

EPICODE

S5 - L3

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 7:

- OS fingerprint.

OS Fingerprint

Sulla macchina Metasploitable effettuiamo uno scan del sistema operativo con il comando:

```
nmap -O 192.168.50.101
```

Il flag “**-O**” nel comando nmap è utilizzato per l'identificazione del sistema operativo. Quando si esegue una scansione di rete con nmap -O, il programma cerca di determinare il sistema operativo in esecuzione sui dispositivi connessi alla rete analizzando le risposte alle sue richieste.

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 05:56 EDT
Nmap scan report for 192.168.50.101
Host is up (0.000080s 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:D4:BF:A7 (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 14.47 seconds
```

Syn Scan

Adesso effettuiamo una scansione inviando dei pacchetti Syn alla macchina Metasploitable per vedere se risponde. Il comando è il seguente:

```
nmap -sS 192.168.50.101
```

Il flag “`-sS`” nel comando nmap indica una scansione SYN. Il comando nmap invia un pacchetto **SYN** al dispositivo di destinazione e aspetta una risposta. Se riceve un pacchetto **SYN/ACK**, indica che la porta è **aperta**. Se riceve un pacchetto **RST**, la porta è **chiusa**. Questa scansione è più veloce e discreta rispetto alla scansione TCP completa, poiché non completa l'handshake TCP.

```
(root㉿kali)-[~/home/kali/Desktop]
# nmap -sS 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 05:58 EDT
Nmap scan report for 192.168.50.101
Host is up (0.000052s 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:D4:BF:A7 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.16 seconds
```

TCP Connect

Effettuiamo una scansione completa con l'invio dei pacchetti TCP verso Metasploitable con il comando:

```
nmap -sT 192.168.50.101
```

Il flag “-sT” nel comando nmap indica una scansione **TCP connect**. nmap stabilisce una connessione **TCP completa** con il dispositivo di destinazione, inviando un pacchetto di richiesta di connessione e attendendo una risposta. Se la porta è **aperta**, il dispositivo di destinazione accetta la connessione e nmap lo rileva come aperto. Al contrario la porta è chiusa.

```
(root㉿kali)-[~/home/kali/Desktop]
# nmap -sT 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 05:59 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00089s 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:D4:BF:A7 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.13 seconds
```

Version Detection

```
[root@kali]~[/home/kali/Desktop]
# nmap -sV 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 06:00 EDT
Nmap scan report for 192.168.50.101
Host is up (0.000065s 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?
25/tcp    open  smtp?
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  shell?
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  ccproxy-ftp?
3306/tcp  open  mysql?
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  unknown
MAC Address: 08:00:27:D4:BF:A7 (Oracle VirtualBox virtual NIC)
Service Info: Host: 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 192.94 seconds
```

Il comando `nmap -sV 192.168.50.101` esegue una scansione delle porte aperte su un host specificato e tenta di determinare il servizio in esecuzione su ciascuna porta aperta, oltre alla sua versione.

Nmap invierà dei pacchetti specializzati a ciascuna porta aperta e analizzerà le risposte per cercare di identificare il servizio e la sua versione.

OS Fingerprint Win7

```
└# nmap -O 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 06:13 EDT
Nmap scan report for 192.168.50.102
Host is up (0.00013s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5357/tcp   open  wsdapi
MAC Address: 08:00:27:B5:A7:64 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least
        1 open and 1 closed port
Device type: specialized|phone
Running: Microsoft Windows 7|Phone
OS CPE: cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows
OS details: Microsoft Windows Embedded Standard 7, Microsoft Windows Phone 7
            .5 or 8.0
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 21.53 seconds
```

Questo comando esegue una scansione remota per determinare il sistema operativo in esecuzione sulla macchina target. Il comando è che eseguiremo è:

```
nmap -O 192.168.50.102
```

Il flag “-O” è utilizzato per attivare il rilevamento del sistema operativo tramite Nmap. Tuttavia, se i dati ricevuti sono bloccati a causa del **firewall**, ciò indica che il dispositivo potrebbe non rispondere in modo appropriato alla richiesta di scansione del sistema operativo.

OS Fingerprint Win7 senza Firewall

```
(root㉿kali)-[~/home/kali/Desktop]
# nmap -O 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 06:21 EDT
Nmap scan report for 192.168.50.102
Host is up (0.000095s latency).
Not shown: 990 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
49157/tcp  open  unknown
MAC Address: 08:00:27:B5:A7:64 (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:microsoft: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 20.76 seconds
```

Con lo stesso comando di `nmap -O 192.168.50.102` andiamo a rieffettuare la scansione e adesso senza firewall ci sono più dati in risposta.