

Scansione dei servizi con Nmap

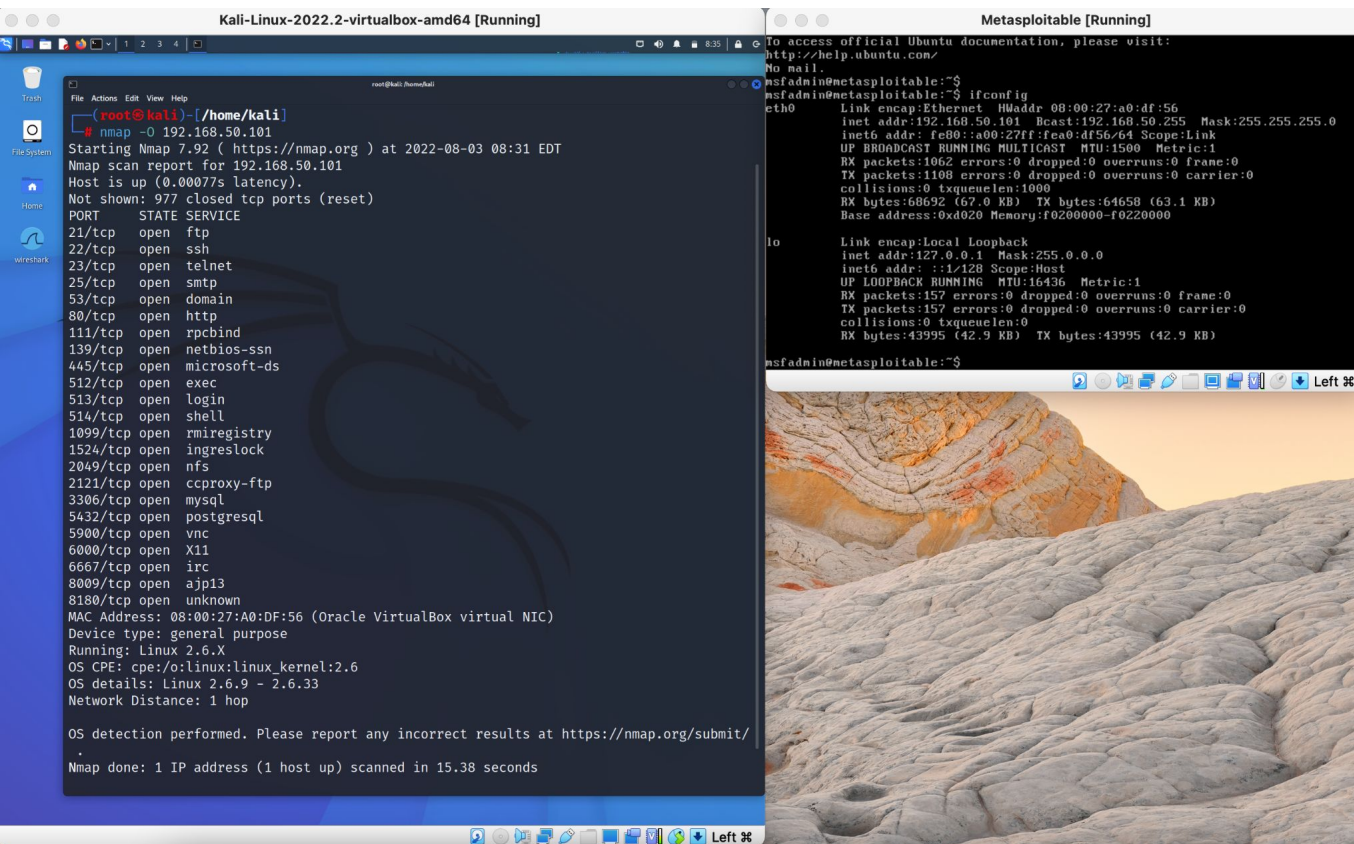
MACCHINE UTILIZZATE: Kali Linux - Windows 7 - Metasploitable

Andremo ad analizzare
vari servizi di
Metasploitable con
nmap.

