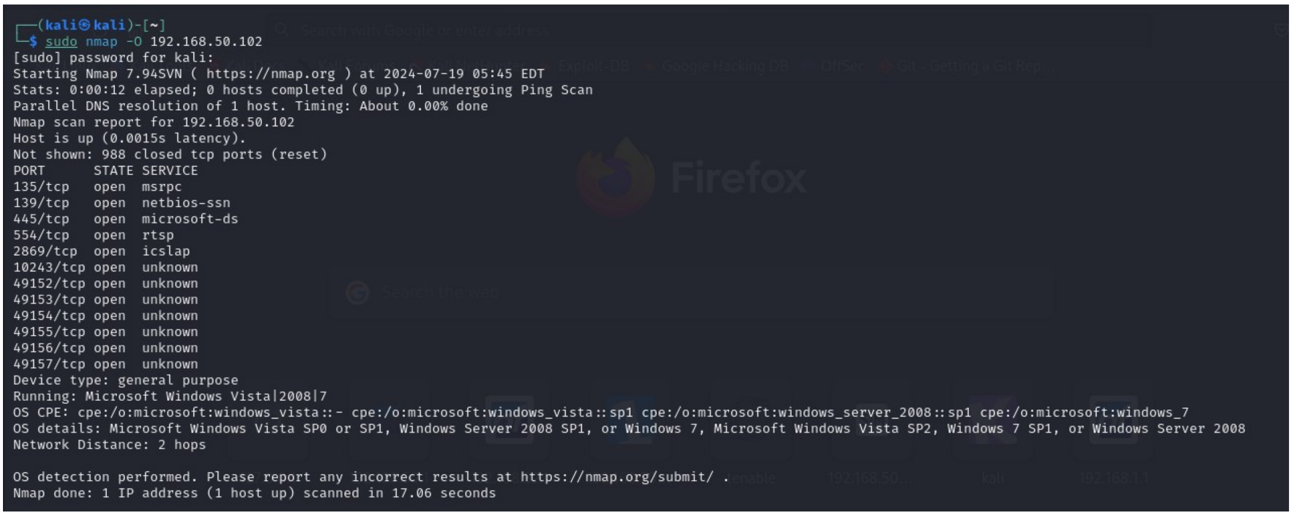
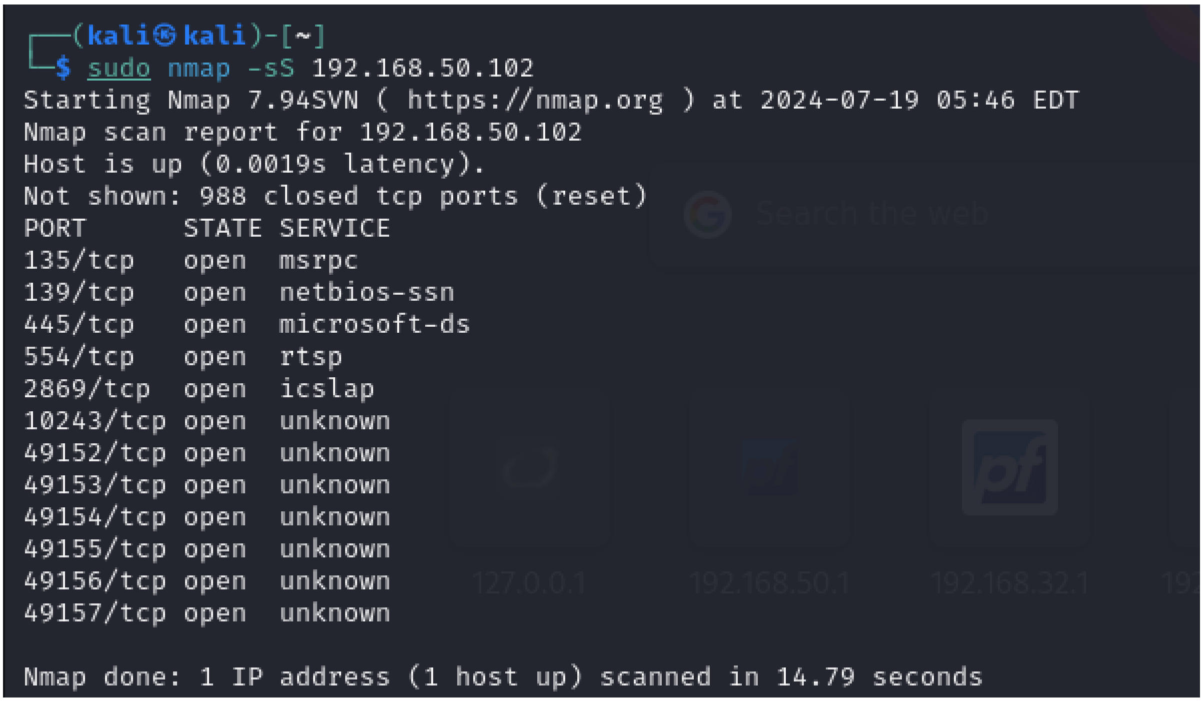
Consegna M3 – Week 11 – Day 4 – Daniele Rufo

