

ESERCITAZIONE S5/L2

TRACCIA: Tecniche di scansione con Nmap

È stato richiesto allo studente di effettuare le seguenti scansioni sul target Metasploitable: OS fingerprint, Syn Scan, TCP connect, Version detection e di trovare differenze tra i risultati della scansioni TCP connect e SYN

E la seguente sul target Windows: OS fingerprint.

SVOLGIMENTO

Ho svolto l'esercizio tramite l'utilizzo dello strumento nMap, network mapping, strumento open-source estremamente potente e versatile per la scansione della rete e l'identificazione dei dispositivi e dei servizi. Le sue funzioni principali sono quattro:

- Scansione degli Host: Identifica gli host attivi all'interno di una rete.
- Identificazione dei Servizi: Rileva i servizi in esecuzione su ciascun host
- Rilevamento dei Sistemi Operativi: Utilizza varie tecniche di fingerprinting per determinare il sistema operativo in esecuzione su un host.
- Scansione delle Vulnerabilità: Può essere utilizzato per identificare potenziali vulnerabilità.

```
(kali@kali)~$ sudo su
[sudo] password for kali:
(root@kali) /home/kali# nmap -O 192.168.1.194
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 07:31 EDT
Nmap scan report for 192.168.1.194
Host is up (0.0010s 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
8080/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:E4:6F:D3 (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 2.05 seconds
```

Prima di tutto ho recuperato l'indirizzo IP dalla macchina virtuale di Metasploitable2: 192.168.1.194.

Successivamente per lo svolgimento dell'esercizio, nel terminale della macchina di Kali Linux, ho utilizzato i comandi "nmap -O" per il rilevamento del Sistema Operativo, che ha la funzione di determinare il sistema operativo dell'host di destinazione.

Il **sistema operativo** risulta: Linux 2.6.9 - 2.6.33

Una volta trovato il Sistema Operativo vengono effettuati i comandi di identificazione dei Servizi, nello specifico, TCP Connect che esegue una scansione che stabilisce connessioni TCP (nmap -sT) e SYN Scan, che esegue una scansione "half-open", inviando pacchetti SYN e attendendo risposte SYN/ACK (nmap -sS).

```
(root@kali) /home/kali# nmap -sT 192.168.1.194
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 10:08 EDT
Nmap scan report for 192.168.1.194
Host is up (0.0092s 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
8080/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:E4:6F:D3 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.51 seconds
```

```
(kali@kali)~$ sudo su
[sudo] password for kali:
(root@kali) /home/kali# nmap -sS 192.168.1.194
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 10:07 EDT
Nmap scan report for 192.168.1.194
Host is up (0.0048s 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
8080/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:E4:6F:D3 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.73 seconds
```

Nell'immagine a sinistra comando nmap -sT, a destra invece nmap -sS

ESERCITAZIONE S5/L2

La differenza tra SYN Scan e TCP Connect, sta nella comunicazione. Come possiamo vedere nelle immagini precedenti prima delle porte appaiono, in quella di sinistra la voce "conn-refused" mentre in quella di destra "reset". La sostanziale differenza è proprio che nel caso del SYN Scan non viene completata 3-way-handshake, chiudendo la comunicazione con un pacchetto RST (reset), risultando meno invasivo generando meno rumore al livello di rete.

Infine con lo strumento "nmap -sV" sono state individuate le versioni dei servizi attivi.

Porte aperte: Sono state individuate 22 porte aperte.

```
(root@kali): ~/home/kali
nmap -sV 192.168.1.194
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 10:10 EDT
Nmap scan report for 192.168.1.194
Host is up (0.00077s 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 Subuntu1 (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         netkit-rsh rexecd
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          ProFTPD 1.3.1
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:E4:6F:D3 (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 12.50 seconds
```

Versioni e servizi attivi:

- Porta 21, si riferisce al servizio FTP versione vsftpd 2.3.4
- Porta 22, si riferisce al servizio SSH versione OpenSSH 4.7p1 Debian Subuntu1 (protocollo 2.0)
- Porta 23, si riferisce al servizio TELNET versione Linux telnetd
- Porta 25, si riferisce al servizio SMTP versione postfix smtpd
- Porta 139, si riferisce al servizio Netbois-ssn versione Samba smbd 3.X, 4.X (workgroup: WORKGROUP)

Come esercizio bonus, utilizzando come target Windows, bisognava determinare il Sistema Operativo con il comando "nmap -O" sempre dal terminale terminale di Kali

```
Prompt dei comandi
Suffisso DNS specifico per connessione: lan
Indirizzo IPv6 . . . . . : 2a0d:3344:3206:6010::da1
Indirizzo IPv6 . . . . . : 2a0d:3344:3206:6010:3480:1bda:5d0b:9f4b
Indirizzo IPv6 . . . . . : fdc1:5ae8:b4dc:10::da1
Indirizzo IPv6 . . . . . : fdc1:5ae8:b4dc:10:3480:1bda:5d0b:9f4b
Indirizzo IPv6 temporaneo. . . . . : 2a0d:3344:3206:6010:ec86:af0:e7ee:82a5
Indirizzo IPv6 temporaneo. . . . . : fdc1:5ae8:b4dc:10:ec86:af0:e7ee:82a5
Indirizzo IPv6 locale rispetto al collegamento . : fe80::3480:1bda:5d0b:9f4b%3
Indirizzo IPv4 . . . . . : 192.168.1.26
Subnet mask . . . . . : 255.255.255.0
Gateway predefinito . . . . . : fe80::7624:9fff:fe77:ebb6%3
192.168.1.1

Scheda Tunnel Tereedo Tunneling Pseudo-Interface:
Suffisso DNS specifico per connessione:
Indirizzo IPv6 . . . . . : 2001:0:2851:782c:30d2:1517:277f:e546
Indirizzo IPv6 locale rispetto al collegamento . : fe80::30d2:1517:277f:e546%4
Gateway predefinito . . . . . :

Scheda Tunnel isatap.lan:
Stato supporto. . . . . : Supporto disconnesso
Suffisso DNS specifico per connessione: lan
C:\Users\user>
```

Nella prima immagine, è stato recuperato l'indirizzo IP, con il comando ipconfig, Nella seconda invece tramite il comando sopracitato è risultato il sistema operativo: Microsoft Windows 10.

```
nmap -O 192.168.1.26
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 10:20 EDT
Nmap scan report for 192.168.1.26
Host is up (0.039s latency).
Not shown: 982 closed tcp ports (reset)
PORT      STATE SERVICE
7/tcp     open  echo
9/tcp     open  discard
13/tcp    open  daytime
17/tcp    open  qotd
19/tcp    open  chargen
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1801/tcp  open  msmq
2102/tcp  open  zephyr-clt
2105/tcp  open  eklogin
2107/tcp  open  msmq-mgmt
3389/tcp  open  ms-wbt-server
5432/tcp  open  postgresql
8009/tcp  open  ajp13
8080/tcp  open  http-proxy
8443/tcp  open  https-alt
MAC Address: 08:00:27:86:C3:23 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1507 - 1607
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 5.12 seconds
```