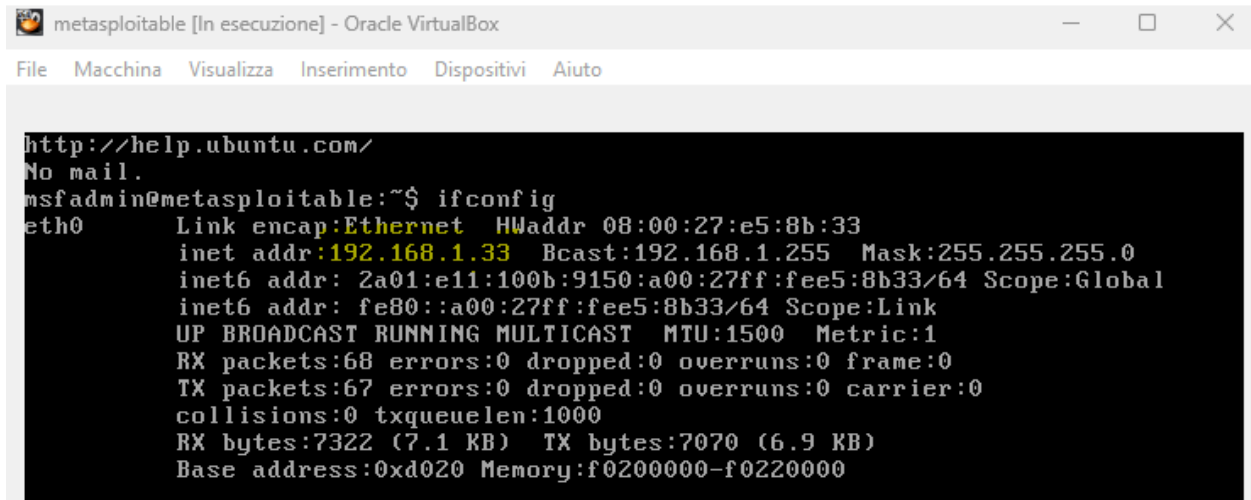


S5 - L2 NMAP

Di seguito sono stati effettuati dei test di scansione sul target Metasploitable.



```
metasploitable [In esecuzione] - Oracle VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:e5:8b:33
          inet addr:192.168.1.33  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: 2a01:e11:100b:9150:a00:27ff:fee5:8b33/64 Scope:Global
          inet6 addr: fe80::a00:27ff:fee5:8b33/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:68 errors:0 dropped:0 overruns:0 frame:0
          TX packets:67 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:7322 (7.1 KB)  TX bytes:7070 (6.9 KB)
          Base address:0xd020 Memory:f0200000-f0220000
```

Una volta individuato l'indirizzo IP della macchina target, in questo caso 192.168.1.33 possiamo iniziare ad effettuare le scansioni di rete con NMAP da Kali.

Il primo test è stato effettuato con la scansione SYN utilizzando il comando **nmap -sS [target]** (vedi immagine sotto) Questa scansione è molto utilizzata in quanto più veloce rispetto alla cugina TCP (-sT, che vedremo successivamente) perchè non stabilisce una connessione TCP completa non terminando di fatto il 3-Way handshake, inoltre per poter funzionare la scansione SYN necessita di privilegi di root.

Come possiamo vedere dall'immagine seguente ha effettuato la scansione in soli 0.31 secondi riportandoci di fatto le porte che risultano aperte e con quali servizi, in questo caso ci ha riportato in output anche il MAC Address della macchina virtuale.

```
(root@kali)-[/home/kali/Desktop]
# nmap -sS 192.168.1.33
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 13:41 CET
Nmap scan report for 192.168.1.33
Host is up (0.00013s 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:E5:8B:33 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds
```

Per la seconda scansione, come anticipato nel paragrafo sopra, è stato utilizzando il comando **nmap -sT [target]**, questo a differenza del precedente test crea una connessione TCP completa pertanto richiede maggior tempo e risulta più affidabile. Non necessita di privilegi di root.

