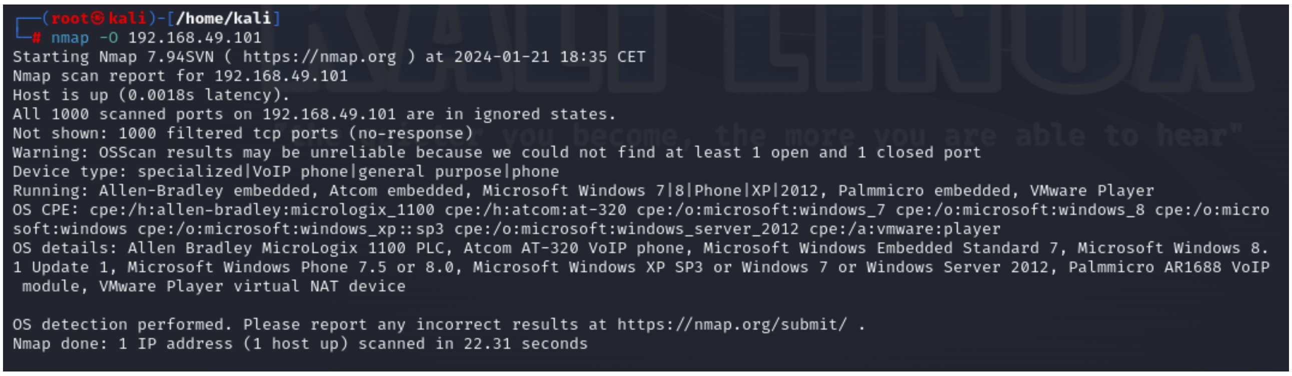
- OS fingerprint
- Syn Scan
- Version detection

IP Windows tramite prompt dei comandi digitare ipconfig



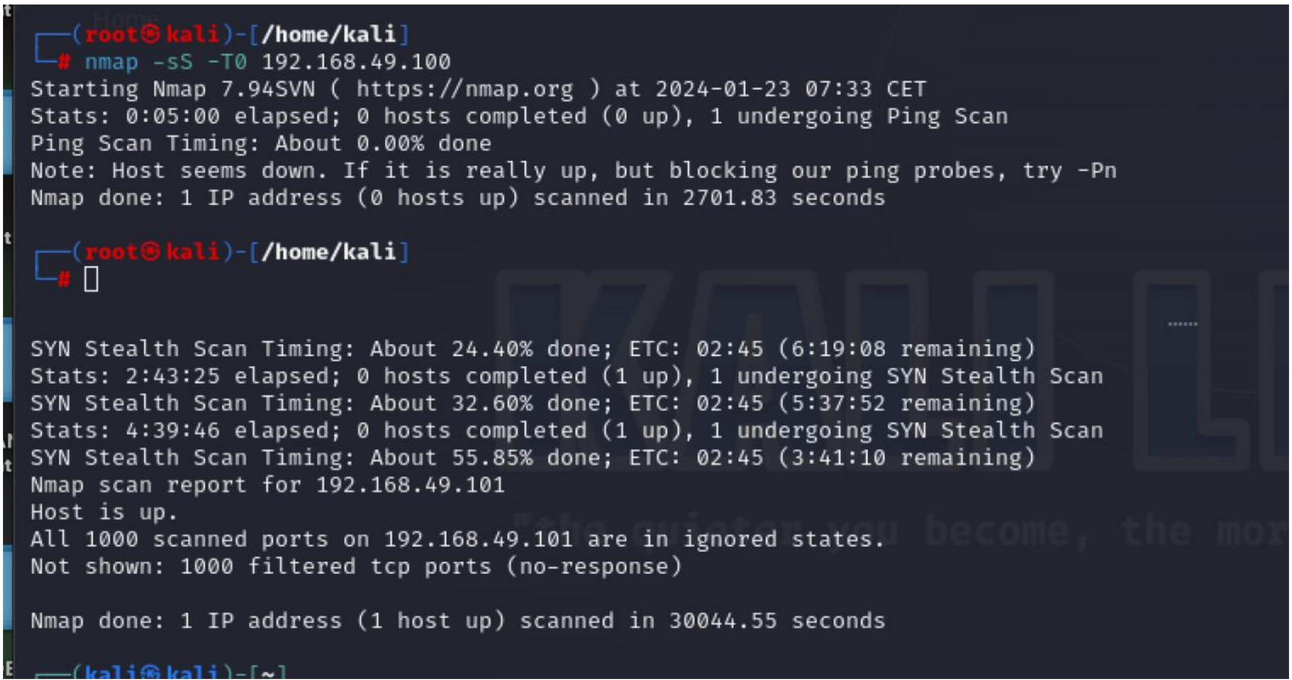
```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\vboxuser>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::ed88:7a34:d1a2:6d0b%11
   IPv4 Address. . . . . . . . . . . : 192.168.49.101
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.49.1

Tunnel adapter isatap.{7C9E4B09-9EB4-4CC1-A4E4-28B0924C1AB7}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\vboxuser>_
```

