

Settimana 5 Esercizio 3

Utilizzo di NMAP

Oggi andremo a prendere dimestichezza con le scansioni tramite il tool NMAP.

Esso rappresenta un'ottima risorsa da utilizzare per effettuare mapping di rete per l'enumerazione dei servizi e la scansione degli host target: il mapping ci permette di conoscere dettagliatamente gli obiettivi prima del pentest, di rendere quest'ultimo efficiente e di creare un ambiente di lavoro organizzato.

Iniziamo con la scansione su Metasploitable come target andando ad usare vari comandi a seconda del tipo di scansione:

1. OS Fingerprint: questo comando serve per determinare il sistema operativo della macchina target attraverso la dicitura '`nmap -O <IP target>`'. Con esso possiamo notare (come in figura 1) che oltre alla descrizione delle porte aperte e dei protocolli associati ad esse ci mostra anche il dettaglio del sistema operativo di quell'IP 192.168.1.35 con tutte le versioni.



```
andrea@Andrea: ~/Desktop
File Actions Edit View Help

[andrea@Andrea]-(~/Desktop)
$ sudo nmap -O 192.168.1.35
[sudo] password for andrea:
Sorry, try again.
[sudo] password for andrea:
Sorry, try again.
[sudo] password for andrea:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 14:45 CEST
Nmap scan report for METASPLOITABLE.station (192.168.1.35)
Host is up (0.00052s 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  XI1
6667/tcp  open  irc
8080/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:6D:03:BF (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/s
ubmit/ .
```

```
andrea@Andrea: ~/Desktop
File Actions Edit View Help

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 10.49 seconds

(andrea@Andrea)~[~/Desktop]
$ sudo nmap -O 192.168.1.37
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 15:28 CEST
Nmap scan report for andrea-PC.station (192.168.1.37)
Host is up (0.00044s 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  wsddapi
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49157/tcp  open  unknown
49163/tcp  open  unknown
MAC Address: 08:00:27:BA:F8:80 (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 3.16 seconds

(andrea@Andrea)~[~/Desktop]
$
```

È possibile eseguire la stessa scansione verso una macchina Windows con IP 192.168.1.37; la grande differenza sta nell'andare ad impostare il firewall di Windows in modo tale che il nostro IP di Kali possa comunicare con esso impostando la regola.

Anche qui possiamo notare che ci fornisce i dettagli inerenti al sistema operativo Windows.

2. Syn Scan: tramite il comando `'nmap -sS <IP>'` riusciamo a capire quali porte sono aperte e quali servizi sono attivi su di esse. Rispetta solo il primo passaggio dell' HandShake SYN/ACK senza chiuderlo in modo tale da risultare più veloce e meno invasivo/rumoroso. Questo porta, tuttavia, ad un'accuratezza minore. Possiamo identificare servizi molto importanti e le relative porte predefinite come: 21 FTP, 22 SSH, 80 HTTP, 443 HTTPS.

```
andrea@Andrea: ~/Desktop
File Actions Edit View Help

(andrea@Andrea)~[~/Desktop]
$ sudo nmap -sS 192.168.1.35
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 15:46 CEST
Nmap scan report for METASPLOITABLE.station (192.168.1.35)
Host is up (0.00028s 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: 08:00:27:6D:03:BF (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.35 seconds

(andrea@Andrea)~[~/Desktop]
$
```

3. TCP Connect: è, in poche parole, la conclusione del metodo di scansione precedente. Esso tramite comando `'nmap -sT <IP>'` va a concludere tutte le fasi dell' HandShake risultando più invasivo rispetto al solo SYN. Aspetta di ricevere tutte le fasi e ciò porta a creare una latenza maggiore. Esso, tuttavia, è molto attendibile.

```
andrea@Andrea: ~/Desktop
File Actions Edit View Help
sudo nmap -sT 192.168.1.35
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 15:57 CEST
Nmap scan report for METASPLOITABLE.station (192.168.1.35)
Host is up (0.00059s 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: 08:00:27:6D:03:BF (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds

(andrea@Andrea)-[~/Desktop]
$
```

4. Version Detection: è un tipo di scansione chiamata anche *'banner grabbing'* che permette di recuperare informazioni inerenti al software su una determinata porta e alla sua versione. Questo ci permette di sperimentare in laboratorio virtuale le vulnerabilità e di verificarne l'attendibilità nel caso la porta predefinita sia stata cambiata (contromisura efficace).

```
andrea@Andrea: ~/Desktop
File Actions Edit View Help
$ sudo nmap -p 80
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 16:20 CEST
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.05 seconds

(andrea@Andrea)~-[~/Desktop]
$ sudo nmap -sV 192.168.1.35
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 16:33 CEST
Nmap scan report for METASPLOITABLE.station (192.168.1.35)
Host is up (0.00024s 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: 08:00:27:6D:03:BF (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
g/submit/.
Nmap done: 1 IP address (1 host up) scanned in 64.70 seconds

(andrea@Andrea)~-[~/Desktop]
$
```

Un altro comando molto utile è anche *'nmap <IP> --script smb-os-discovery'* che mostra le informazioni di un sistema operativo con un particolare script molto dettagliato che riporta anche i nomi utenti o del PC:

```
andrea@Andrea: ~/Desktop
File Actions Edit View Help
See the output of nmap -h for a summary of options.

(andrea@Andrea)~-[~/Desktop]
$ sudo nmap 192.168.1.37 --script smb-os-discovery
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 16:56 CEST
Nmap scan report for andrea-PC.station (192.168.1.37)
Host is up (0.00042s latency).
Not shown: 990 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft
5357/tcp  open  wsdaapi
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:BA:F8:80 (Oracle VirtualBox virtual NIC)

Host script results:
| smb-os-discovery:
| OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
| OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
| Computer name: andrea-PC
| NetBIOS computer name: ANDREA-PC\x00
| Workgroup: WORKGROUP\x00
| System time: 2023-10-25T16:56:53+02:00
|_

Nmap done: 1 IP address (1 host up) scanned in 13.29 seconds

(andrea@Andrea)~-[~/Desktop]
$
```