Come si può vedere nell'immagine seguente riporta lo stesso output del precedente test senza nessuna differenza.

```
(root@kali)-[/home/kali/Desktop]
# nmap -sT 192.168.1.33
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 13:42 CET
Nmap scan report for 192.168.1.33
Host is up (0.0025s 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:E5:8B:33 (Oracle VirtualBox virtual NIC)
```

Di seguito invece possiamo vedere il comando **nmap -sV [target]**, in particolar modo a differenza dei precedenti test questo comando ci permette di poter raccogliere informazioni fondamentali per quanto riguarda i servizi attivi sulle porte e le loro versioni, di conseguenza conoscendo quest'ultimi possiamo avere un quadro generale per poter identificare eventuali vulnerabilità.

Di seguito l'output: da questa schermata abbiamo un chiaro e preciso report di quali sono le porte aperte, i servizi e le loro versioni.

```
(root@kali)~/Desktop
# nmap -sV 192.168.1.33
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 13:44 CET
Nmap scan report for 192.168.1.33
Host is up (0.00081s 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          OpenBSD or Solaris rlogind
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:E5:8B:33 (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 11.76 seconds
```

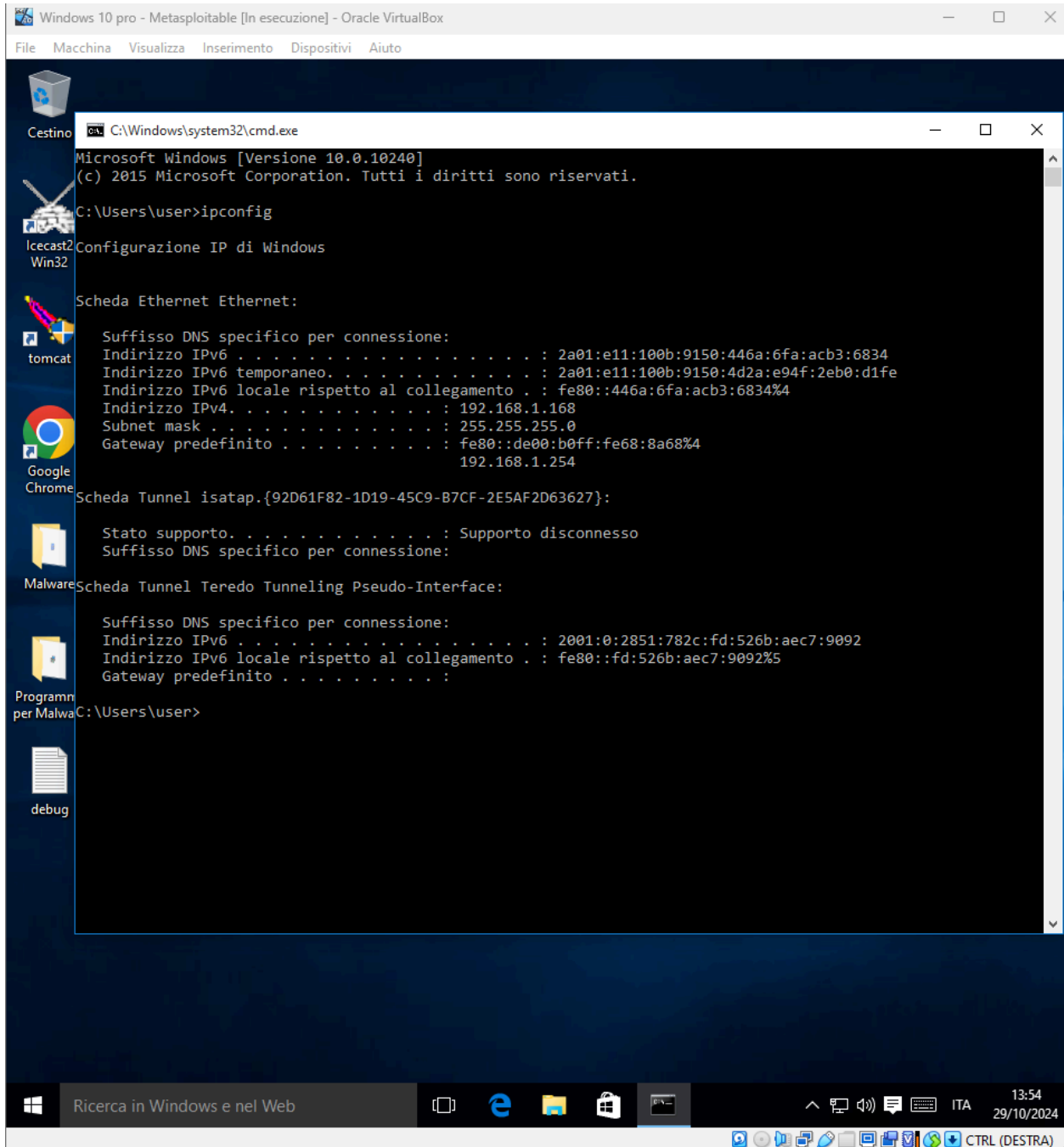
Abbiamo inoltre eseguito il comando **nmap -O**, questo ci permette di poter rilevare il sistema operativo della macchina target in questo caso abbiamo effettuato la scansione sia su Metasploitable che su Win10.

