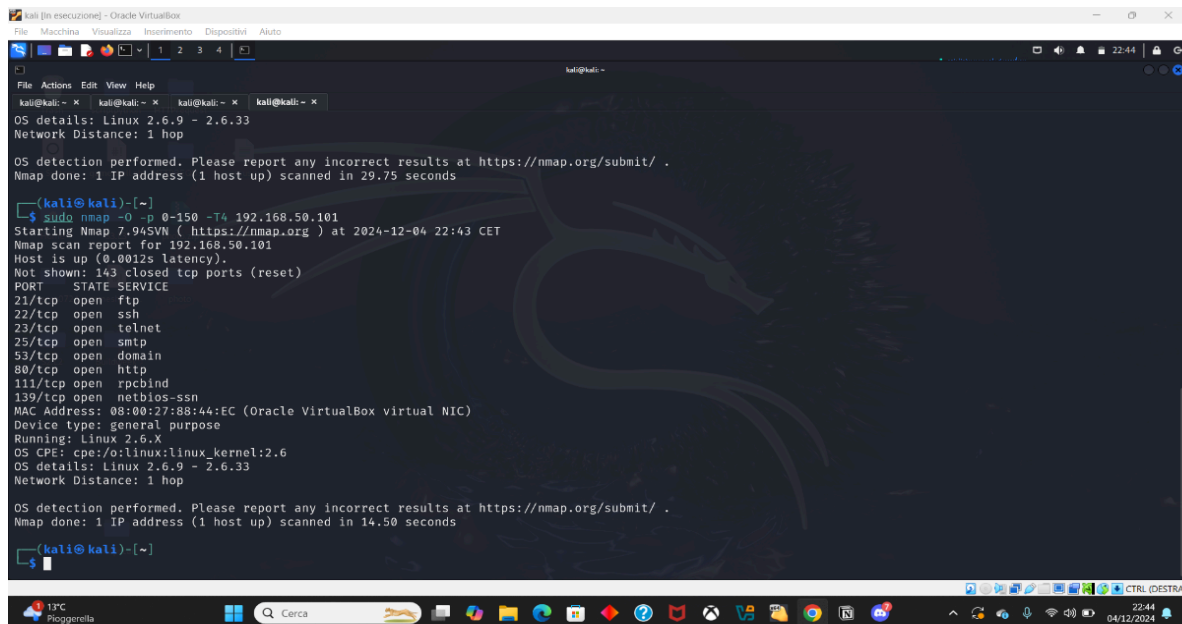


## MACCHINA TARGET: Metasploitable

IP: 192.168.50.101

il primo scan effettuato sulla macchina metasploitable è stato l' OSfingerprint



```
kali [in esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto

kali@kali: ~
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 29.75 seconds

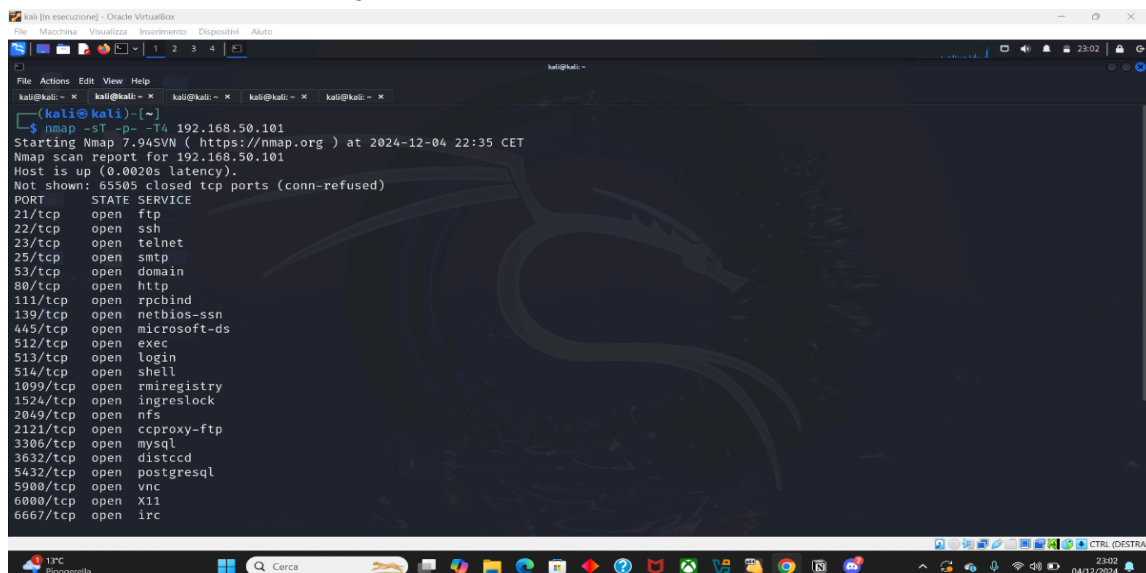
(kali@kali)-[~]
└─$ sudo nmap -O -p 0-150 -T4 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-04 22:43 CET
Nmap scan report for 192.168.50.101
Host is up (0.0012s latency).
Not shown: 143 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
MAC Address: 08:00:27:88:44:EC (Oracle VM 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 14.50 seconds

(kali@kali)-[~]
```

