

1. Traccia**2. Soluzione****2.1 OS fingerprint****2.2 Syn Scan****2.3 TCP connect****2.4 Version Detection****2.5 Report finale tramite nmap****2.6 OS fingerprint WINDOWS**

1. Traccia

Tecniche di scansione con Nmap

Si richiede allo studente di effettuare le seguenti scansioni sul target Metasploitable:

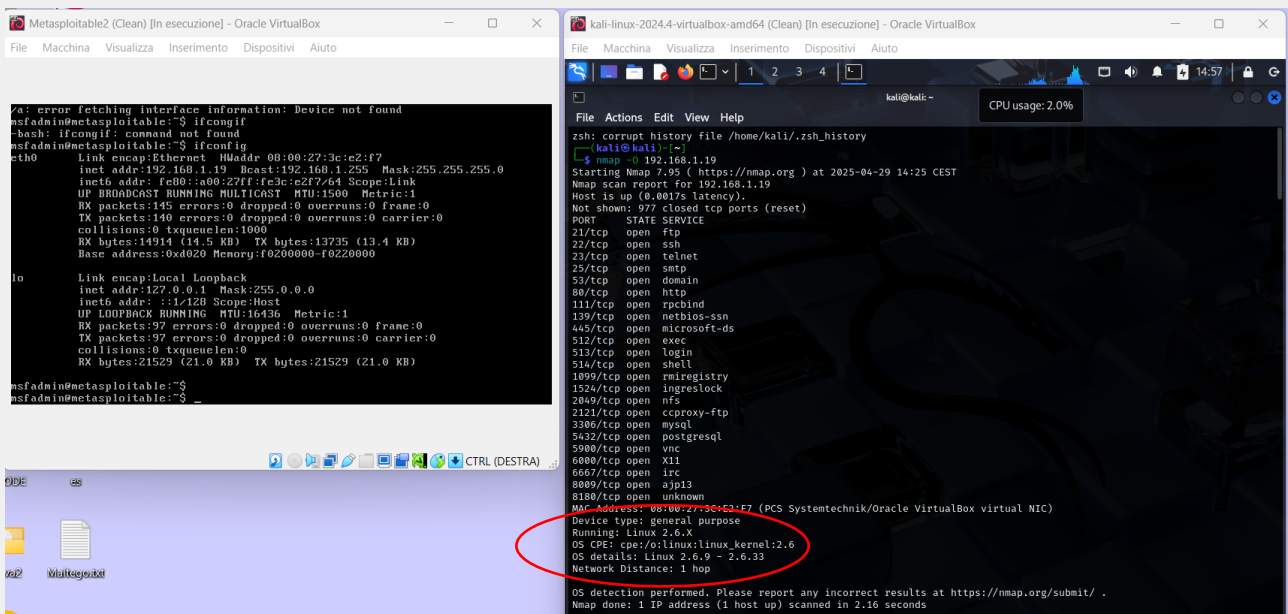
- OS fingerprint
- Syn Scan
- TCP connect - trovate differenze tra i risultati delle scansioni TCP connect e SYN?
- Version detection.

E la seguente sul target Windows:

