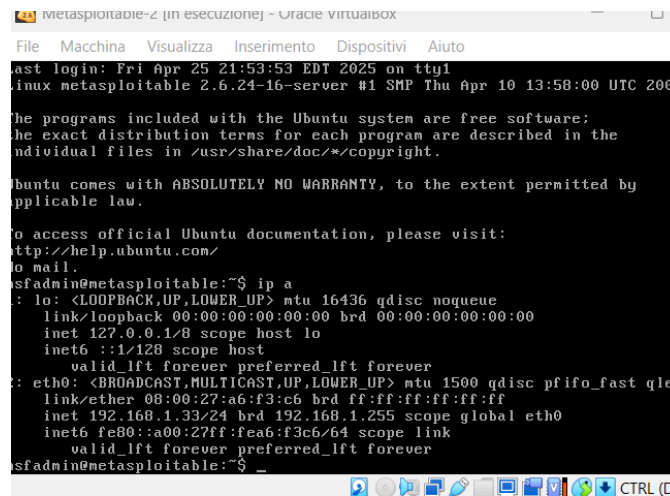


## Report Nmap

- Per poter eseguire delle scansioni con Nmap al fine di ottenere i risultati richiesti, abbiamo bisogno dell'indirizzo IP del sistema Target.

In questo caso si sono effettuate delle simulazioni impostando come Target desiderato la Metasploitable.

Abbiamo ricavato quindi l'ip sulla Meta con <<ip a>>, in questo caso l'ip fornito dalla macchina è: 192.168.1.33/24



```
metasploitable-z [in esecuzione] - Oracle virtualbox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
last login: Fri Apr 25 21:53:53 EDT 2025 on tty1
linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008

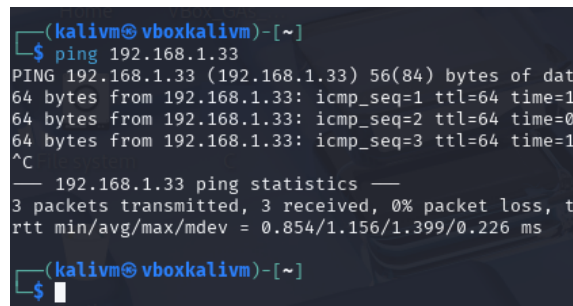
The programs included with the Ubuntu system are free software:
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
to mail.
sfadmin@metasploitable:~$ ip a
: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:a6:f3:c6 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.33/24 brd 192.168.1.255 scope global eth0
        inet6 fe80::a00:27ff:fea6:f3c6/64 scope link
            valid_lft forever preferred_lft forever
sfadmin@metasploitable:~$
```

Una volta trovato l'ip del Target, si possono effettuare le varie scansioni e per iniziare, sono state effettuate la TCP Connect Scan, con l'utilizzo del comando <<-sT>> e la TCP SYN Scan, con il comando <<-sS>>.

Quindi, per poter procedere, si è verificata la connessione con la macchina target, in questo caso pingandola ( questo passaggio è stato effettuato per una prova visto il Target della Meta, essendo che il ping verrebbe rilevato molto facilmente, sarebbe meglio rimanere più Stealth direttamente con i passaggi successivi ).



```
(kalivm@vboxkalivm)-[~]
$ ping 192.168.1.33
PING 192.168.1.33 (192.168.1.33) 56(84) bytes of data:
64 bytes from 192.168.1.33: icmp_seq=1 ttl=64 time=1.05 ms
64 bytes from 192.168.1.33: icmp_seq=2 ttl=64 time=0.85 ms
64 bytes from 192.168.1.33: icmp_seq=3 ttl=64 time=1.39 ms
^C
--- 192.168.1.33 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time=0.001s
rtt min/avg/max/mdev = 0.854/1.156/1.399/0.226 ms
(kalivm@vboxkalivm)-[~]
$
```

Con la scansione TCP Connect Scan, abbiamo rilevato tutte le porte aperte, indicando un segnale di rischio in quanto probabilmente non è stato applicato nessun tipo di Firewall o IDS.

```
(kalivm@vboxkalivm)-[~]
$ nmap -sT 192.168.1.33
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 15:03 CEST
Nmap scan report for Host-004.homenet.telecomitalia.it (192.168.1.33)
Host is up (0.00050s 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:A6:F3:C6 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds
```

E' stata poi eseguita una scansione inviando solo pacchetti SYN.

```
(kalivm@vboxkalivm)-[~]
$ nmap -sS 192.168.1.33
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 15:07 CEST
Nmap scan report for Host-004.homenet.telecomitalia.it (192.168.1.33)
Host is up (0.0016s 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
```

Anche qui, tutte le porte, sono risultate aperte.