Da questa scansione possiamo notare oltre le porte scansionate risultate aperte che vanno dalla porta 1 alla porta 150, soprattutto il sistema operativo della metasploitable in questo caso dalla scansione risulta essere una macchina Linux e la versione può essere fra la 2.6.9 e la 2.6.33, possiamo anche recuperare il mac address della macchina target con questa scansione, in questo caso uguale a 08:00:27:88:44:EC e in questo caso ci restituisce anche il tipo di kernel e la sua versione, in questo caso è un linux\_kernel versione 2.6.

La seconda scansione eseguita è una scansione TCP di tipo SYN

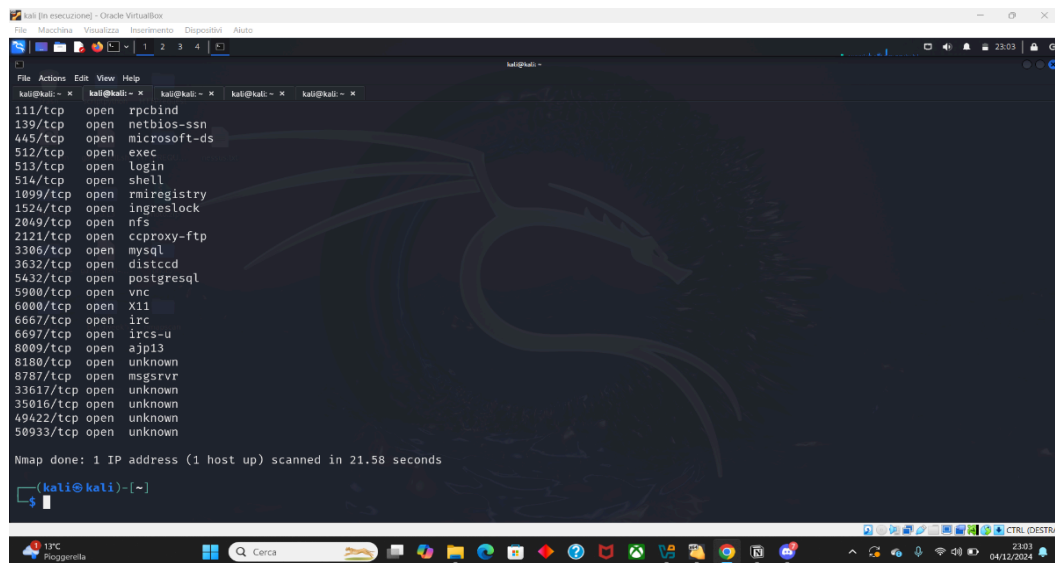


```
kali [in esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto

kali@kali: ~
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 29.75 seconds

(kali@kali)-[~]
└─$ nmap -ST -p- -T4 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-04 22:35 CET
Nmap scan report for 192.168.50.101
Host is up (0.0020s latency).
Not shown: 65505 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
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
```