- OS fingerprint

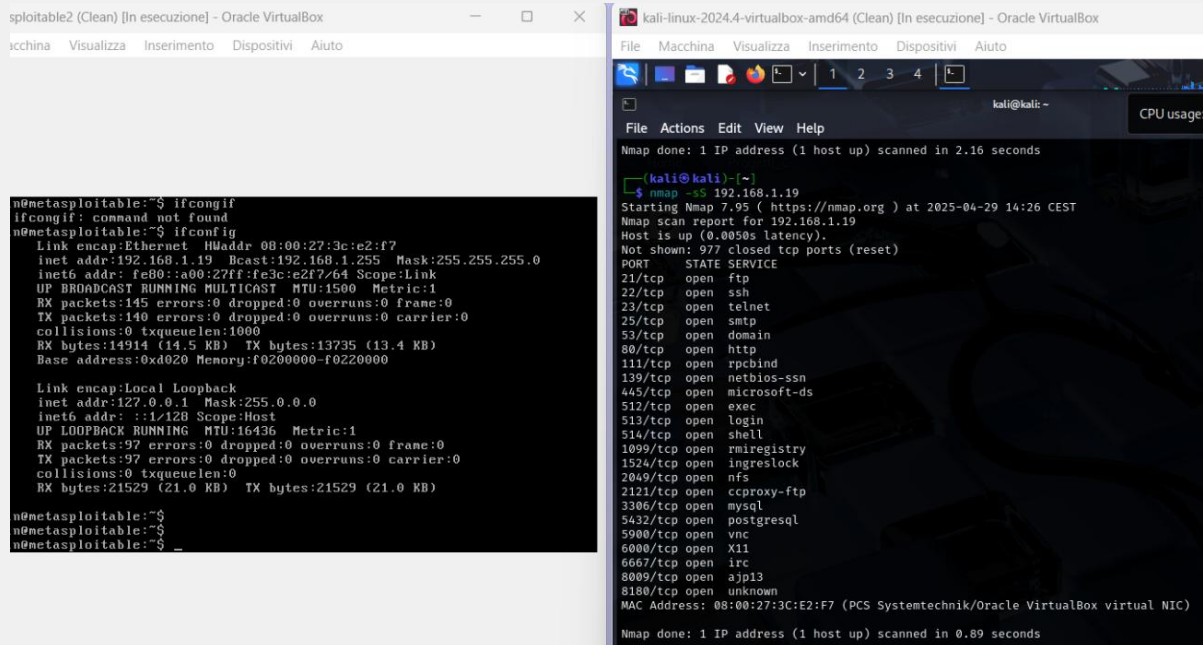
2. Soluzione

2.1 OS fingerprint



A sinistra l'IP della macchina di Metasploitable. A destra, da Kali Linux, il comando nmap -O con IP di Metasploitable per ottenere info sul sistema operativo.

