S5/L1 Progetto Paolo Tavian

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.

A valle delle scansioni è prevista la produzione di un report contenente le seguenti info (dove disponibili):

- IP.
- Sistema Operativo.
- Porte Aperte.
- Servizi in ascolto con versione.

Ipotizzando di essere in una white box e dobbiamo scoprire diverse informazioni su una macchia Metasploitable2.
Per scoprirlo utilizziamo il software NMAP:
E' utilizzato per l'esplorazione della rete, analizza i sistemi e scopre quali porte sono aperte e quali servizi sono attivi su una macchina host:
Ecco un elenco:

- Scansione porte
- Scansione servizi
- Scansione di rete
- NSE (Script): usa degli script (creati da noi) per automatizzare varie attività tipo l'identificazione delle vulnerabilità

Il proprietario ci ha gentilmente fornito L'indirizzo IP della macchina "vittima" 192.168.1.253

SISTEMA OPERATIVO

Per prima cosa cerchiamo la versione del sistema operativo

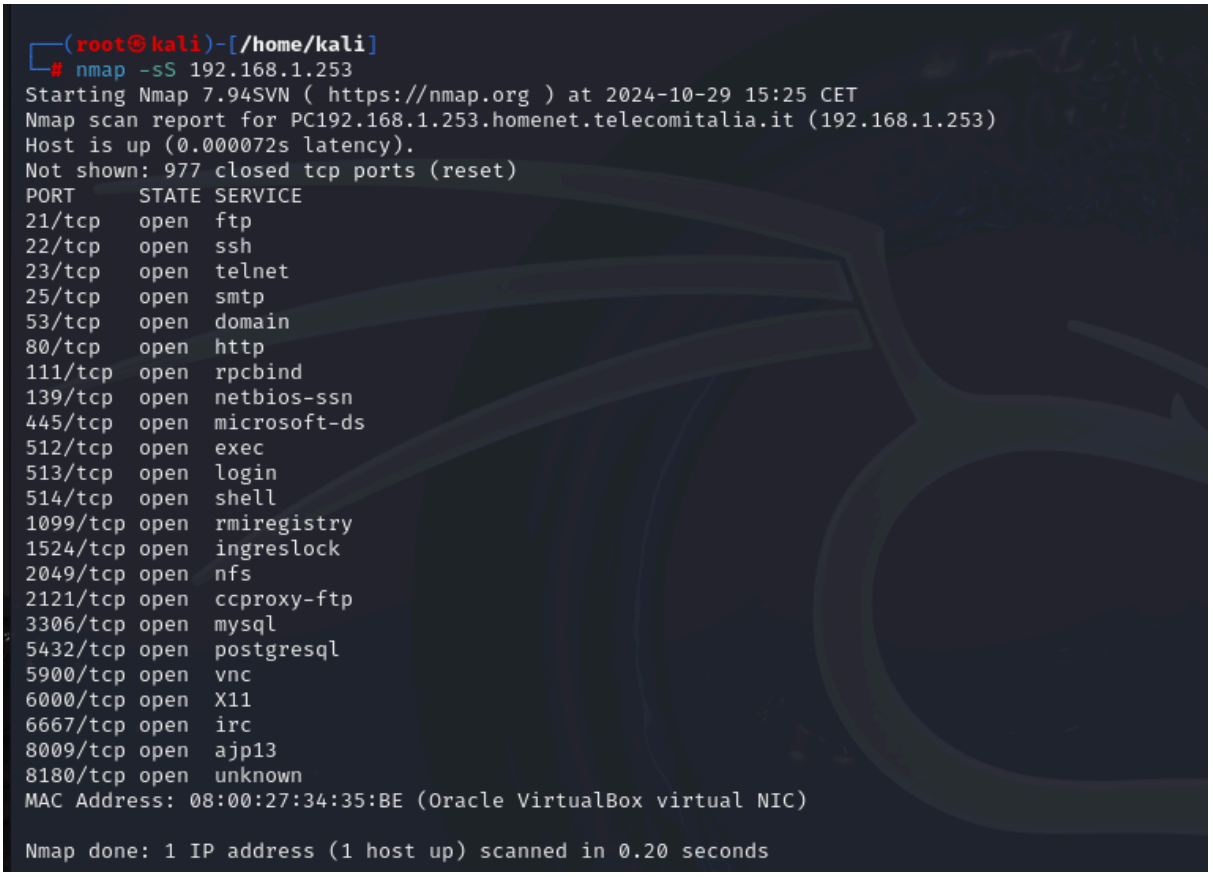
Utilizziamo il comando nmap -o

Possiamo individuare la versione dell'OS, in questo caso la macchina
Running Linux 2.6.X
Linux 2.6.9 - 2.6.33

ATTENZIONE!!!

Per avere una migliore raccolta di informazioni; utilizziamo i privilegi di amministratore così possiamo ottenere maggiori risultati.