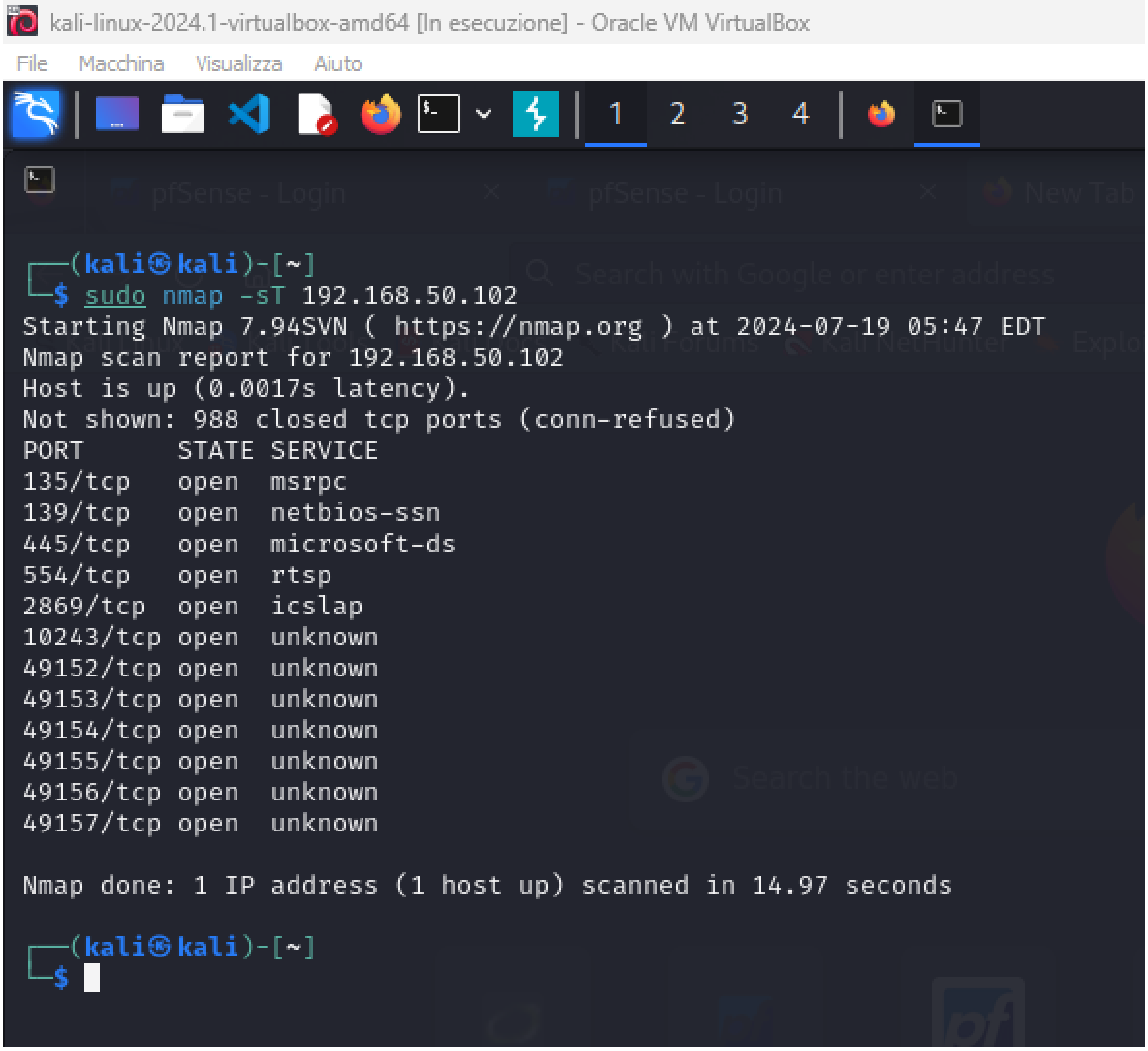
Ho eseguito i vari scan con i comandi proposti sulla macchina wnìindows7. Le macchine sono su reti differenti e utilizzano pfsense come gateway. Propongo gli screenshot dei vari comandi