La differenza principale, si è verificata nel tempo della scansione effettiva di tutte le porte utilizzando il comando <<-p>>, utile per poter scansionare tutte le porte presenti e non solo quelle preimpostate dalla normale scansione.

-Successivamente alle scansioni di porte, è stata effettuata una scansione relativa alla versione dei servizi in esecuzione sulle porte Target, con l'utilizzo del comando <<-sV>>.

Viene effettuato al fine di valutare la vulnerabilità del sistema Target.

```
(kalivm@vboxkalivm)-[~]
$ nmap -sV 192.168.1.33
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 15:23 CEST
Stats: 0:00:23 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 15:24 (0:00:01 remaining)
Stats: 0:00:37 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 15:24 (0:00:02 remaining)
Stats: 0:01:04 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 15:24 (0:00:03 remaining)
Nmap scan report for Host-004.homenet.telecomitalia.it (192.168.1.33)
Host is up (0.000098s 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?
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:A6:F3:C6 (PCS Systemtechnik/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 64.21 seconds
```

Questa scansione ci ha portato alla conferma di quanto detto prima, sono presenti delle vulnerabilità e si consiglia di aggiornare le versioni quanto prima.

-Infine, per trovare il SO target, è stato utilizzato l'OS fingerprint, in questo caso combinando il comando <<--osscan-limit>> con il comando <<--osscan-guess>>, per una scansione più accurata.

```
(kalivm@vboxkalivm)-[~]
$ nmap -O --osscan-limit --osscan-guess 192.168.1.33
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 15:33 CEST
Nmap scan report for Host-004.homenet.telecomitalia.it (192.168.1.33)
Host is up (0.00090s 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:A6:F3:C6 (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
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 1.74 seconds
```

Il Sistema Operativo è stato identificato con successo, in questo caso Linux 2.6 con tanto di versione. ( Anche se con un leggero range per la versione esatta ).

## Conclusioni

-Dopo aver effettuato tutte le scansioni, si può affermare che il Target presenta diverse vulnerabilità, come detto in precedenza, si consiglia di aggiornare le versioni dei servizi e se possibile ma estremamente raccomandato, implementare un Firewall di sicurezza, accompagnato da un IDS, così da poter essere informati in caso di minacce o meglio ancora, configurare un IPS così da prevenire qualsiasi eventuale attacco.

Infine, è stata aggiunta una scansione OS fingerprint al nostro sistema.

```
(kali@kali:~)$ nmap -O --osscan-guess 192.168.1.13
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 15:49 CEST
Nmap scan report for 192.168.1.13 (192.168.1.13)
Host is up (0.0011s 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: BC:17:88:F2:82:E6 (Intel Corporate)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows 11 21H2 (94%), Microsoft Windows 10 (91%), Microsoft Windows 10 1607 (91%), Microsoft Windows Server 2022 (90%), Microsoft Windows Server 2008 SP1 (88%), Microsoft Windows Phone 7.5 or 8.0 (86%)
, Microsoft Windows 10 1511 - 1607 (86%), Microsoft Windows 10 1703 (86%), Microsoft Windows 10 1511 (85%), Microsoft Windows 7 or Windows Server 2008 R2 (85%)
No exact OS matches for host (test conditions non-ideal).
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 9.59 seconds
```

I risultati della scansione non sono stati accurati al 100%, in quanto ci suggerisce Windows 10 con una probabilità dell'85%, ma comunque si è avvicinato parecchio, in quanto il SO utilizzato è Windows 11.

