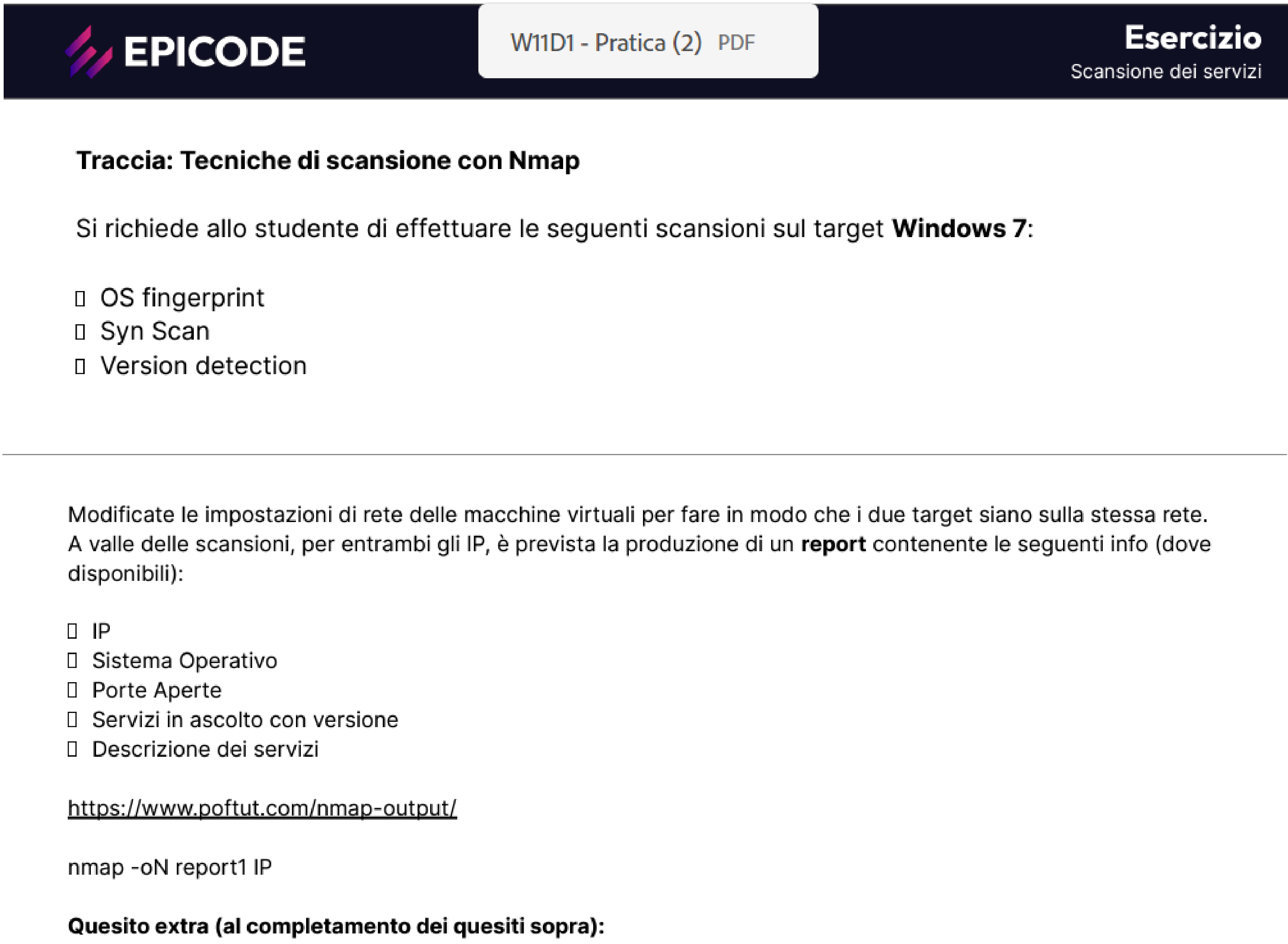
W11D1 pratica 2

Giacomo di Giacinto



EPICODE

W11D1 - Pratica (2) PDF

Esercizio

Scansione dei servizi

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

Modificate le impostazioni di rete delle macchine virtuali per fare in modo che i due target siano sulla stessa rete. A valle delle scansioni, per entrambi gli IP, è prevista la produzione di un **report** contenente le seguenti info (dove disponibili):

