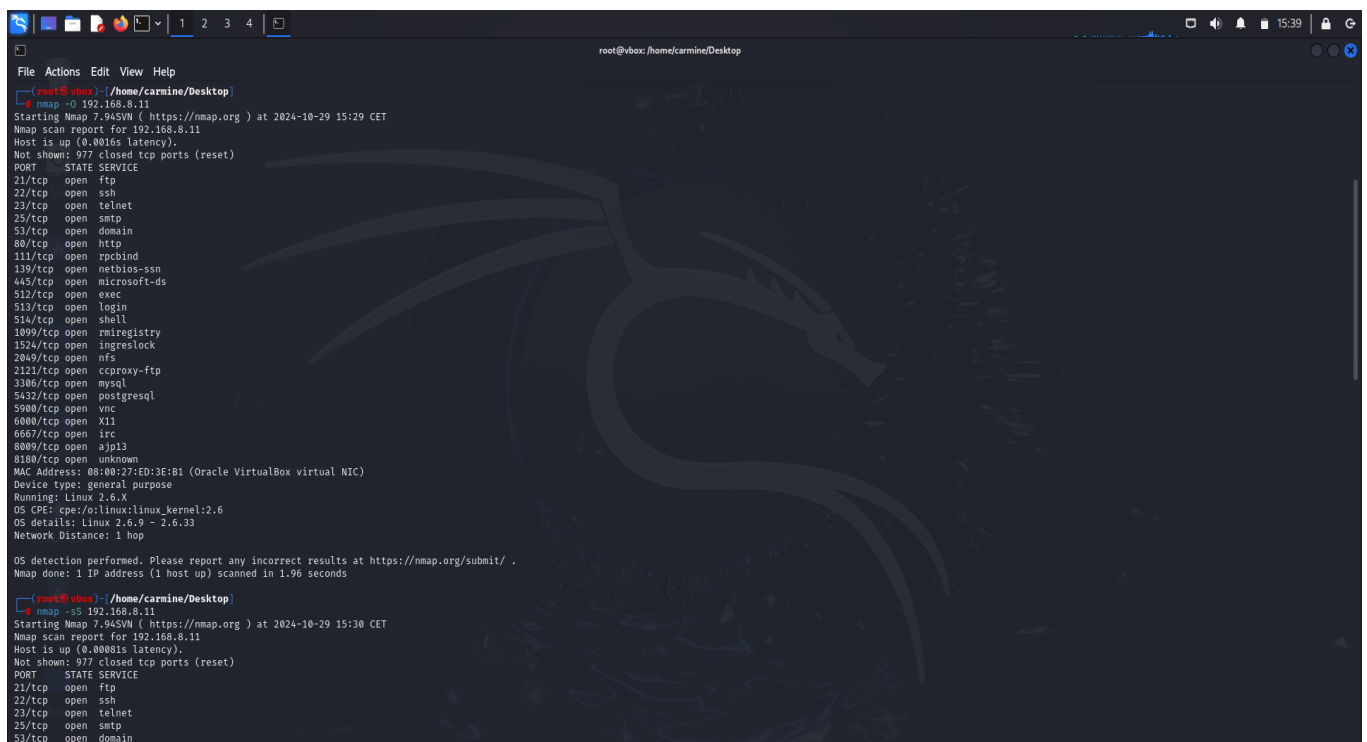


SCANSIONE NMAP

Nmap è (Network Mapper) è un potente strumento open-source utilizzato per scansionare le reti:

- **Identificare host attivi:** Scoprire quali computer o dispositivi sono connessi alla tua rete.
- **Determinare servizi e applicazioni:** Individuare quali servizi (come HTTP, FTP, SSH) sono in esecuzione su ciascun host e su quali porte.
- **Riconoscere sistemi operativi:** Identificare il sistema operativo in uso su ciascun dispositivo.
- **Scoprire vulnerabilità:** Con l'aiuto di script aggiuntivi, Nmap può rilevare potenziali vulnerabilità nei sistemi.