2.2 Syn Scan



```
n@metasploitable:~$ ifconfig
ifconfig: command not found
n@metasploitable:~$ ifconfig
Link encap:Ethernet HWaddr 08:00:27:3c:e2:f7
inet addr:192.168.1.19 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:fe3c:e2f7/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:145 errors:0 dropped:0 overruns:0 frame:0
TX packets:140 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:14914 (14.5 KB) TX bytes:13735 (13.4 KB)
Base address:0xd020 Memory:f0200000-f0220000

Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:97 errors:0 dropped:0 overruns:0 frame:0
TX packets:97 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:21529 (21.0 KB) TX bytes:21529 (21.0 KB)

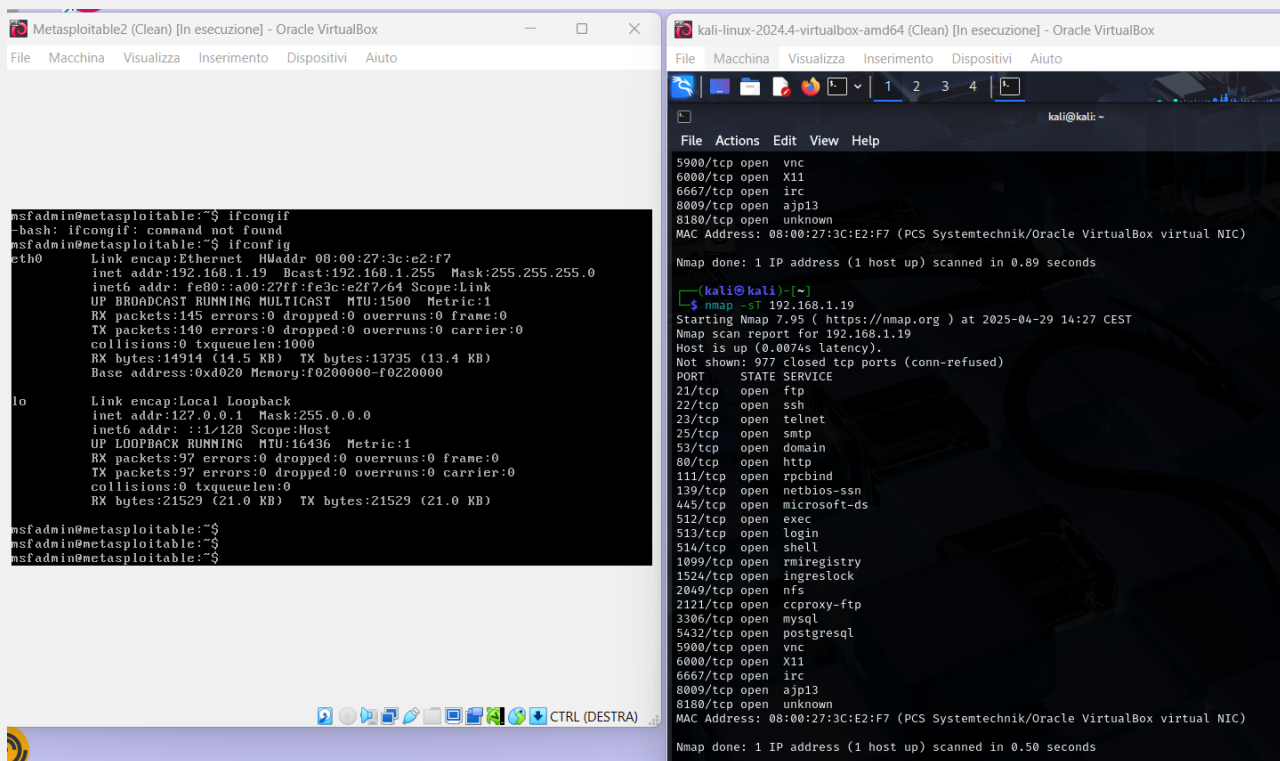
n@metasploitable:~$
n@metasploitable:~$
n@metasploitable:~$ _
```

```
kali@kali:~$ nmap -sS 192.168.1.19
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 14:26 CEST
Nmap scan report for 192.168.1.19
Host is up (0.0050s 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: 08:00:27:3C:E2:F7 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.89 seconds
```

A sinistra l'IP della macchina di Metasploitable. A destra, da Kali Linux, il comando `nmap -sS` con IP di Metasploitable per ottenere info sulle porte e servizi aperti.

2.3 TCP connect



```

msfadmin@metasploitable:~$ ifconfig
-bash: ifconfig: command not found
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:3c:e2:f7
          inet addr:192.168.1.19  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe3c:e2f7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:145 errors:0 dropped:0 overruns:0 frame:0
          TX packets:140 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:14914 (14.5 KB)  TX bytes:13735 (13.4 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:97 errors:0 dropped:0 overruns:0 frame:0
          TX packets:97 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:21529 (21.0 KB)  TX bytes:21529 (21.0 KB)

msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$

kali@kali:~$ nmap -sT 192.168.1.19
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 14:27 CEST
Nmap scan report for 192.168.1.19
Host is up (0.0074s 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: 08:00:27:3C:E2:F7 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

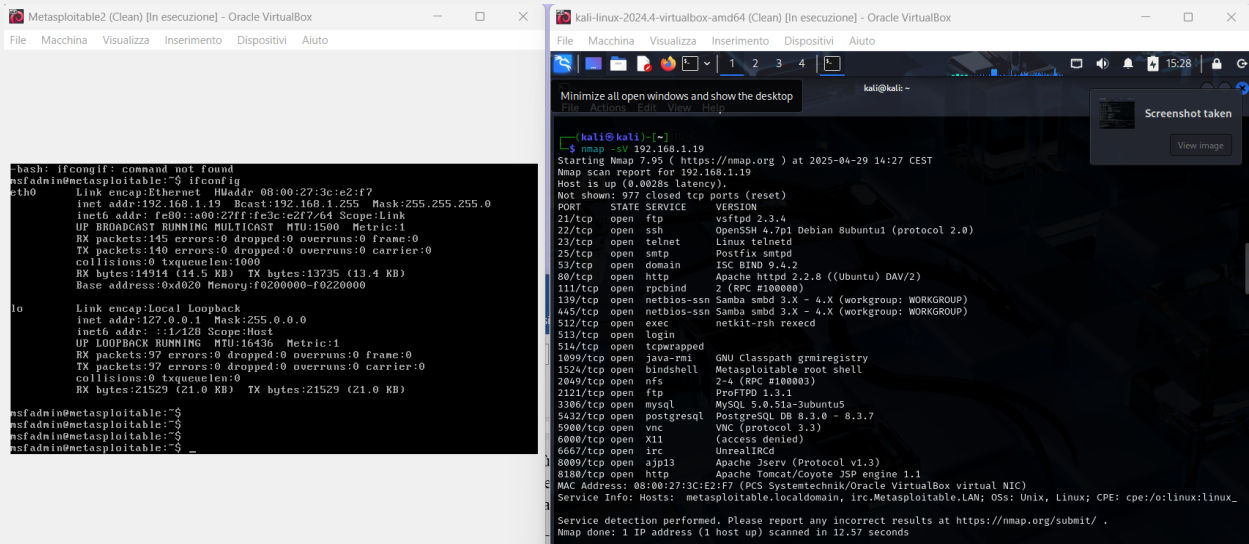
Nmap done: 1 IP address (1 host up) scanned in 0.89 seconds
  