- nmap -O: Os Fingerprinting

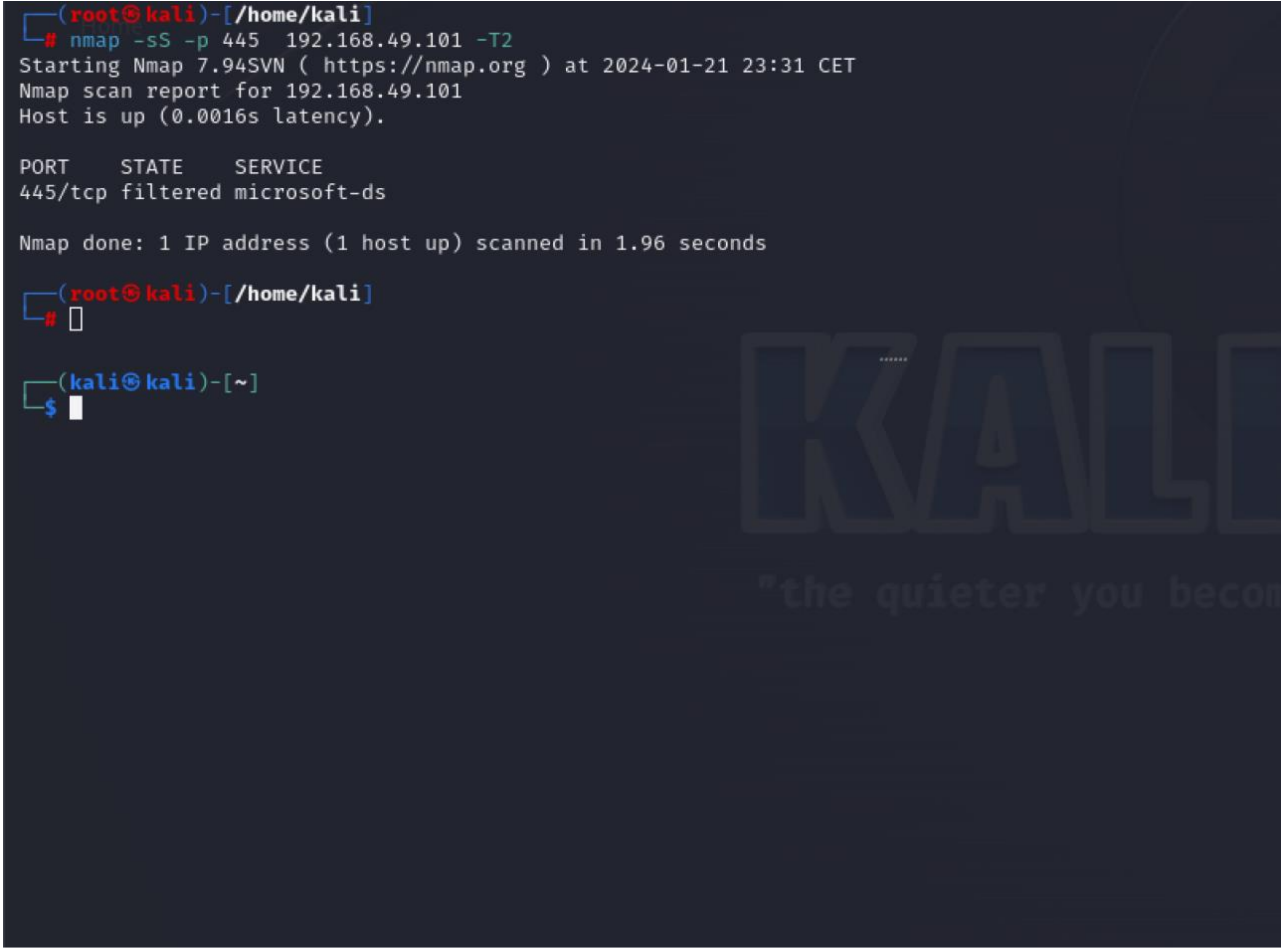


```
┌──(root㉿kali)-[/home/kali]
└─# nmap -O 192.168.49.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-21 18:35 CET
Nmap scan report for 192.168.49.101
Host is up (0.0018s latency).
All 1000 scanned ports on 192.168.49.101 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized|VoIP phone|general purpose|phone
Running: Allen-Bradley embedded, Atcom embedded, Microsoft Windows 7|8|Phone|XP|2012, Palmmicro embedded, VMware Player
OS CPE: cpe:/h:allen-bradley:micrologix_1100 cpe:/h:atcom:at-320 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_8 cpe:/o:micro
soft:windows cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_server_2012 cpe:/a:vmware:player
OS details: Allen Bradley MicroLogix 1100 PLC, Atcom AT-320 VoIP phone, Microsoft Windows Embedded Standard 7, Microsoft Windows 8.
1 Update 1, Microsoft Windows Phone 7.5 or 8.0, Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012, Palmmicro AR1688 VoIP
 module, VMware Player virtual NAT device

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.31 seconds
```

- nmap -sS: Syn Scan



```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS -T0 192.168.49.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-23 07:33 CET
Stats: 0:05:00 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Ping Scan Timing: About 0.00% done
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 2701.83 seconds

┌──(root㉿kali)-[/home/kali]
└─# ▯


SYN Stealth Scan Timing: About 24.40% done; ETC: 02:45 (6:19:08 remaining)
Stats: 2:43:25 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 32.60% done; ETC: 02:45 (5:37:52 remaining)
Stats: 4:39:46 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 55.85% done; ETC: 02:45 (3:41:10 remaining)
Nmap scan report for 192.168.49.101
Host is up.
All 1000 scanned ports on 192.168.49.101 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 30044.55 seconds

┌──(kali㉿kali)-[~]
```



```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS -p 445  192.168.49.101 -T2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-21 23:31 CET
Nmap scan report for 192.168.49.101
Host is up (0.0016s latency).

PORT    STATE    SERVICE
445/tcp filtered microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 1.96 seconds

┌──(root㉿kali)-[/home/kali]
└─# ▯

┌──(kali㉿kali)-[~]
└─$ █
```

Scansione con nmap con switch -T0 non ci dice nulla in quanto il firewall effettua la sua funzione di filtro