29/10/2024

Traccia:

Tecniche di scansione con Nmap

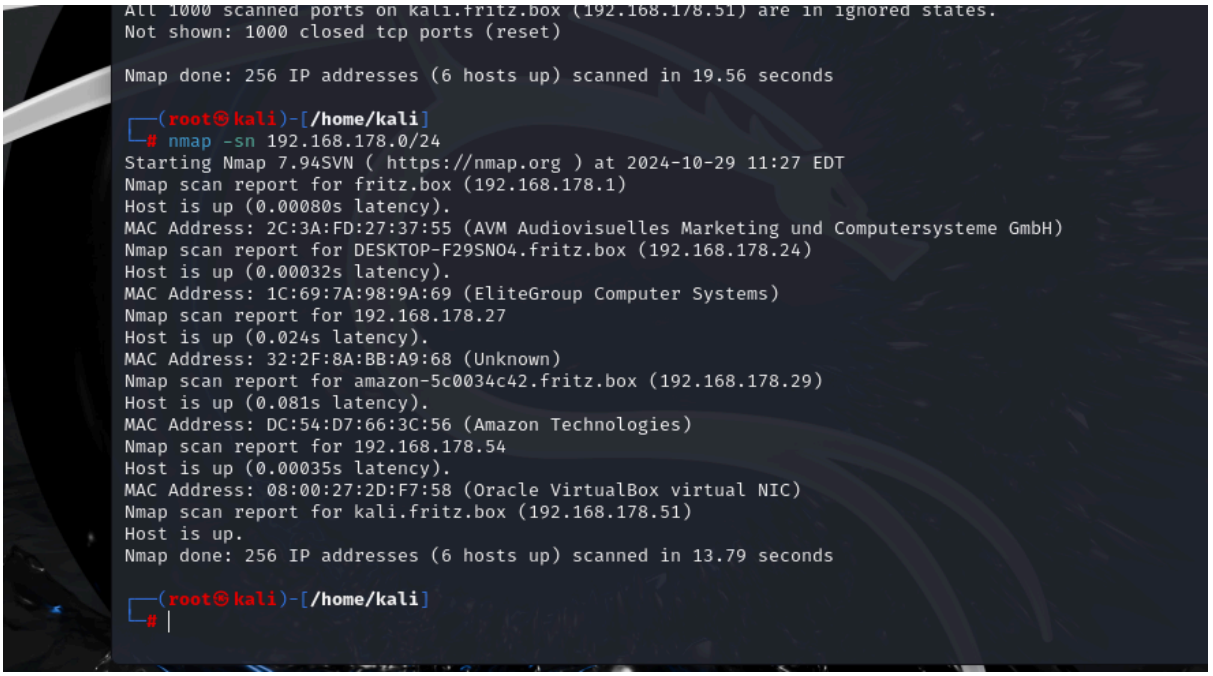
Si richiede allo studente di effettuare le seguenti scansioni sul target Metasploitable:

- 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.



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:

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.178.54
Starting Nmap 7.94SVN ( 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/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?
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
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: 08:00:27:2D:F7:58 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_k
ernel

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.

```
root@kali: /home/kali
File  Actions  Edit  View  Help

┌──(root㉿kali)-[/home/kali]
└─# nmap -sS 192.168.178.54
Starting Nmap 7.94SVN ( 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/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: 08:00:27:2D: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