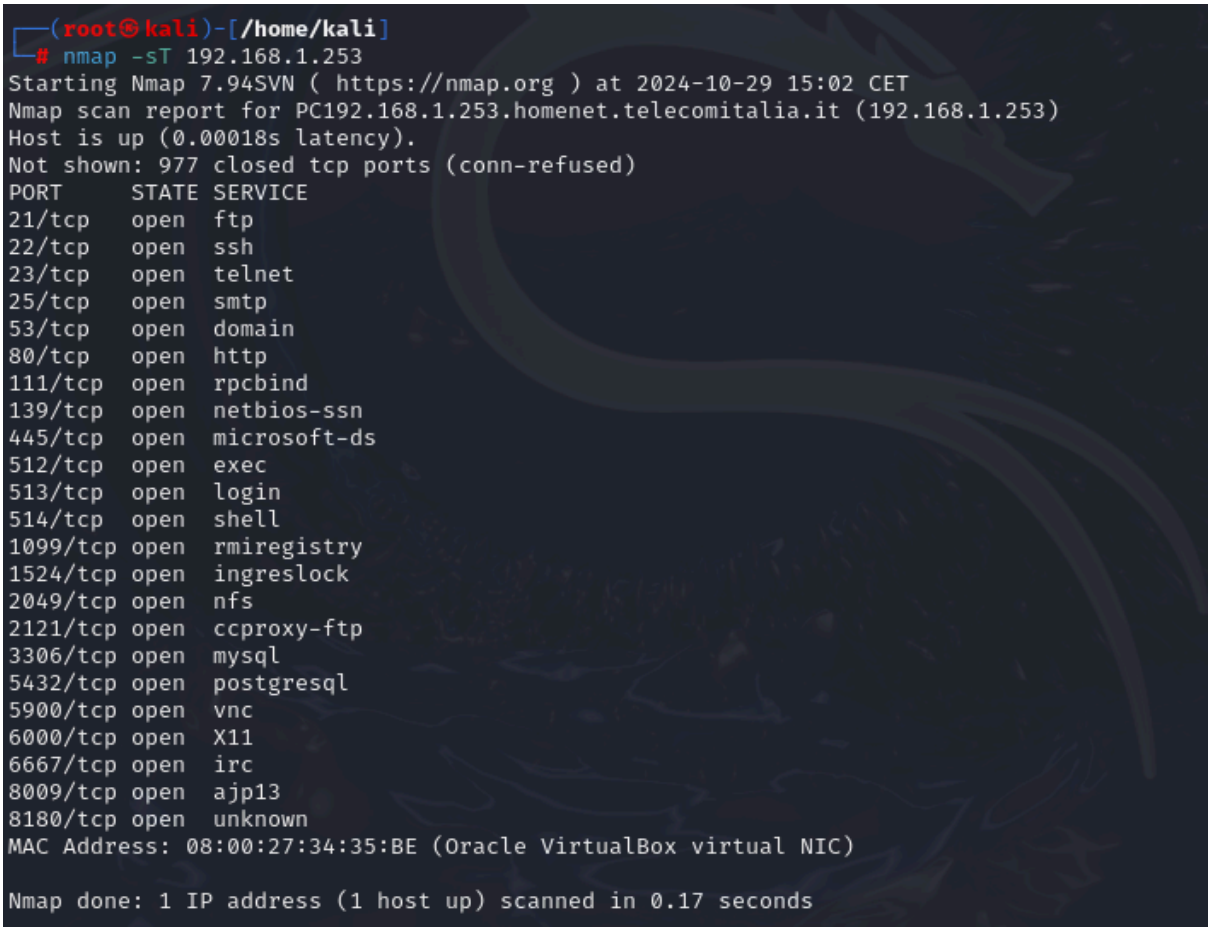
SYN SCAN RACCOLTA INFORMAZIONI



Utilizzando il comando nmap -sS andiamo a creare una richiesta syn per la macchina “vittima”:
La comunicazione sarà soltanto attraverso una richiesta syn, una risposta ack ed infine un pacchetto reset che blocca la comunicazione

Il comando viene utilizzato quando si vuole essere silenziosi o non farsi scoprire dal proprietario

RICHIESTA TCP



Per creare una richiesta TCP usiamo il comando nmap -sT
La comunicazione sarà attraverso una richiesta syn, una risposta syn-ack ed infine un ack di risposta
Viene utilizzato quando dobbiamo stabilire una connessione completa ma ad un costo: saremo visibili

La differenza tra i due comandi è che -sT crea una richiesta completa mentre l'altro (-sS) utilizza una connessione con solo un syn

VERSION DETECTION

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.1.253
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 15:17 CET
Nmap scan report for PC192.168.1.253.homenet.telecomitalia.it (192.168.1.253)
Host is up (0.00010s 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
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: 08:00:27:34:35:BE (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 64.77 seconds
```

Per scoprire la versione dei servizi utilizzati nelle porte utilizziamo il comando nmap -sV

BONUS OS DI WINDOWS

Ci hanno anche chiesto di trovare la versione del OS della macchina windows 192.168.1.252

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -O 192.168.1.252
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 15:26 CET
Nmap scan report for PC192.168.1.252 (192.168.1.252)
Host is up (0.00012s latency).
Not shown: 991 closed tcp ports (reset)
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:B6:CE:BB (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:mic
rosoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
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 7.06 seconds
```