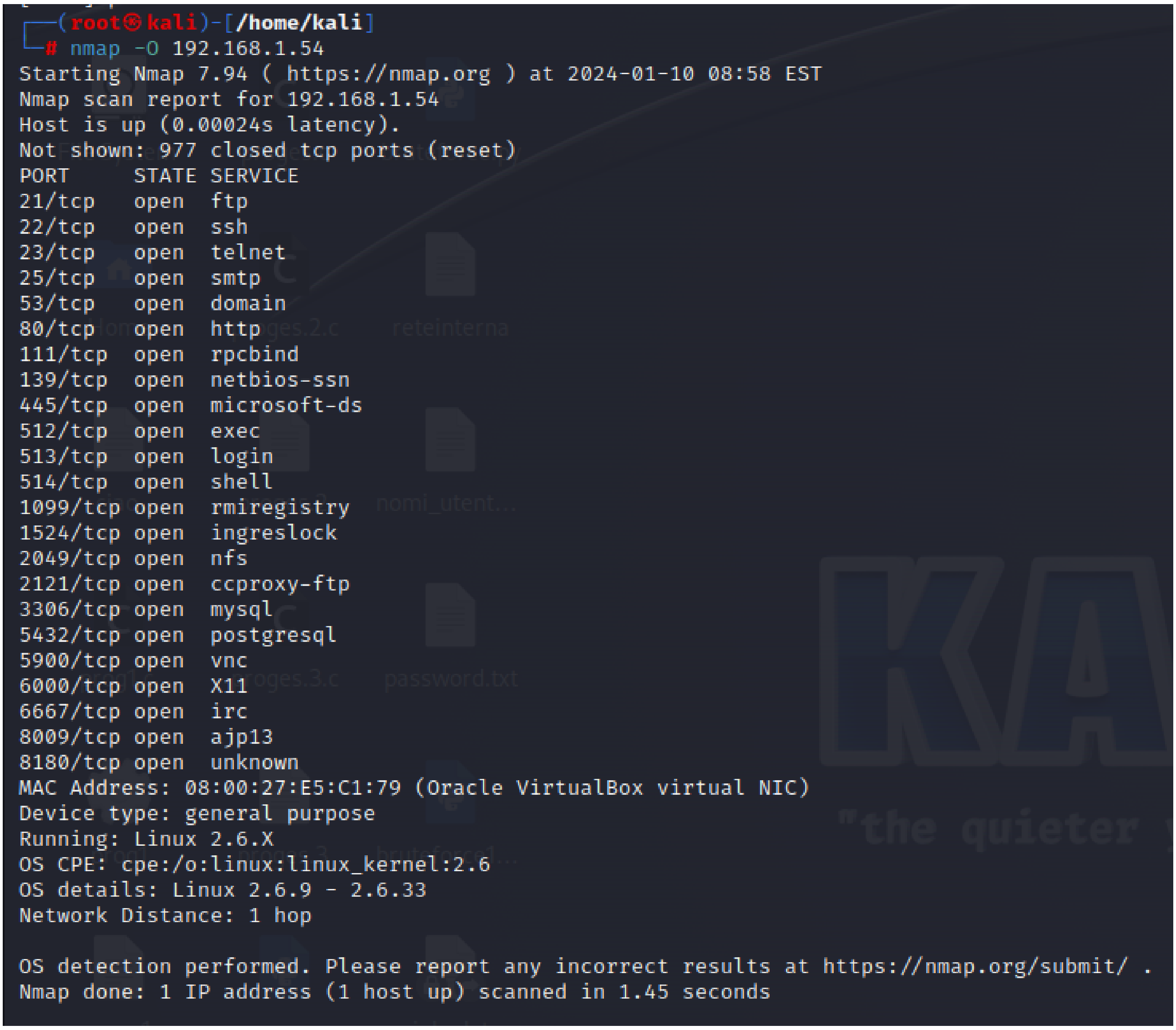
Viene richiesto di effettuare le seguenti scansioni sul target Metasploitable:

