

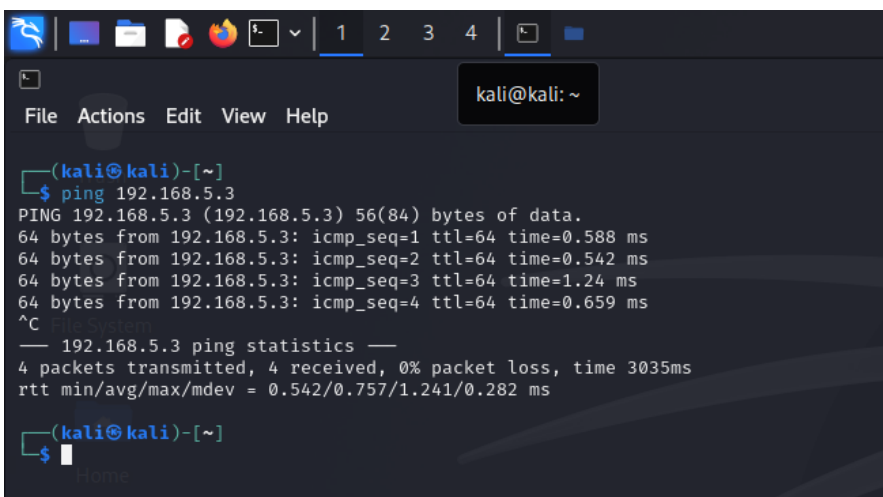
Traccia: Tecniche di scansione con Nmap

Si richiede allo studente di effettuare le seguenti scansioni sul target Metasploitable:

- OS fingerprint
- Syn Scan
- TCP connect - trovate differenze tra i risultati della scansioni TCP connect e SYN?
- Version detection

Per lo svolgimento dell'esercizio per prima cosa dobbiamo permettere a kali linux e metasploitable di essere sulla stessa rete, quindi procediamo a testare le macchine con un ping:

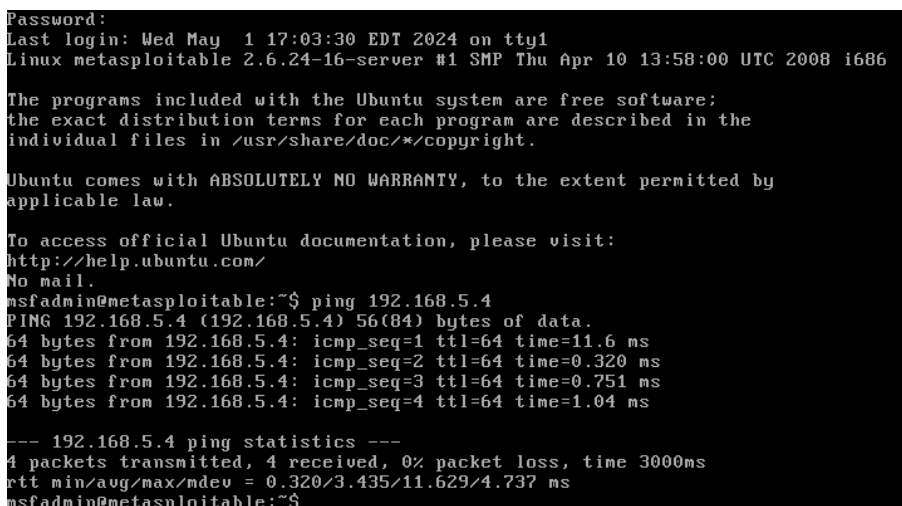
- Ping da kali linux a metasploitable



```
(kali㉿kali)-[~]
$ ping 192.168.5.3
PING 192.168.5.3 (192.168.5.3) 56(84) bytes of data:
64 bytes from 192.168.5.3: icmp_seq=1 ttl=64 time=0.588 ms
64 bytes from 192.168.5.3: icmp_seq=2 ttl=64 time=0.542 ms
64 bytes from 192.168.5.3: icmp_seq=3 ttl=64 time=1.24 ms
64 bytes from 192.168.5.3: icmp_seq=4 ttl=64 time=0.659 ms
^C
--- 192.168.5.3 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3035ms
rtt min/avg/max/mdev = 0.542/0.757/1.241/0.282 ms

(kali㉿kali)-[~]
$
```