Dopo aver aperto un terminale in Kali andiamo ad eseguire il comando `sudo su` per passare in root ed eseguire successivamente i comandi `nmap`. Poi andiamo ad aprire `metasploitable2` ed eseguiamo il comando `ip addr` per vedere il suo ip che è 192.168.8.11.



```
root@vbox: /home/carmino/Desktop
File Actions Edit View Help
root@vbox ~ - ssh - /home/carmino/Desktop
nmap -O 192.168.8.11
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 15:29 CET
Nmap scan report for 192.168.8.11
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
1924/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:ED:3E:B1 (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

root@vbox ~ - ssh - /home/carmino/Desktop
nmap -sS 192.168.8.11
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 15:30 CET
Nmap scan report for 192.168.8.11
Host is up (0.00081s 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
```

Qui abbiamo usato il comando `nmap -O 192.168.8.11` che ci da il sistema operativo in uso.

```
root@vbox: /home/carmin/Desktop
File Actions Edit View Help

root@vbox: /home/carmin/Desktop
# nmap -sT 192.168.8.11
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 15:32 CET
Nmap scan report for 192.168.8.11
Host is up (0.0022s 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  cproxy-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:ED:3E:B1 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds

root@vbox: /home/carmin/Desktop
# nmap -sV 192.168.8.11
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 15:38 CET
Nmap scan report for 192.168.8.11
Host is up (0.00076s 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 rshcd
```

Qui abbiamo eseguito il comando **nmap -sT 192.168.8.11**, indica una **scansione SYN**. In una scansione SYN, Nmap invia un pacchetto TCP SYN al target per ogni porta. Se la porta è aperta, il sistema target risponde con un pacchetto SYN-ACK. Nmap invia quindi un pacchetto RST per abortire la connessione. Questo metodo è relativamente discreto poiché non stabilisce una connessione completa.

```
root@vbox: /home/carmina/Desktop
File Actions Edit View Help

root@vbox: /home/carmina/Desktop
nmap -sS 192.168.8.11
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 15:30 CET
Nmap scan report for 192.168.8.11
Host is up (0.00001s 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
1924/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:ED:3E:B1 (Oracle VirtualBox virtual NIC)

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

root@vbox: /home/carmina/Desktop
nmap -sT 192.168.8.11
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 15:32 CET
Nmap scan report for 192.168.8.11
Host is up (0.0022s 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
```

Qui abbiamo usato il comando **nmap -sS 192.168.8.11** viene usato per "TCP SYN Scan" è anche conosciuta come "half-open scan" perché non stabilisce una connessione TCP completa. Invia pacchetti SYN e attende una risposta SYN/ACK (indicando una porta aperta) o RST (indicando una porta chiusa). Se riceve un SYN/ACK, invia un pacchetto RST per terminare la connessione, senza completare la stretta di mano TCP.

```
root@vbox: /home/carmine/Desktop
File Actions Edit View Help
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:ED:3E:B1 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds

root@vbox: /home/carmine/Desktop
nmap -sV 192.168.8.11
Starting Nmap 7.94SVN (https://nmap.org) at 2024-10-29 15:38 CET
Nmap scan report for 192.168.8.11
Host is up (0.00075s 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 rshcd
513/tcp   open  login          OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi       GNU Classpath gmicregistry
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-Subuntu5
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:ED:3E:B1 (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 17.08 seconds

root@vbox: /home/carmine/Desktop
```

Qui abbiamo eseguito il comando **nmap -sV 192.168.8.11**, quando utilizzi l'opzione -sV con Nmap, il programma invia una serie di pacchetti di probe ai servizi sulle porte aperte e analizza le risposte. Questo processo è una forma avanzata di banner grabbing. Nmap confronta le risposte ottenute con un database di firme per identificare il servizio e la versione in esecuzione.

Differenza tra scansione syn e tcp connect:

- La scansione syn è più veloce e meno dettagliata. Nmap invia un pacchetto TCP SYN alla porta target. Se la porta è aperta, il sistema target risponde con un pacchetto SYN-ACK. Nmap invia quindi un pacchetto RST per abortire la connessione senza stabilirla completamente.
- La tcp connect è più lenta e più dettagliata, Nmap tenta di stabilire una connessione TCP completa con la porta target. Se la connessione viene stabilita, la porta è considerata aperta.