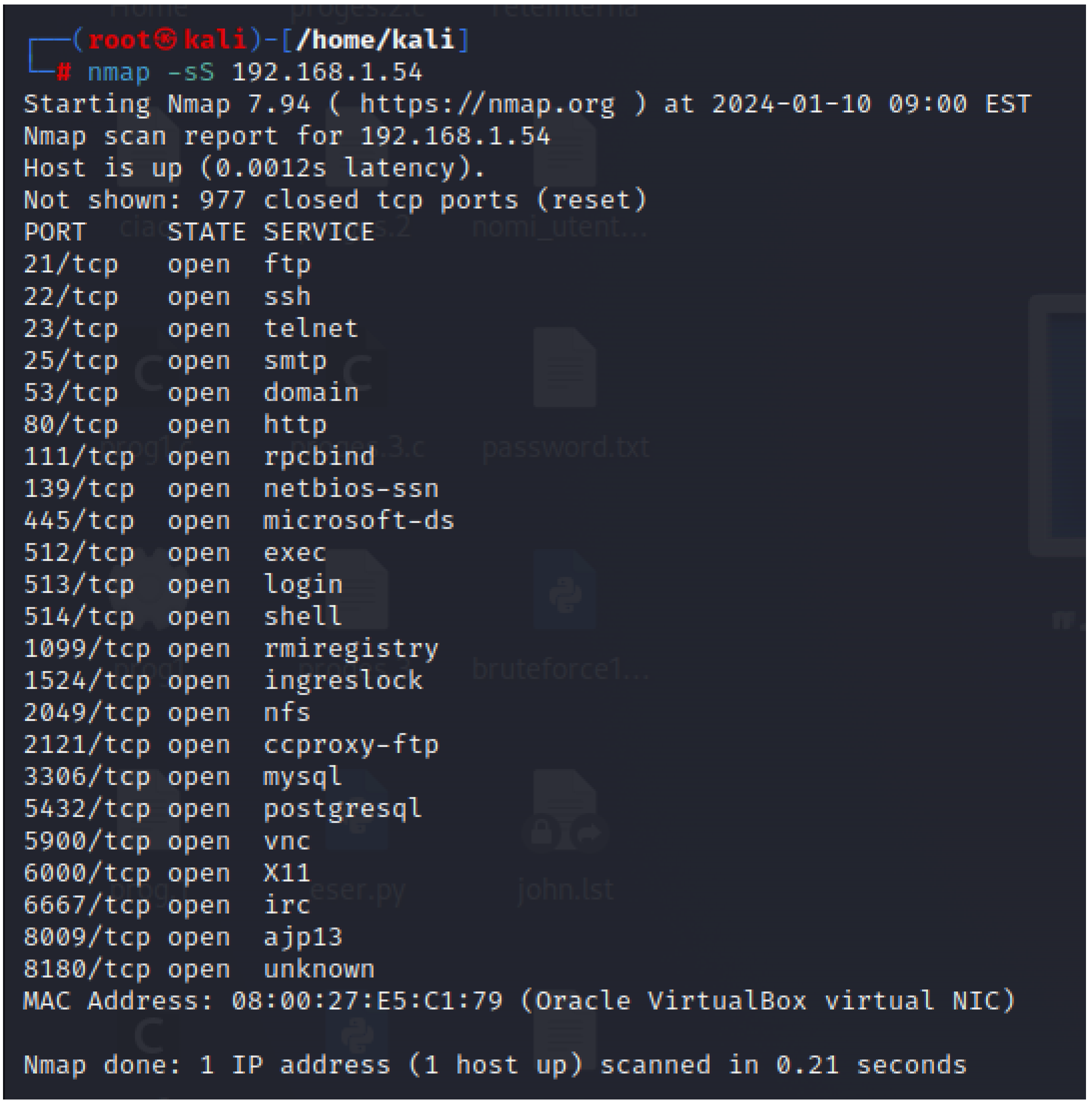
- **OS fingerprint**



```
┌──(root㉿kali)-[/home/kali]
└─# nmap -O 192.168.1.54
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-10 08:58 EST
Nmap scan report for 192.168.1.54
Host is up (0.00024s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:E5:C1:79 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
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 1.45 seconds
```