□ IP
□ Sistema Operativo
□ Porte Aperte
□ Servizi in ascolto con versione
□ Descrizione dei servizi

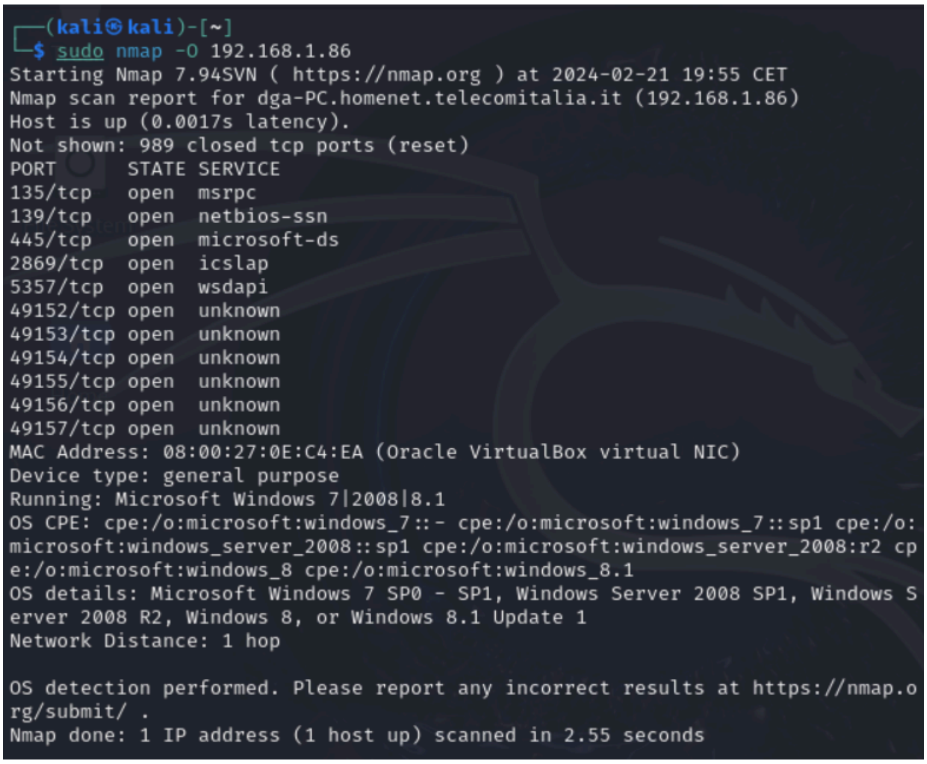
https://www.poftut.com/nmap-output/

nmap -oN report1 IP

Quesito extra (al completamento dei quesiti sopra):

Di seguito elenco le tre scansioni indicate nella traccia dell’esercizio con il firewall di Windows disattivato