Nmap è un software che
esegue attività di port
scanning

- OS fingerprint
- Syn Scan
- TCP connect
- Version detection

OS fingerprint



The image shows two terminal windows side-by-side. The left window is titled 'Kali-Linux-2022.2-virtualbox-amd64 [Running]' and shows the output of an Nmap scan performed on 192.168.50.101. The scan detected 23 open ports, including ftp, ssh, telnet, smtp, domain, http, rpcbind, netbios-ssn, microsoft-ds, exec, login, shell, rmiregistry, ingreslock, nfs, ccproxy-ftp, mysql, postgresql, vnc, X11, irc, and ajp13. The OS is identified as Linux 2.6.9. The right window is titled 'Metasploitable [Running]' and shows the output of the 'ifconfig' command. It displays network details for the 'eth0' interface, including the IP address 192.168.50.101, netmask 255.255.255.0, and broadcast address 192.168.50.255. It also shows statistics for RX and TX packets and bytes.

```
root@kali:~# nmap -O 192.168.50.101
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 08:31 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00077s 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:A0:DF:56 (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 15.38 seconds
```

```
msfadmin@metasploitable:~$ ifconfig
eth0:
Link encap:Ethernet HWaddr 08:00:27:a0:df:56
inet addr:192.168.50.101 Bcast:192.168.50.255 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:fea0:df56/64 Scope:Link
UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
RX packets:1062 errors:0 dropped:0 overruns:0 frame:0
TX packets:1100 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:68692 (67.0 KB) TX bytes:64658 (63.1 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:16436  Metric:1
RX packets:157 errors:0 dropped:0 overruns:0 frame:0
TX packets:157 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:43995 (42.9 KB) TX bytes:43995 (42.9 KB)

msfadmin@metasploitable:~$
```

Il risultato del comando `"nmap -O 192.168.50.101"` ci mostra le porte aperte ed il servizio delle stesse.

Altre informazioni interessanti sono il **MAC Address** di Metasploitable e la versione di Linux(2.6.) che utilizza.

Banner grabbing

"nmap -sV -sS 192.168.50.101"

Con il comando su riportato stiamo facendo il "banner grabbing" che consiste nel recuperare le informazioni offerte dal software, come il nome del software utilizzato.

Hosts:

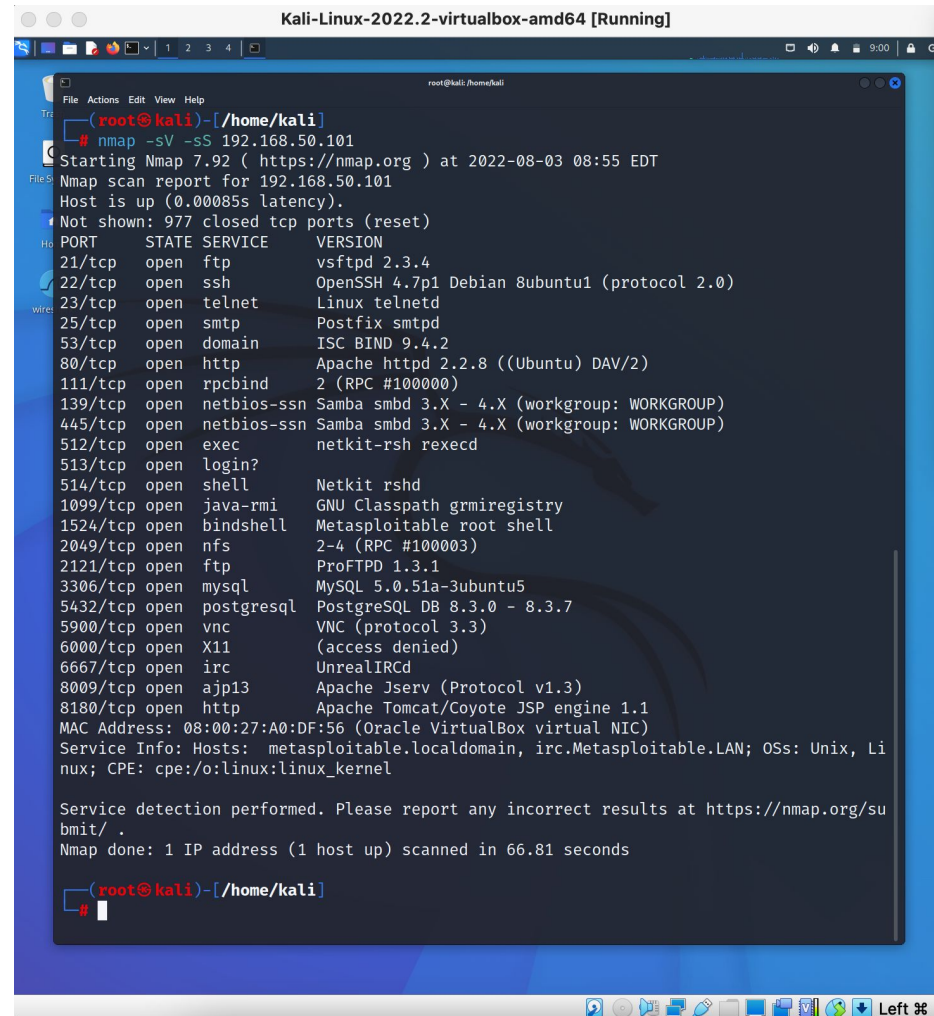
- metasploitable.localdomain
- irc.Metasploitable.LAN