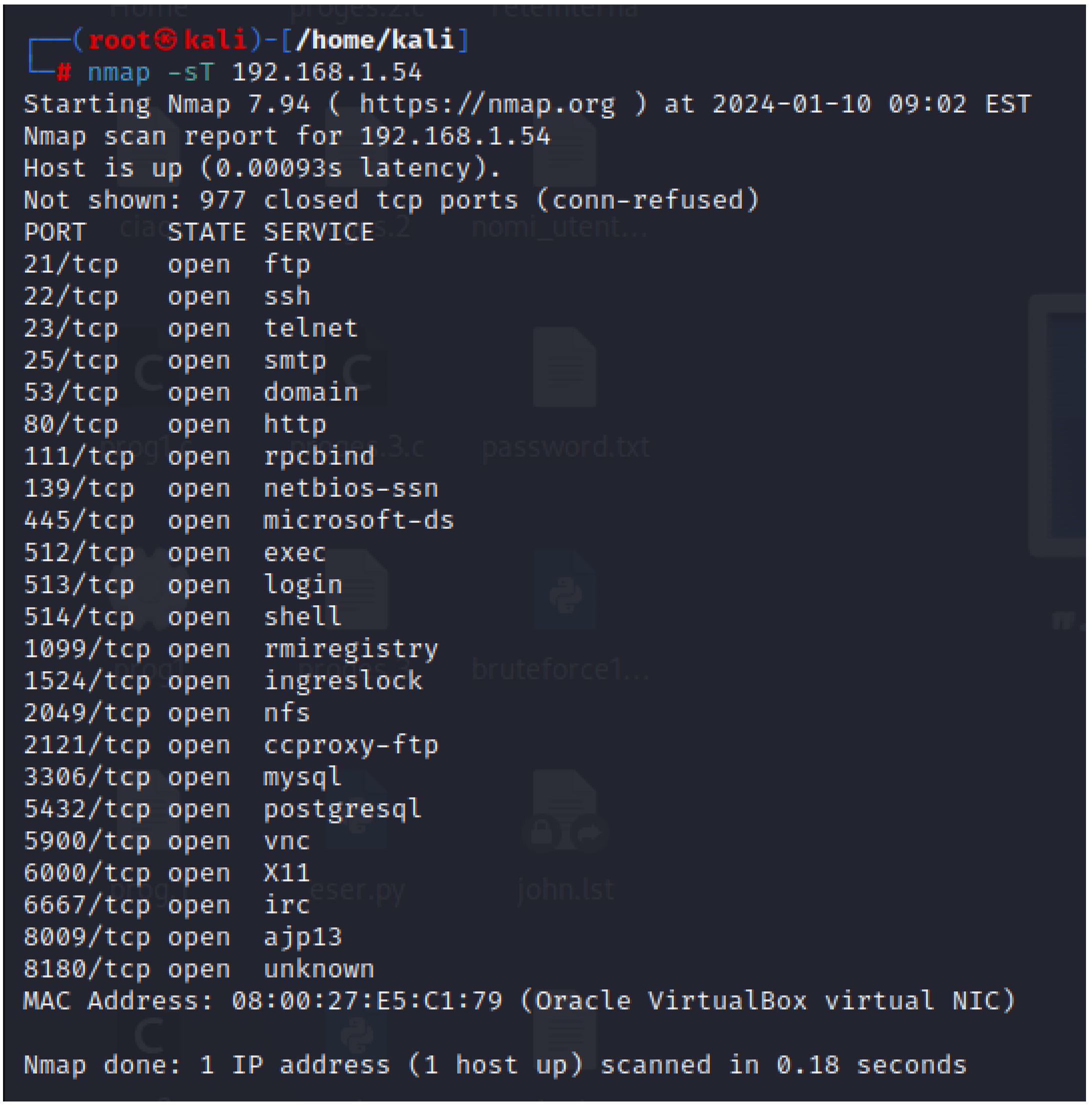
- **Syn Scan**



```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS 192.168.1.54
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-10 09:00 EST
Nmap scan report for 192.168.1.54
Host is up (0.0012s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:E5:C1:79 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds
```