- Ping da metasploitable a kali linux



```
Password:
Last login: Wed May  1 17:03:30 EDT 2024 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

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/
No mail.
msfadmin@metasploitable:~$ ping 192.168.5.4
PING 192.168.5.4 (192.168.5.4) 56(84) bytes of data:
64 bytes from 192.168.5.4: icmp_seq=1 ttl=64 time=11.6 ms
64 bytes from 192.168.5.4: icmp_seq=2 ttl=64 time=0.320 ms
64 bytes from 192.168.5.4: icmp_seq=3 ttl=64 time=0.751 ms
64 bytes from 192.168.5.4: icmp_seq=4 ttl=64 time=1.04 ms
--- 192.168.5.4 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3000ms
rtt min/avg/max/mdev = 0.320/3.435/11.629/4.737 ms
msfadmin@metasploitable:~$
```

Adesso procediamo con le scansioni da parte di kali linux a metasploitable.

- OS fingerprint : utilizzando il flag -O , nmap cercherà di determinare il sistema operativo dell' host.

```
kali@kali:~$ nmap -sS 192.168.5.3
Nmap scan report for 192.168.5.3
Host is up (0.0000s 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
6067/tcp  open  irc
8080/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:70:24:F2 (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 1.60 seconds
```

- Syn Scan : il flag -sS indica a nmap di utilizzare la scansione tcp syn. Durante questa scansione , nmap invia un pacchetto syn al target per stabilire una connessione, se quest'ultimo risponde con un pacchetto syn/ack , nmap lo interpreterà come aperta.

```
kali@kali:~$ nmap -sS 192.168.5.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-01 17:24 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.5.3
Host is up (0.00019s 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
6067/tcp  open  irc
8080/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:70:24:F2 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds
```

- TCP connect : Durante questa scansione, Nmap tenta di stabilire una connessione completa con ciascuna porta dell'host. Se la porta è aperta, Nmap completa la connessione e la considera aperta. Altrimenti, se la porta è chiusa, Nmap riceve un rifiuto di connessione (RST) e la considera chiusa. Possiamo quindi dire che in questa scansione completiamo il II Three-way handshake.

```
kali@kali:~$ sudo nmap -sT 192.168.5.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-01 17:27 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.5.3
Host is up (0.00051s 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  miregistry
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
8080/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:7B:24:F2 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds

kali@kali:~$
```

- Version detection : Il comando `nmap -sV` esegue una scansione delle porte utilizzando il metodo TCP Connect scan e include anche il rilevamento delle versioni dei servizi. Questo può essere utile per comprendere meglio quali servizi sono in esecuzione e se potrebbero essere vulnerabili.

```
kali@kali:~$ sudo nmap -sV 192.168.5.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-01 17:28 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.5.3
Host is up (0.00034s 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?
25/tcp    open  smtp?
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?
514/tcp   open  shell?
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  ccproxy-ftp
3306/tcp  open  mysql?
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
8080/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:7B:24:F2 (Oracle VirtualBox virtual NIC)
Service Info: Host: irc.Metasploitable.LAN; OS: 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 180.31 seconds

kali@kali:~$
```

trovare differenze tra i risultati della scansioni TCP connect e SYN

la differenza sostanziale tra i due tipi di scansione è che la prima completa il Three-way handshake, la seconda non ha bisogno di completare il Three-way handshake perché invia un pacchetto syn per sapere se la porta è aperta e subito dopo chiude la connessione.

Possiamo dire che in fase di rilevamento di eventuali firewall la scansione syn potrebbe essere meno intrusiva e quindi potenzialmente potrebbe creare meno rilevamenti. La scansione completa tcp invece è più intrusiva e quindi potrebbe fare attivare qualche meccanismo di difesa.