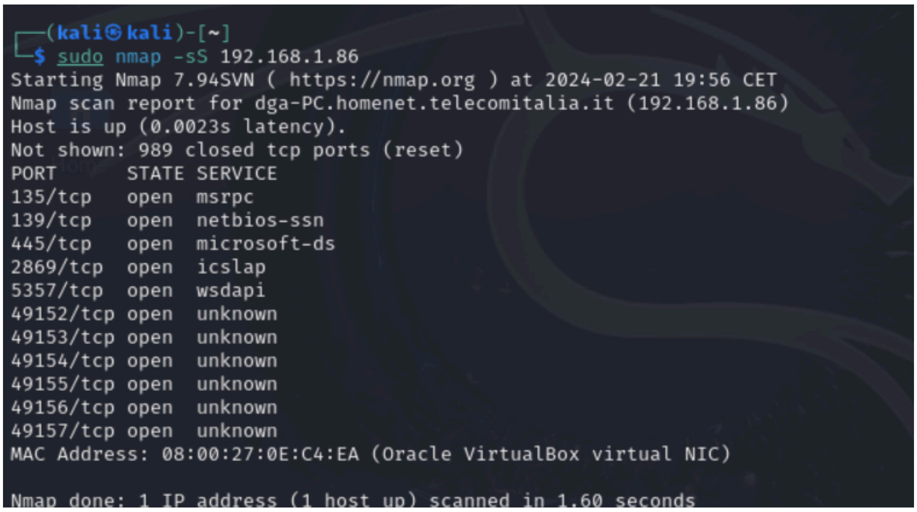
Os fingerprint



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.1.86
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 19:55 CET
Nmap scan report for dga-PC.homenet.telecomitalia.it (192.168.1.86)
Host is up (0.0017s latency).
Not shown: 989 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
2869/tcp  open  icslap
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: 08:00:27:0E:C4:EA (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 2.55 seconds
```

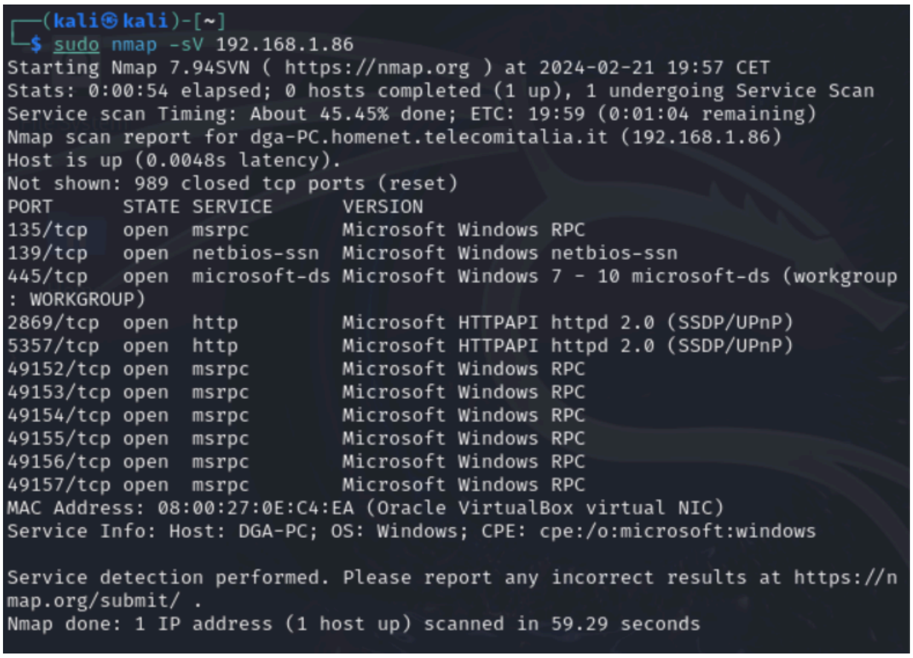
Syn scan



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.1.86
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 19:56 CET
Nmap scan report for dga-PC.homenet.telecomitalia.it (192.168.1.86)
Host is up (0.0023s latency).
Not shown: 989 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
2869/tcp  open  icslap
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: 08:00:27:0E:C4:EA (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.60 seconds
```