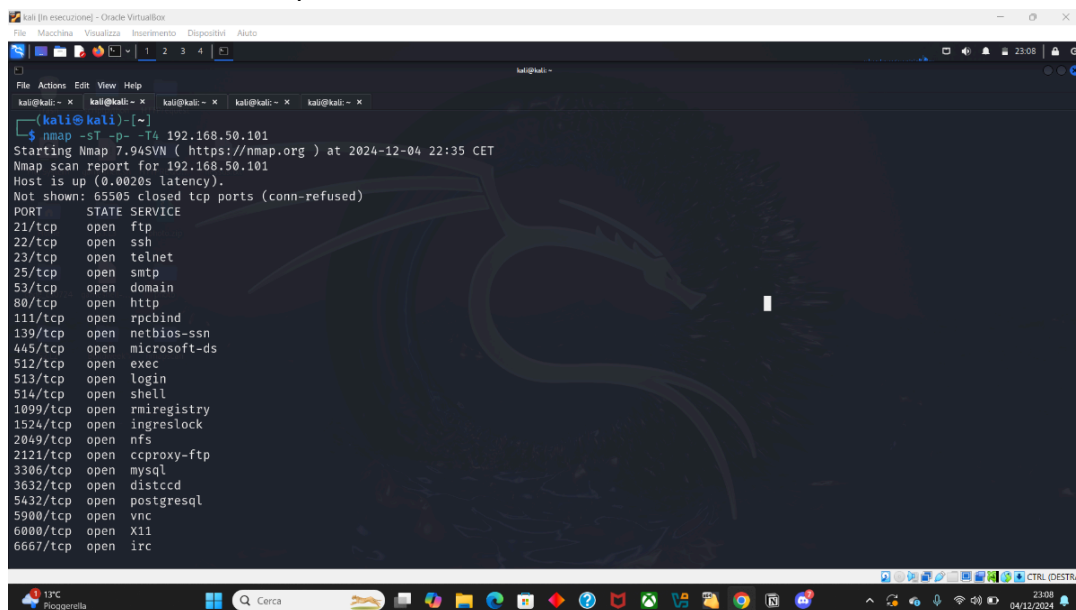
```
kali [in esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto

kali@kali: ~
File Actions Edit View Help
kali@kali: ~ kali@kali: ~ kali@kali: ~ kali@kali: ~
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
3632/tcp open distccd
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
6697/tcp open ircs-u
8009/tcp open ajp13
8180/tcp open unknown
8787/tcp open msgsrvr
33617/tcp open unknown
35016/tcp open unknown
49422/tcp open unknown
50933/tcp open unknown

Nmap done: 1 IP address (1 host up) scanned in 21.58 seconds
kali@kali: ~
$
```

Questa scansione ha la caratteristica di non completare il triplo hand shake, ogni volta che la scansione controlla se una porta è aperta o chiusa, manda una richiesta di SYN e se la porta aperta risponde con un ACK, mentre se la porta è chiusa risponde con un RST. Questa è la prima differenza che ho notato fra la scansione tcp di tipo syn e quella di tipo connect. Si può notare anche dalla 4 riga della scansione alla voce tcp ports (reset), il motivo di questa cosa è proprio quello sopra elencato.

La terza scansione di tipo TCP connect:

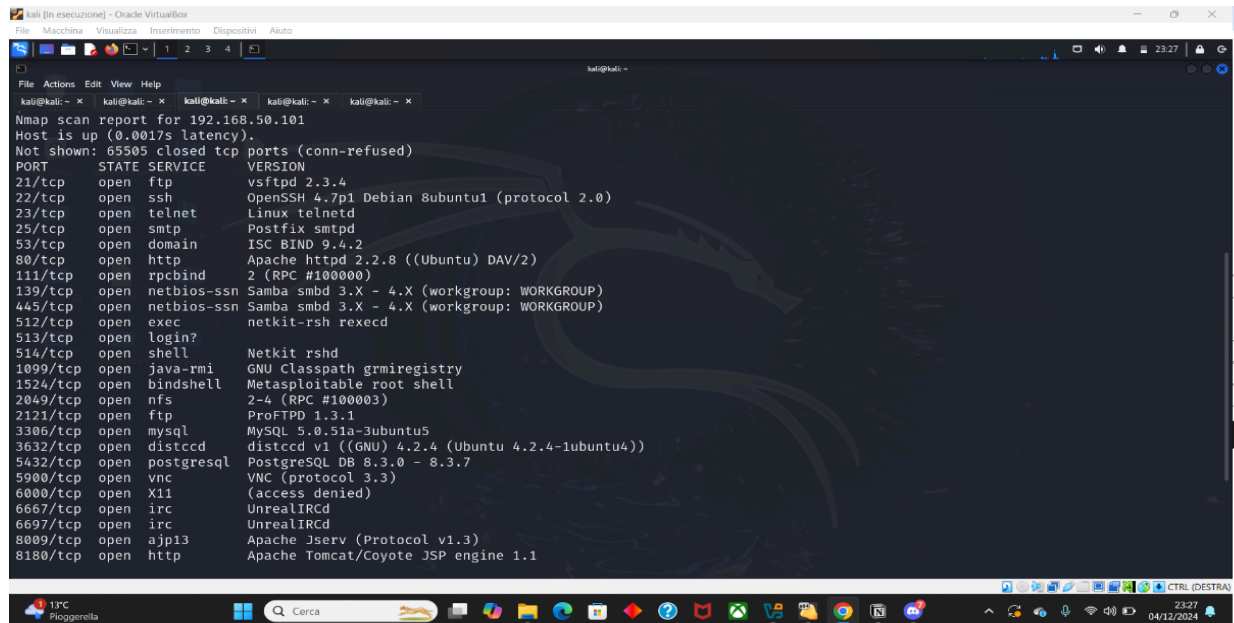


```
kali [in esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto

kali@kali: ~
File Actions Edit View Help
kali@kali: ~ kali@kali: ~ kali@kali: ~ kali@kali: ~ kali@kali: ~
kali@kali: ~
$ nmap -sT -p- -T4 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-04 22:35 CET
Nmap scan report for 192.168.50.101
Host is up (0.0020s latency).
Not shown: 65505 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
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
```