```

A sinistra l'IP della macchina di Metasploitable. A destra, da Kali Linux, il comando `nmap -sT` con IP di Metasploitable per ottenere info sulle porte e servizi aperti. Non si riscontra nessuna differenza con il comando `nmap -sS` poiché ciò che varia è la modalità con cui si ottengono le informazioni.

sT è più invasivo e completa tutti i passaggi del 3-way-handshake, stabilendo di fatto un canale.

sS è meno invasivo in quanto nmap, una volta ricevuto il pacchetto SYN/ACK dalla macchina target, non conclude il 3-way-handshake, ma appurato che la porta è aperta chiude la comunicazione, di fatto evitando overload dato dalla creazione del canale.

2.4 Version detection



```

bash: ifconfig: command not found
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:3c:e2:f7
          inet addr:192.168.1.19  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe3c:e2f7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:145 errors:0 dropped:0 overruns:0 frame:0
          TX packets:140 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:14914 (14.5 KB)  TX bytes:13735 (13.4 KB)
          Base address:0xd020 Memory:10200000-10220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:97 errors:0 dropped:0 overruns:0 frame:0
          TX packets:97 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:21529 (21.0 KB)  TX bytes:21529 (21.0 KB)

msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$

```

```

kali@kali:~$ nmap -sV 192.168.1.19
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 14:27 CEST
Nmap scan report for 192.168.1.19
Host is up (0.0028s 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         netkit-rsh rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi      GNU Classpath gmrregistry
1524/tcp  open  bindshell     Metasploitable root shell
2049/tcp  open  nfs           2-4 (RPC #100000)
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
8080/tcp  open  ajp13         Apache Jserv (Protocol v1.3)
8180/tcp  open  http          Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:3C:E2:F7 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OS: Unix, Linux; CPE: cpe:/o:linux:linux_
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.57 seconds