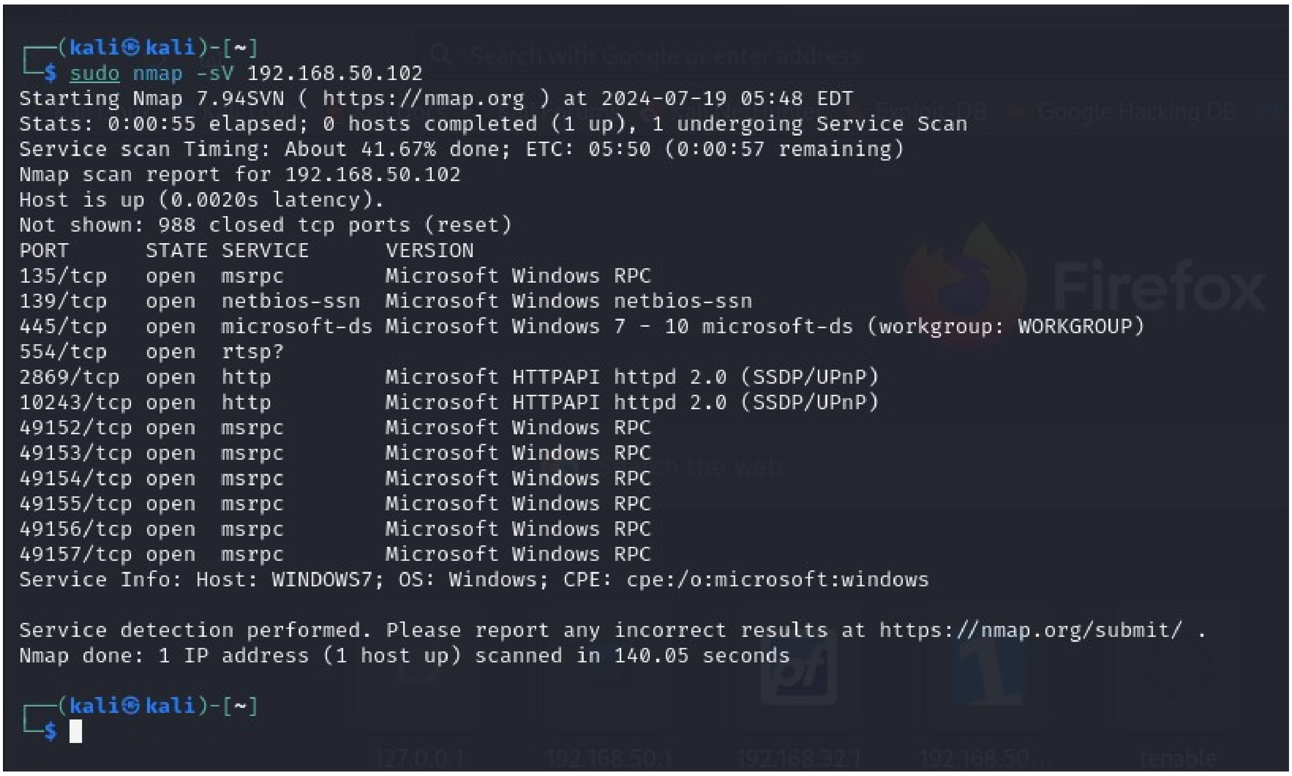
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.50.102
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-19 05:45 EDT
Stats: 0:00:12 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Nmap scan report for 192.168.50.102
Host is up (0.0015s latency).
Not shown: 988 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  icslap
10243/tcp open  unknown
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, Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008
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 17.06 seconds
```



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-19 05:46 EDT
Nmap scan report for 192.168.50.102
Host is up (0.0019s latency).
Not shown: 988 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  icslap
10243/tcp open  unknown
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 14.79 seconds
```


kali-linux-2024.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
File
Macchina
Visualizza
Aiuto
1
2
3
4

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-19 05:47 EDT
Nmap scan report for 192.168.50.102
Host is up (0.0017s latency).
Not shown: 988 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  icslap
10243/tcp open  unknown
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 14.97 seconds

┌──(kali㉿kali)-[~]
└─$ 
```



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-19 05:48 EDT
Stats: 0:00:55 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 41.67% done; ETC: 05:50 (0:00:57 remaining)
Nmap scan report for 192.168.50.102
Host is up (0.0020s latency).
Not shown: 988 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)
554/tcp   open  rtsp?
2869/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
10243/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
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 140.05 seconds

┌──(kali㉿kali)-[~]
└─$ 
```