Version detection

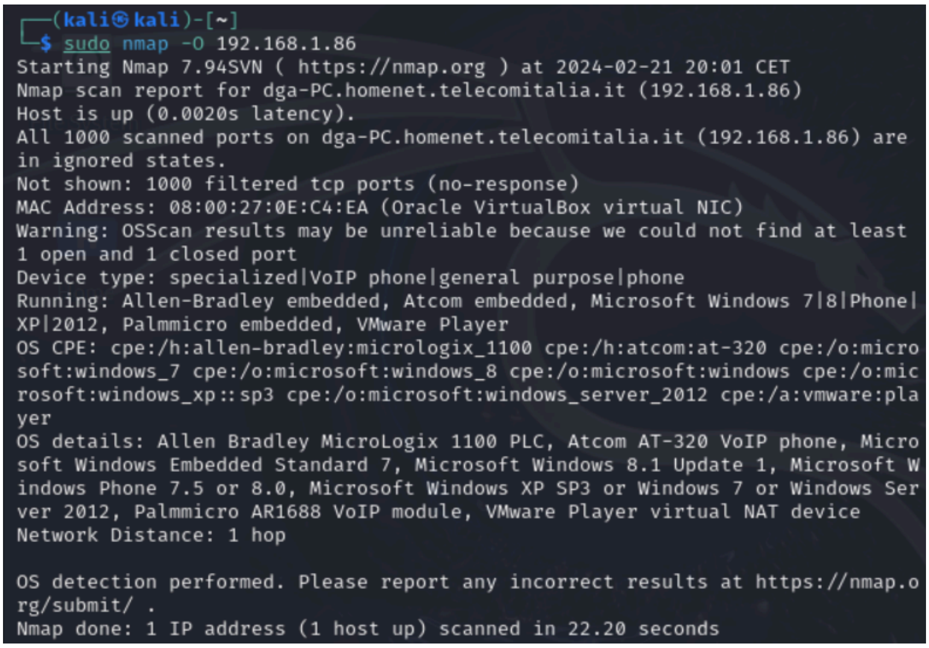


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.1.86
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 19:57 CET
Stats: 0:00:54 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 45.45% done; ETC: 19:59 (0:01:04 remaining)
Nmap scan report for dga-PC.homenet.telecomitalia.it (192.168.1.86)
Host is up (0.0048s latency).
Not shown: 989 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)
2869/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
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: 08:00:27:0E:C4:EA (Oracle VirtualBox virtual NIC)
Service Info: Host: DGA-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 59.29 seconds
```

Di seguito elenco le tre scansioni effettuate in precedenza ma con il firewall di windows attivo

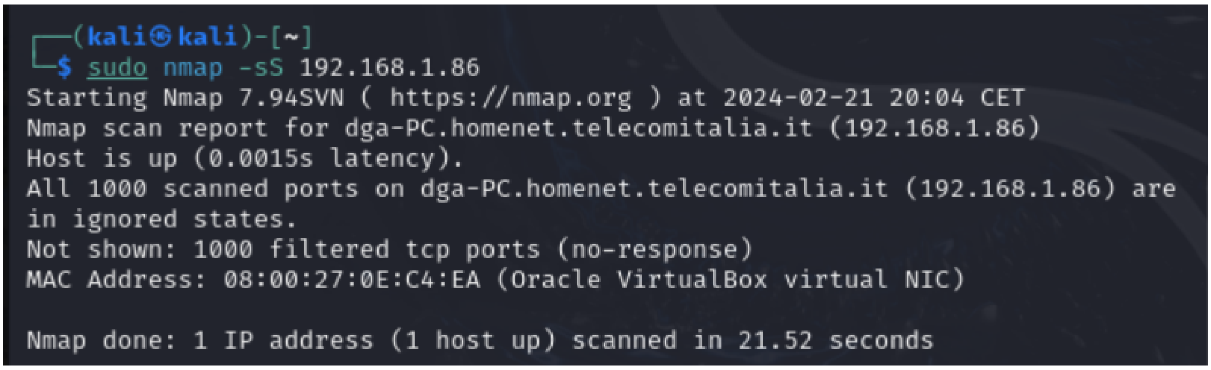
Os fingerprint



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.1.86
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 20:01 CET
Nmap scan report for dga-PC.homenet.telecomitalia.it (192.168.1.86)
Host is up (0.0020s latency).
All 1000 scanned ports on dga-PC.homenet.telecomitalia.it (192.168.1.86) are
in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:0E:C4:EA (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|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:micro
soft:windows_7 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows cpe:/o:mic
rosoft:windows_xp::sp3 cpe:/o:microsoft:windows_server_2012 cpe:/a:vmware:pla
yer
OS details: Allen Bradley MicroLogix 1100 PLC, Atcom AT-320 VoIP phone, Micro
soft Windows Embedded Standard 7, Microsoft Windows 8.1 Update 1, Microsoft W
indows Phone 7.5 or 8.0, Microsoft Windows XP SP3 or Windows 7 or Windows Ser
ver 2012, Palmmicro AR1688 VoIP module, VMware Player virtual NAT device
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 22.20 seconds
```