- **TCP connect**

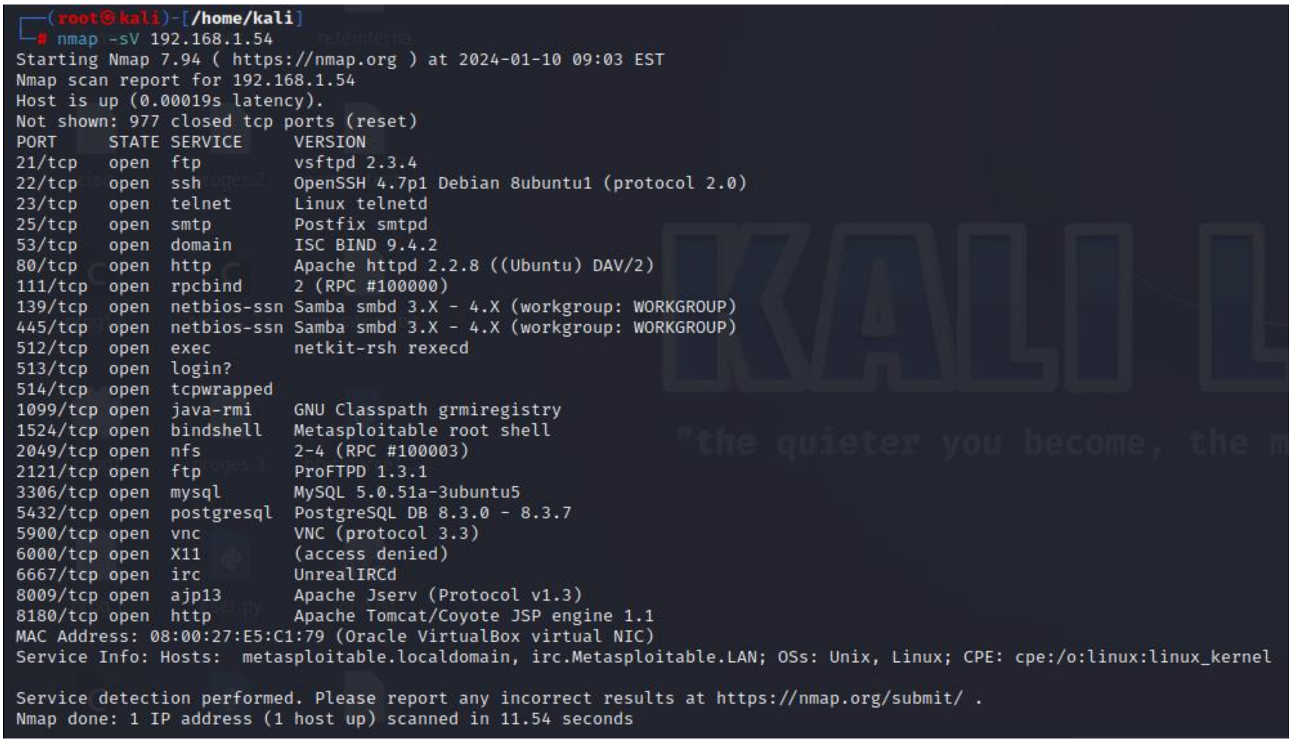


```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sT 192.168.1.54
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-10 09:02 EST
Nmap scan report for 192.168.1.54
Host is up (0.00093s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:E5:C1:79 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds
```

Non ci sono evidenti differenze fra le scansioni TCP e SYN. Tuttavia *-sT* è molto più invasiva rispetto a *-sS*, in quanto deve necessariamente fare tutte e 3 le strette di mano (*-sS* fa solo SYN).

