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.

E la seguente sul target Windows:

• OS fingerprint.

Analizziamo il seguente scenario: macchina kali IP 192.168.178.51 macchina MetaSploitable IP 192.168.178.54

dopo aver eseguito il comando nmap -sn 192.168.178.0/24 abbiamo ottenuto il seguente risultato.

```
Att 1000 scanned ports on Kall.fritz.box (192.168.1/8.51) are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (6 hosts up) scanned in 19.56 seconds

(root@kall)-[/home/kali]

(mmap -sn 192.168.178.0/24

Starting Nmap 7.945VN (https://nmap.org ) at 2024-10-29 11:27 EDT

Nmap scan report for fritz.box (192.168.178.1)

Host is up (0.00080s latency).

MAC Address: 2C:3A:FD:27:37:55 (AVM Audiovisuelles Marketing und Computersysteme GmbH)

Nmap scan report for DESKTOP-F29SN04.fritz.box (192.168.178.24)

Host is up (0.00032s latency).

MAC Address: 10:69:7A:98:98:A6:96 (EliteGroup Computer Systems)

Nmap scan report for 192.168.178.27

Host is up (0.024s latency).

MAC Address: 25:F8A:B8:A9:68 (Unknown)

Nmap scan report for amazon-5c0034c42.fritz.box (192.168.178.29)

Host is up (0.081s latency).

MAC Address: 05:54:D7:66:3C:56 (Amazon Technologies)

Nmap scan report for 192.168.178.54

Host is up (0.00035s latency).

MAC Address: 08:00:27:20:F7:58 (Oracle VirtualBox virtual NIC)

Nmap scan report for kali.fritz.box (192.168.178.51)

Host is up.

Nmap done: 256 IP addresses (6 hosts up) scanned in 13.79 seconds
```

Da qui possiamo intendere che la MetaSploitable potrebbe essere la macchina 192.168.178.54.

Eseguendo il comando nmap -sV 192.168.178.54 otteniamo:

```
-(<mark>root@kali</mark>)-[/home/kali
/ nmap -sV 192.168.178.54
Starting Nmap 7.945VN (https://nmap.org ) at 2024-10-29 07:20 EDT Nmap scan report for 192.168.178.54 Host is up (0.00057s latency).

Not shown: 977 closed tcp ports (reset)

PORT STATE SERVICE VERSION

21/fcp. open fits version 2.2 /
                                       SERVICE VERSION

ftp vsftpd 2.3.4

ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)

telnet Linux telnetd

smtp Postfix smtpd

domain ISC BIND 9.4.2

http Apache httpd 2.2.8 ((Ubuntu) DAV/2)

rpcbind 2 (RPC #100000)

netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
                         open ftp
open ssh
 21/tcp
22/tcp
23/tcp
 25/tcp
                         open
 53/tcp
                         open
open
53/tcp open
80/tcp open
111/tcp open
139/tcp open
445/tcp open
512/tcp open
513/tcp open
514/tcp open
1099/tcp open
1524/tcp open
2049/tcp open
                                                                           OpenBSD or Solaris rlogind
                                          tcpwrapped
                                         java-rmi
bindshell
                                                                           GNU Classpath grmiregistry
Metasploitable root shell
2049/tcp open
2121/tcp open
3306/tcp open
5432/tcp open
                                                                           Metasploitable foot shell
2-4 (RPC #100003)
ProFTPD 1.3.1
MySQL 5.0.51a-3ubuntu5
PostgreSQL DB 8.3.0 - 8.3.7
VNC (protocol 3.3)
(access denied)
                                        nfs
ftp
                                         mysql
postgresql
5900/tcp open
6000/tcp open
                                                                            UnrealIRCd
6667/tcp open irc
8009/tcp open ajp
8009/tcp open ajp13 Apache Jserv (Protocol v1.3)
8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:2D:F7:58 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_k
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ . Nmap done: 1 IP address (1 host up) scanned in 65.26 seconds
```

Da qui capiamo che la macchina 192.168.178.54 è effettivamante la MetaSploitable. Con il comando nmap -sS 192.168.178.54 andremo a vedere le porte aperte ed i relativi servizi.

```
<u>-</u>
                                                                                                              root@kali: /home/kali
 File Actions Edit View Help
__(root@ kail) = [/home/kali]
# nmap -sS 192.168.178.54
Starting Nmap 7.945VN ( https://nmap.org ) at 2024-10-29 08:22 EDT
Nmap scan report for 192.168.178.54
Host is up (0.00062s latency).
Not shown: 977 closed tcp ports (reset)
PORT STATE SERVICE
21/17cp open fit
                open ftp
open ssh
21/tcp
                  open telnet
open smtp
23/tcp
25/tcp
53/tcp
80/tcp
                   open domain
open http
80/tcp open http
111/tcp open rpcbind
139/tcp open metbios-ssn
445/tcp open microsoft-ds
512/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
6000/tcp open
6667/tcp open irc
8009/tcp open ajp13
8180/tcp open unknown
MAC Address: 08:00:27:2D:F7:58 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.48 seconds
root@kali)-[/home/kali]
```

Potremmo ottenere un risultato simile con nmap -sT 192.168.178.54 con la differenza che il primo (-sS) andrà a stabilire la connessione solo con un Ack e ciò significa che sarà poco riconoscibile da firewall e riuscirà ad essere più in incognito; invece il comando (-sT) andrà a creare una Ack/syn-ack/ack.

L'utlizzo di nmap come strumento per un ottenere informazioni sull'azienda cliente è uno strumento molto malleabile e potente che ci consente di avere un chiaro quadro della situazione della rete aziendale.

Otteniamo un mapping di rete chiaro ed esaustivo grazie al quale riusciamo ad analizzare debolezze e vulenrabilità della rete in esame.

Antonio Bevilaqua