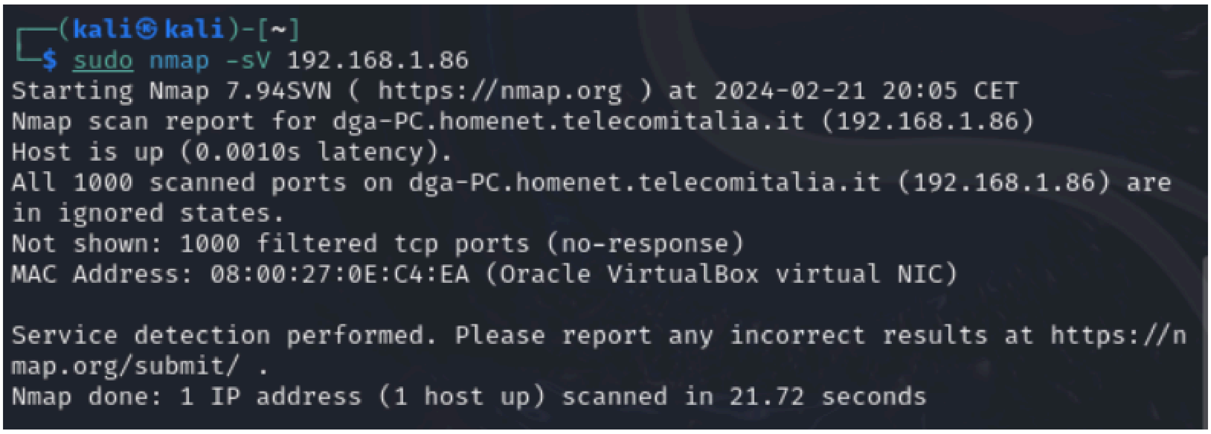
Syn scan



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.1.86
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 20:04 CET
Nmap scan report for dga-PC.homenet.telecomitalia.it (192.168.1.86)
Host is up (0.0015s latency).
All 1000 scanned ports on dga-PC.homenet.telecomitalia.it (192.168.1.86) are
in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:0E:C4:EA (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 21.52 seconds
```

Version detection



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.1.86
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 20:05 CET
Nmap scan report for dga-PC.homenet.telecomitalia.it (192.168.1.86)
Host is up (0.0010s latency).
All 1000 scanned ports on dga-PC.homenet.telecomitalia.it (192.168.1.86) are
in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:0E:C4:EA (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.72 seconds
```

Per l’esecuzione dell’esercizio sono stati assegnati degli IP in DHCP e le schede di rete delle macchine sono state impostate in brigde; alla macchina Kali linux è stato assegnato l’indirizzo 192.168.1.100 mentre alla macchina Windows 7 è stato assegnato l’IP 192.168.1.86.

Dal comando OS fingerprint <sudo nano -O 192.168.1.86> si nota che il sistema operativo è Windows 7|2008|8.1

Dalle scansioni effettuate col firewall spento vengono evidenziate le porte aperte; dalla scansione version detection si notano, oltre le porte aperte, anche le versioni di ogni servizio.

Per concludere, noto una grande differenza tra le scansioni effettuate col firewall attivo rispetto alle scansioni effettuate col firewall spento. Il firewall riesce a bloccare tutte le scansioni e non mi permette di conoscere alcuna informazione sulla macchina target Windows 7.