Metasploitable: come si evince dall'immagine viene riportato che il SO è Linux 2.6.9 - 2.6.33

```
(root@kali)-[/home/kali/Desktop]
# nmap -O 192.168.1.33
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 14:27 CET
Nmap scan report for 192.168.1.33
Host is up (0.00023s latency).
Not shown: 978 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
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:E5:8B:33 (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 1.96 seconds
```

WIN 10 - Metasploitable.



```
Windows 10 pro - Metasploitable [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto

Cestino C:\Windows\system32\cmd.exe
Microsoft Windows [Versione 10.0.10240]
(c) 2015 Microsoft Corporation. Tutti i diritti sono riservati.

C:\Users\user>ipconfig

Configurazione IP di Windows

Scheda Ethernet Ethernet:

Suffisso DNS specifico per connessione:
Indirizzo IPv6 . . . . . : 2a01:e11:100b:9150:446a:6fa:acb3:6834
Indirizzo IPv6 temporaneo. . . . . : 2a01:e11:100b:9150:4d2a:e94f:2eb0:d1fe
Indirizzo IPv6 locale rispetto al collegamento . : fe80::446a:6fa:acb3:6834%4
Indirizzo IPv4. . . . . : 192.168.1.168
Subnet mask . . . . . : 255.255.255.0
Gateway predefinito . . . . . : fe80::de00:b0ff:fe68:8a68%4
192.168.1.254

Scheda Tunnel isatap.{92D61F82-1D19-45C9-B7CF-2E5AF2D63627}:

Stato supporto. . . . . : Supporto disconnesso
Suffisso DNS specifico per connessione:

Scheda Tunnel Teredo Tunneling Pseudo-Interface:

Suffisso DNS specifico per connessione:
Indirizzo IPv6 . . . . . : 2001:0:2851:782c:fd:526b:aec7:9092
Indirizzo IPv6 locale rispetto al collegamento . : fe80::fd:526b:aec7:9092%5
Gateway predefinito . . . . . :

C:\Users\user>
```

Ricerca in Windows e nel Web

13:54
29/10/2024

CTRL (DESTRA)

```
(root@kali)-[/home/kali/Desktop]
# nmap -O 192.168.1.168
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 13:53 CET
Nmap scan report for 192.168.1.168
Host is up (0.00026s latency).
Not shown: 981 closed tcp ports (reset)
PORT      STATE SERVICE
7/tcp     open  echo
9/tcp     open  discard
13/tcp    open  daytime
17/tcp    open  qotd
19/tcp    open  chargen
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1801/tcp  open  msmq
2103/tcp  open  zephyr-clt
2105/tcp  open  eklogin
2107/tcp  open  msmq-mgmt
2869/tcp  open  icslap
3389/tcp  open  ms-wbt-server
5432/tcp  open  postgresql
8009/tcp  open  ajp13
8080/tcp  open  http-proxy
8443/tcp  open  https-alt
MAC Address: 08:00:27:10:D9:89 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1507 - 1607
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 14.91 seconds
```