Esercitazione S5L2

In questa esercitazione vediamo il funzionamento di “nmap”.
Nmap è un software utile per creare una mappatura della rete, scansionando e individuando i dispositivi nella stessa.
Ho utilizzato Metaspoitable come macchina target per effettuare i test della rete.
Con nmap possiamo personalizzare le richieste che vengono effettuate per modellarle affinché siano più utili all’utilizzo che dobbiamo farne, ad esempio si può essere più o meno “silenziosi” e lasciare meno tracce possibili.
Nmap dispone di diversi comandi per raccogliere informazioni, in questo caso ho utilizzato:

- OS fingerprint
- SYN scan
- TCP connect
- Version detection

OS FINGERPRINT

Con l’OS fingerprint si può vedere il sistema operativo attivo sulla macchina di destinazione della scansione.
Si può vedere in figura la procedura utilizzata con il comando “nmap -O”.
Il risultato è visibile dopo la lista delle porte aperte (OS details:).
Questo comando è utile per raccogliere informazioni e capire se il S.O. attivo sull’host possa avere delle vulnerabilità.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -O 192.168.1.12
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 09:47 EDT
Nmap scan report for PENTOLAPTOP.station (192.168.1.12)
Host is up (0.00035s 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:E6:BE:7F (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 1.67 seconds
```

SYN SCAN – TCP CONNECT

Finito questo comando ho utilizzato “SYN scan” e “TCP connect”, sono due comandi simili per raccogliere informazioni sulle porte aperte. Si stabilisce nel caso del “TCP connect” una connessione TCP completa (con scambio di SYN-SYN\ACK-ACK) con l’host di destinazione. Ciò ci porterà ad avere come output la lista delle porte aperte e i servizi associati ad esse.
Con “SYN scan”, invece, non ci sarà una connessione TCP completa ma lo scambio verrà chiuso da un segnale di RST(reset). In output abbiamo dei risultati simili, la differenza sta

appunto nello scambio di pacchetti che è diverso, in base alle situazioni e alle nostre necessità si può utilizzare uno piuttosto che l'altro.
Nel dettaglio il "SYN scan" non effettuando la connessione completa TCP è molto più silenzioso e lascia meno tracce, ci vogliono i permessi di amministratore (root) per poterla fare ed è solitamente più veloce.
Di seguito allego le foto dei test dove si può vedere la minima differenza prima dell'elenco delle porte aperte:

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sT 192.168.1.12
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 09:32 EDT
Nmap scan report for PENTOLAPTOP.station (192.168.1.12)
Host is up (0.00026s 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  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:E6:BE:7F (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS 192.168.1.12
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 09:33 EDT
Nmap scan report for PENTOLAPTOP.station (192.168.1.12)
Host is up (0.00018s 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:E6:BE:7F (Oracle VirtualBox virtual NIC)

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

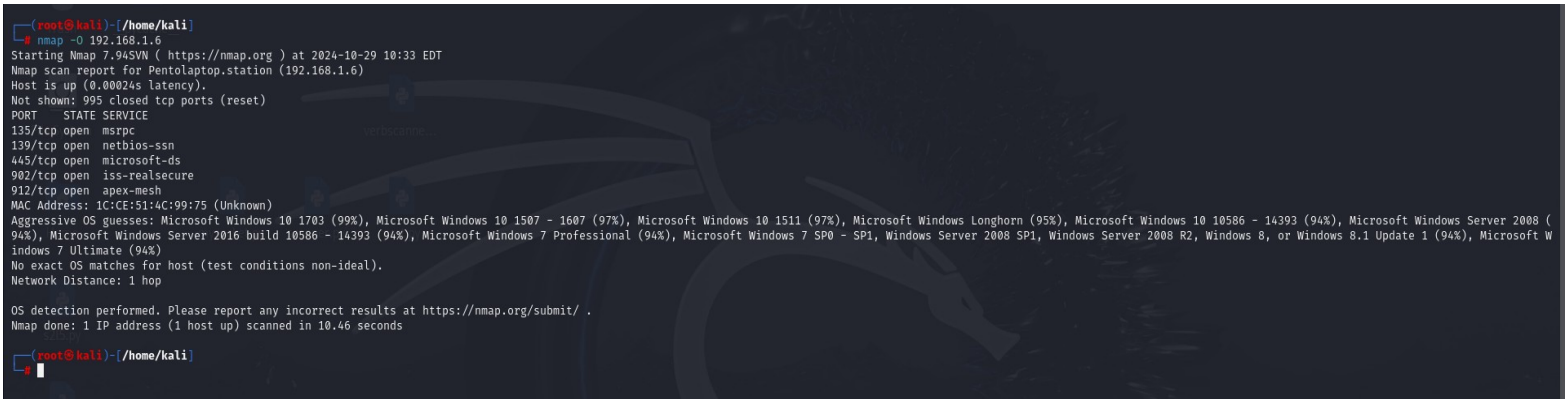
VERSION DETECTION

Come ultimo comando utilizzato ho utilizzato il "Version detection", questo ci permette di raccogliere informazioni sui servizi e la loro versione in esecuzione sulle porte aperte. Conoscere la versione dei servizi ci è utile per avere ulteriori informazioni sul servizio attivo e riconoscere se ci sono vulnerabilità nel sistema.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.1.12
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 11:22 EDT
Nmap scan report for PENTOLAPTOP.station (192.168.1.12)
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:E6:BE:7F (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 64.78 seconds
```

Infine come bonus ho provato a fare un OS fingerprint su windows 11.
Ho notato che con il firewall attivo (Windows defender) non è stato possibile ricevere informazioni. Disabilitando il firewall invece sono riuscito ad effettuare la connessione ed a ricevere le informazioni richieste.



Ho provato anche il comando “-A” per fare una richiesta aggressiva e ricavare tutte le informazioni possibili.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -A -T4 192.168.1.6
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 10:33 EDT
Nmap scan report for Pentolaptop.station (192.168.1.6)
Host is up (0.00027s latency).
Not shown: 995 closed tcp ports (reset)
PORT    STATE SERVICE         VERSION
135/tcp open  msrpc           Microsoft Windows RPC
139/tcp open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds?
902/tcp open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912/tcp open  vmware-auth     VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
MAC Address: 1C:CE:51:4C:99:75 (Unknown)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=10/29%OT=135%CT=1%CU=41123%PV=Y%DS=1%DC=D%G=Y%M=1CC
OS:E51%TM=6720F266%P=x86_64-pc-linux-gnu)SEQ(SP=100%GCD=1%ISR=106%TI=I%CI=I
OS:%II=I%SS=S%TS=A)SEQ(SP=103%GCD=1%ISR=109%TI=I%CI=I%II=I%SS=S%TS=A)OPS(O1
OS:=M5B4NW8ST11%O2=M5B4NW8ST11%O3=M5B4NW8NNT11%O4=M5B4NW8ST11%O5=M5B4NW8ST1
OS:1%O6=M5B4ST11)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FFFF)ECN(R=
OS:Y%DF=Y%T=80%W=FFFF%O=M5B4NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+%F=AS%R
OS:D=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T=80%W=0
OS:%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T5(
OS:R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S=A%A=O%
OS:F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N
OS:%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=80%C
OS:D=Z)

Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_nbstat: NetBIOS name: PENTOLAPTOP, NetBIOS user: <unknown>, NetBIOS MAC: 1c:ce:51:4c:99:75 (unknown)
| smb2-time:
|   date: 2024-10-29T14:34:10
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required

TRACEROUTE
HOP RTT     ADDRESS
1   0.27 ms Pentolaptop.station (192.168.1.6)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.05 seconds
```