- **Version detection**

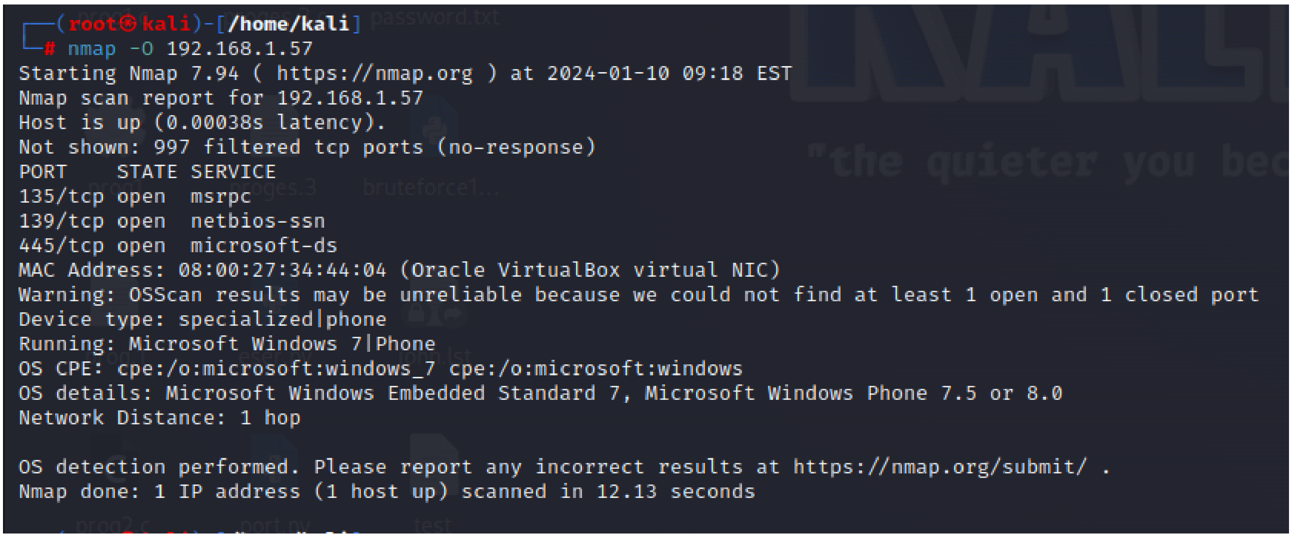


```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.1.54
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-10 09:03 EST
Nmap scan report for 192.168.1.54
Host is up (0.00019s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:E5:C1:79 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.54 seconds
```

E la seguente sul target Windows 7:

- **OS fingerprint**



```
┌──(root㉿kali)-[/home/kali]
└─# nmap -O 192.168.1.57
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-10 09:18 EST
Nmap scan report for 192.168.1.57
Host is up (0.00038s 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: 08:00:27:34:44:04 (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 12.13 seconds
```

Per quanto riguarda Metasploitable:

indirizzo ip:

192.168.1.54

Sistema Operativo:

Linux 2.6.9-2.6.33

Porte aperte:

21, 22, 23, 25, 53, 80, 111, 139, 445, 512, 513, 514, 1099, 1524, 2049, 2121, 3306, 5432, 5900, 6000, 6667, 8009, 8180

Servizi in ascolto con versione:

- ftp vsftpd 2.3.4
- ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
- telnet Linux telnetd
- smtp Postfix smtpd
- domain ISC BIND 9.4.2
- http Apache httpd 2.2.8 ((Ubuntu) DAV/2)
- rpcbind 2 (RPC #100000)
- netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
- netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
- exec netkit-rsh rexecd
- login?
- tcpwrapped
- java-rmi GNU Classpath grmiregistry
- bindshell Metasploitable root shell
- nfs 2-4 (RPC #100003)
- ftp ProFTPD 1.3.1
- mysql MySQL 5.0.51a-3ubuntu5
- postgresql PostgreSQL DB 8.3.0 - 8.3.7
- vnc VNC (protocol 3.3)
- X11 (access denied)
- irc UnrealIRCd
- ajp13 Apache Jserv (Protocol v1.3)
- http Apache Tomcat/Coyote JSP engine 1.1

Per quanto riguarda Windows 7:

Indirizzo ip:

192.168.1.57

Sistema Operativo:

Microsoft Windows Embedded Standard 7, Microsoft Windows Phone 7.5 or 8.0

Porte aperte:

135, 139, 445

Servizi in ascolto con versione (ho eseguito il comando “ *nmap -sV* ” sull’ ip del dispositivo con Windows 7 (*192.168.1.57*))**:**

- msrpc   Microsoft Windows RPC
- netbios-ssn Microsoft Windows netbios-ssn
- microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)

Su Windows 7 il firewall potrebbe bloccare alcune scansioni (porte, servizi, ecc…). Per eludere questo, possiamo andare sul dispositivo con Windows 7, andare a modificare le impostazioni avanzate del Windows Firewall, cercando fra le Inbound Rule la regola chiamata “File and Printer Sharing (Echo Request - ICMPv4-In)”. Clicchiamo la regola con il tasto desto e selezioniamo “Abilita Regola”.