Questo tipo di scansione completa il triplo handshake, quindi ogni volta che la scansione incontra una porta aperta effettua una richiesta SYN per connettersi e in caso di porta aperta risponde con una richiesta SYN-ACK e conclude con un ACK. Nel caso di porta chiusa anche questa volta la richiesta nel triplo hand shake una volta effettuata una richiesta SYN se la porta è chiusa ci restituirà un RST, ma a differenza della scansione SYN il RST lo dobbiamo interpretare come una connessione rifiutata dopo aver tentato di completare il triplo hand shake. Un'altra differenza fra i due tipo di scansioni ho notato essere il tempo, la scansione SYN in questo caso si è dimostrata essere più lenta anche se non completa il triplo hand shake.

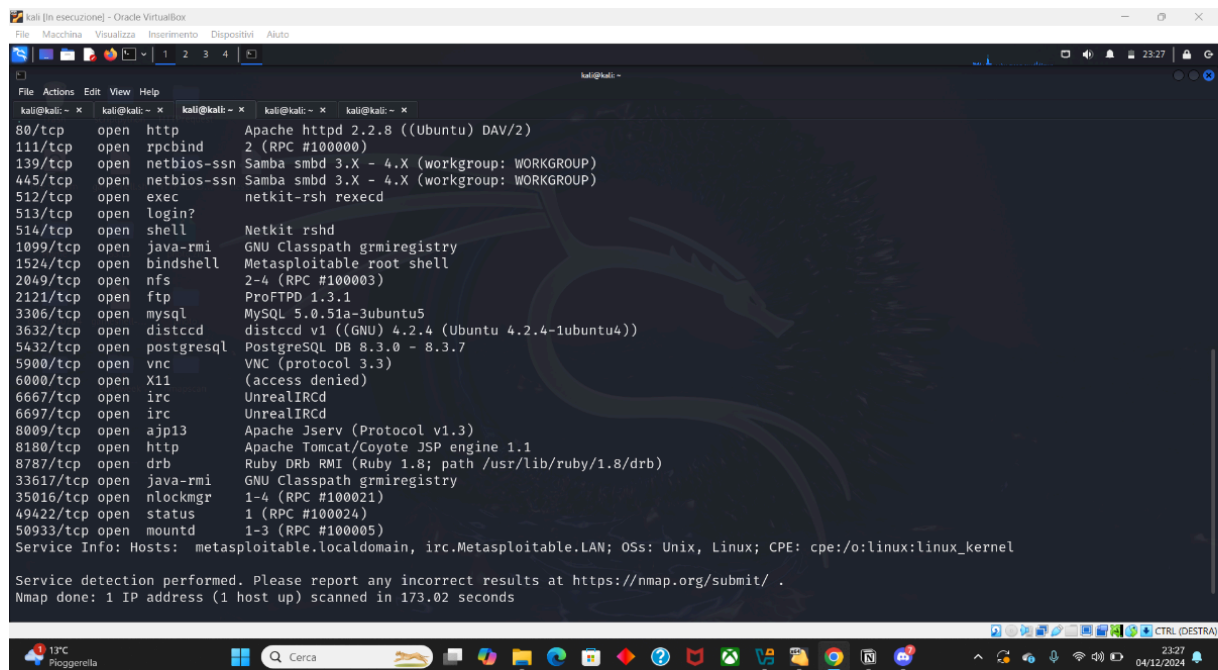
Scansione per controllare la versione dei servizi attivi sulle porte.



```
kali [in esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

kali@kali: ~
kali@kali: ~
kali@kali: ~
kali@kali: ~
kali@kali: ~

Nmap scan report for 192.168.50.101
Host is up (0.0017s 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?         Netkit rshd
514/tcp   open  shell          GNU Classpath grmiregistry
1099/tcp  open  java-rmi       Metasploitable root shell
1524/tcp  open  bindshell      2-4 (RPC #100003)
2049/tcp  open  nfs            ProFTPD 1.3.1
2121/tcp  open  ftp            MySQL 5.0.51a-3ubuntu5
3306/tcp  open  mysql          distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
3632/tcp  open  distccd        PostgreSQL DB 8.3.0 - 8.3.7
5432/tcp  open  postgresql     VNC (protocol 3.3)
5900/tcp  open  vnc            (access denied)
6000/tcp  open  X11            UnrealIRCd
6667/tcp  open  irc            UnrealIRCd
6697/tcp  open  irc            Apache Jserv (Protocol v1.3)
8009/tcp  open  ajp13          Apache Tomcat/Coyote JSP engine 1.1
8180/tcp  open  http           Apache Tomcat/Coyote JSP engine 1.1
```



```
kali [in esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

kali@kali: ~
kali@kali: ~
kali@kali: ~
kali@kali: ~
kali@kali: ~

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 rshd
514/tcp   open  shell          GNU Classpath grmiregistry
1099/tcp  open  java-rmi       Metasploitable root shell
1524/tcp  open  bindshell      2-4 (RPC #100003)
2049/tcp  open  nfs            ProFTPD 1.3.1
2121/tcp  open  ftp            MySQL 5.0.51a-3ubuntu5
3306/tcp  open  mysql          distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
3632/tcp  open  distccd        PostgreSQL DB 8.3.0 - 8.3.7
5432/tcp  open  postgresql     VNC (protocol 3.3)
5900/tcp  open  vnc            (access denied)
6000/tcp  open  X11            UnrealIRCd
6667/tcp  open  irc            UnrealIRCd
6697/tcp  open  irc            Apache Jserv (Protocol v1.3)
8009/tcp  open  ajp13          Apache Tomcat/Coyote JSP engine 1.1
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/drbb)
33617/tcp open  java-rmi       GNU Classpath grmiregistry
35016/tcp open  nlockmgr       1-4 (RPC #100021)
49422/tcp open  status         1 (RPC #100024)
50933/tcp open  mountd         1-3 (RPC #100005)

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 173.02 seconds
```