```

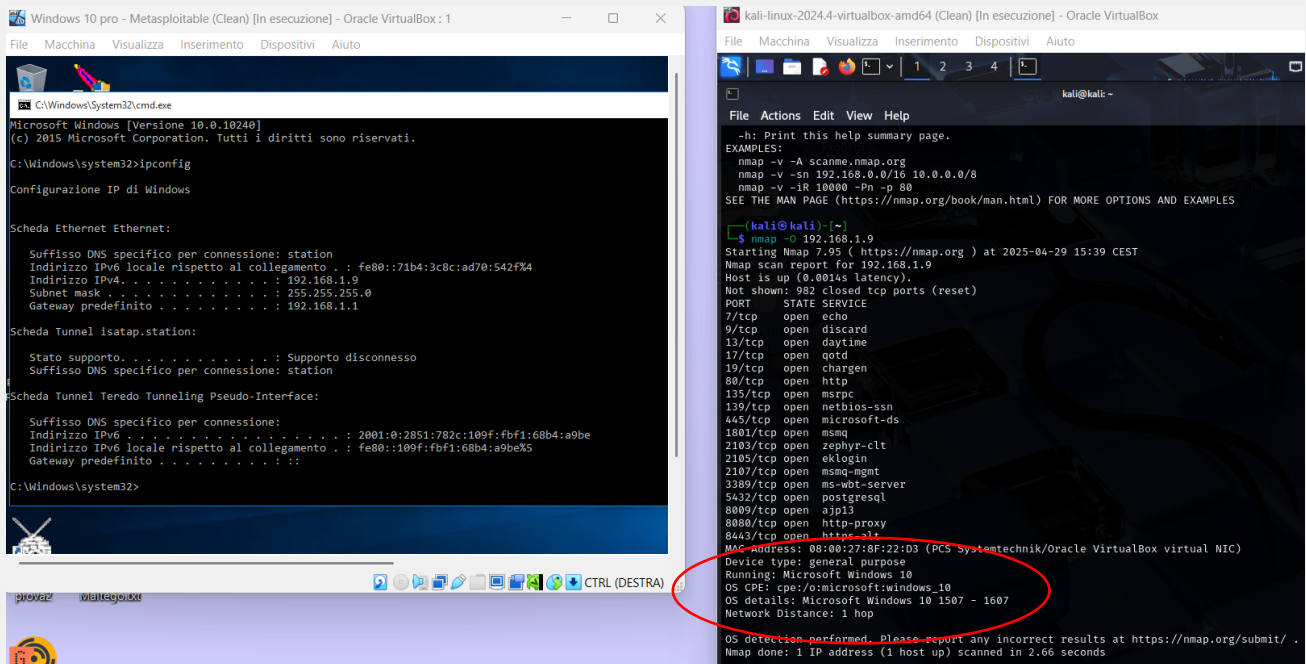
A sinistra l'IP della macchina di Metasploitable. A destra, da Kali Linux, il comando `nmap -sV` con IP di Metasploitable per ottenere i servizi aperti e le versioni in esecuzione sulle porte.

2.5 Report finale tramite nmap

```
(kali@kali)~$ IP="192.168.1.19";R="report_excercise-${date +%Y-%m-%d_%H:%M)-
${IP}";sudo nmap -O -sT -sV -p- -oX "${R}.xml" "${IP}" && xsltproc "${R}.xml -o "${R}").h
tml
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 14:47 CEST
Nmap scan report for 192.168.1.19
Host is up (0.0020s latency).
Not shown: 65505 closed tcp ports (conn-refused)
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        OpenBSD or Solaris rlogind
514/tcp   open  tcpmrapppd
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
3632/tcp  open  distccd      distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
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
6697/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb          Ruby DRB RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drbr)
40746/tcp open  java-rmi     GNU Classpath grmiregistry
40789/tcp open  mountd       1-3 (RPC #100005)
41577/tcp open  nlockmgr     1-4 (RPC #100021)
58972/tcp open  status       1 (RPC #100024)
MAC Address: 08:00:27:3C:E2:F7 (PCS Systemtechnik/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
```

Da Kali Linux, il comando `IP="192.168.1.19";R="report_excercise-${date +%Y-%m-%d_%H:%M)-${IP}";sudo nmap -O -sT -sV -p- -oX "${R}.xml" "${IP}" && xsltproc "${R}.xml -o "${R}").html` per ottenere un report html con tutte le info richieste.

2.6 OS fingerprint WINDOWS



A sinistra l'IP della macchina di Metasploitable. A destra, da Kali Linux, il comando nmap -O con IP di Windows 10 per ottenere info sul sistema operativo.