Os:

- Unix
- Linux

-sS = SYN scan

Il SYNscan viene utilizzato per essere meno visibili, dato che non si conclude il 3wh.



```
Kali-Linux-2022.2-virtualbox-amd64 [Running]

root@kali:~/home/kali# nmap -sV -sS 192.168.50.101
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 08:55 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00085s 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  shell        Netkit rshd
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:A0:DF:56 (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/su
bmit/ .
Nmap done: 1 IP address (1 host up) scanned in 66.81 seconds

root@kali:~/home/kali#
```

```

File Actions Edit View Help
(root@kali)~[/home/kali]
# nmap -sV -sT 192.168.50.101
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 09:15 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0016s latency).
Not shown: 977 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?
514/tcp   open  shell        Netkit rshd
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:A0:DF:56 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; C
PE: 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 66.99 seconds

(root@kali)~[/home/kali]
#

```

Scansione TCP connect

“nmap -sV -sT 192.168.50.101”

Questo è la scansione TCP, con il comando -sT

La differenza sta nella risposta che danno le due scansioni, la prima da ‘reset’ e la seconda ‘conn-refused’.

"nmap 192.168.50.101"

In questa versione oltre alle porte aperte e ai servizi, in fondo possiamo vedere le informazioni sul sistema operativo.

```
Kali-Linux-2022.2-virtualbox-amd64 [Running]
root@kali: /home/kali
File Actions Edit View Help
# nmap 192.168.50.101 --script smb-os-discovery
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 10:27 EDT
Nmap scan report for 192.168.50.101
Host is up (0.035s 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:A0:DF:56 (Oracle VirtualBox virtual NIC)

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2022-08-03T10:27:46-04:00
```


Windows

```
(root@kali)-[/home/kali]
# nmap 192.168.50.105 --script smb-os-discovery
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 10:14 EDT
Nmap scan report for 192.168.50.105
Host is up (0.00040s latency).
All 1000 scanned ports on 192.168.50.105 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:5E:41:D7 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 38.64 seconds
```

```
(root@kali)-[/home/kali]
# nmap 192.168.50.105 --script smb-os-discovery
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 10:32 EDT
Nmap scan report for 192.168.50.105
Host is up (0.00093s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5357/tcp   open  wsdapi
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
MAC Address: 08:00:27:5E:41:D7 (Oracle VirtualBox virtual NIC)

Host script results:
| smb-os-discovery:
|   OS: Windows 7 Ultimate 7601 Service Pack 1 (Windows 7 Ultimate 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: ivona-PC
|   NetBIOS computer name: IVONA-PC\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2022-08-03T16:32:43-07:00

Nmap done: 1 IP address (1 host up) scanned in 18.49 seconds
```

	IP	OS	MAC
Kali Linux	192.168.50.100	Linux	
Windows 7	192.168.50.105	Windows 7 Ultimate 6.1	08:00:27:5E:41:D7
Metasploitable	192.168.50.101	Unix Samba 3.0.20-Debian	08:00:27:A0:DF:56