Questa scansione mira a controllare se tutte le porte siano aperte o chiuse sulla macchina metasploitable, verificando anche le versioni dei vari servizi attivi trovati sulle porte aperte.

MACCHINA TARGET: Windowsxp

IP: 192.168.50.103

scan type: OS fingerprint

risultato:

```
kali [in esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto

kali@kali: ~
File Actions Edit View Help
kali@kali: ~ kali@kali: ~ kali@kali: ~ kali@kali: ~ kali@kali: ~
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 14.50 seconds

kali@kali: ~
$ sudo nmap -O -p 0-150 -T4 192.168.50.103
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-04 23:33 CET
Stats: 0:00:04 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Nmap scan report for 192.168.50.103
Host is up (0.0017s latency).
Not shown: 150 filtered tcp ports (no-response)
PORT      STATE SERVICE
139/tcp   open  netbios-ssn
MAC Address: 08:00:27:5B:1C:B4 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows 2000 SP3/SP4 or Windows XP SP1/SP2 (97%), Microsoft Windows XP SP2 or SP3 (97%), Microsoft Windows 2000 SP0 - SP4 or Windows XP SP0 - SP1 (95%), Microsoft Windows Server 2003 SP1 or SP2 (95%), Microsoft Windows 2000 SP4 or Windows XP SP1a (94%), Microsoft Windows 2000 SP4 (93%), Microsoft Windows XP SP3 (93%), Microsoft Windows XP Professional SP2 or Windows Server 2003 (93%), Microsoft Windows XP SP1 (93%), Microsoft Windows 2000 Server SP3 or SP4 (92%)
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 18.59 seconds

kali@kali: ~
$
```

Dalla scansione si può notare come in questo caso non si ha una sicurezza del 100% sul tipo del sistema operativo e della sua versione precisa, ma ci restituisce una percentuale del 97% che il sistema operativo possa essere windowsxp sp1/sp2 o la versione sp3/sp4.