

S5_L3

21 febbraio 2024

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.

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.

Quesito extra (al completamento dei quesiti sopra): Quale potrebbe essere una valida ragione per spiegare il risultato ottenuto dalla scansione sulla macchina Windows 7? Che tipo di soluzione potreste proporre per continuare le scansioni?

Scansione della rete

Indirizzi IP

Come prima operazione effettuiamo una scansione della rete alla ricerca dei nostri target

All'interno della prima rete individuiamo due dispositivi: il primo è l'interfaccia del gateway (nel nostro caso PFsense), il secondo è l'indirizzo della macchina di Metasploit, il nostro primo target.

```
(root@kali)-[~]  
# nmap -sn 192.168.49.0/24  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 08:44 EST  
Nmap scan report for 192.168.49.1  
Host is up (0.00055s latency).  
Nmap scan report for 192.168.49.101  
Host is up (0.00099s latency).  
Nmap done: 256 IP addresses (2 hosts up) scanned in 4.44 seconds
```

Continuiamo la scansione sulla seconda rete, individuiamo tre dispositivi: il primo è sempre l'interfaccia del gateway, il secondo è la macchina Kali da dove stiamo operando in fine il terzo indirizzo appartiene alla macchina Windows, il secondo target.

```
(root@kali)-[~]  
# nmap -sn 192.168.50.0/24  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 08:55 EST  
Nmap scan report for 192.168.50.1  
Host is up (0.00043s latency).  
MAC Address: 08:00:27:39:5A:9E (Oracle VirtualBox virtual NIC)  
Nmap scan report for 192.168.50.102  
Host is up (0.00023s latency).  
MAC Address: 08:00:27:F4:83:37 (Oracle VirtualBox virtual NIC)  
Nmap scan report for 192.168.50.100  
Host is up.  
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.00 seconds
```

Sistemi operativi, Porte aperte e Servizi in ascolto

Lo step successivo è studiare il sistema operativo dei nostri target così da conoscere l'ambiente in cui ci andremo ad introdurre. Per accelerare la raccolta di informazioni anzichè eseguire le varie interrogazioni con i parametri -O -sT -sS eseguiamo lo script smb-os-discovery

Eseguendo lo script in figura per l'indirizzo **192.168.49.101** rileviamo che:

La macchina ha molte porte aperte fra cui rientrano anche delle porte **non sicure**:

- 21 FTP
- 23 TELNET
- 25 SMTP
- 53 DNS
- 80 HTTP
- 445 SMB

Sulla macchina gira un sistema operativo su base Unix nello specifico Samba 3.0.20-Debian

```

nmap 192.168.49.101 --script smb-os-discovery
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 09:33 E
Nmap scan report for 192.168.49.101
Host is up (0.0011s 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

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2024-02-21T09:34:28-05:00

Nmap done: 1 IP address (1 host up) scanned in 1.00 seconds

```

Tentando di contattare la macchina windows riceviamo le seguenti informazioni. Deduciamo che la sicurezza di windows è molto più alta di quella di Metasploit

```
(root@kali)-[~]
# nmap 192.168.50.102 --script smb-os-discovery
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 09:45 EST
Nmap scan report for 192.168.50.102
Host is up (0.00028s latency).
All 1000 scanned ports on 192.168.50.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:F4:83:37 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 21.72 seconds
```

Tuttavia interrogando la macchina su un gruppo ristretto di porte alla volta riusciamo a raccogliere le informazioni necessarie. Notiamo che tutte le porte sono filtrate dal firewall.

```
(root@kali)-[~]
# nmap -sS -p 1-20 192.168.50.102 -T5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 10:19 EST
Nmap scan report for 192.168.50.102
Host is up (0.00045s latency).

PORT      STATE      SERVICE
1/tcp     filtered  tcpmux
2/tcp     filtered  compressnet
3/tcp     filtered  compressnet
4/tcp     filtered  unknown
5/tcp     filtered  rje
6/tcp     filtered  unknown
7/tcp     filtered  echo
8/tcp     filtered  unknown
9/tcp     filtered  discard
10/tcp    filtered  unknown
11/tcp    filtered  systat
12/tcp    filtered  unknown
13/tcp    filtered  daytime
14/tcp    filtered  unknown
15/tcp    filtered  netstat
16/tcp    filtered  unknown
17/tcp    filtered  qotd
18/tcp    filtered  msp
19/tcp    filtered  chargen
20/tcp    filtered  ftp-data
MAC Address: 08:00:27:F4:83:37 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.69 seconds
```

Modificando la rete da pubblica a domestica, utilizzando il parametro -O otteniamo i seguenti dati:

- Porta 5357 - Aperta - servizio wsdapi
- Il sistema operativo è basato su windows e rientra fra quelli elencati

```
(root@kali)-[~]
# nmap -O 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 10:40 EST
Nmap scan report for 192.168.50.102
Host is up (0.00045s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
5357/tcp  open  wsdapi
MAC Address: 08:00:27:F4:83:37 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows 8.1 R1 (96%), Microsoft Windows Phone 7.5 or 8.0 (94%), Microsoft Windows Embedded Standard 7 (94%), Microsoft Windows Server 2008 or 2008 Beta 3 (92%), Microsoft Windows 7 Professional or Windows 8 (92%), Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (92%), Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (92%), Microsoft Windows Server 2008 R2 or Windows 8.1 (91%), Microsoft Windows 7 (90%), Microsoft Windows Server 2008 R2 SP1 (90%)
No exact OS matches for host (test conditions non-ideal).
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 9.52 seconds
```

Disattivato il firewall riceviamo la seguente risposta:

Eseguendo il medesimo script all'indirizzo **192.168.50.102** rileviamo che:

La macchina ha delle porte aperte di cui molte sono alte e non conosciamo il relativo servizio.

Sulla macchina gira un sistema operativo Windows 7 Home basic

```
(root@kali)-[~]
# nmap 192.168.50.102 --script smb-os-discovery
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 09:36 EST
Nmap scan report for 192.168.50.102
Host is up (0.00027s 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
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:F4:83:37 (Oracle VirtualBox virtual NIC)

Host script results:
| smb-os-discovery:
|   OS: Windows 7 Home Basic 7601 Service Pack 1 (Windows 7 Home Basic 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: Windows7
|   NetBIOS computer name: WINDOWS7\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2024-01-22T21:33:46+01:00

Nmap done: 1 IP address (1 host up) scanned in 9.52 seconds
```

Per ottenere ulteriori sui **servizi attivi** eseguiamo il comando nmap con il parametro -sV, il quale ci ritorna la lista dei servizi attivi sulle macchine, la relativa porta e la versione del servizio.

```
(root@kali)-[~]
# nmap -sV 192.168.49.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 09:48 EST
Nmap scan report for 192.168.49.101
Host is up (0.0014s 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         netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  shell        Netkit rshd
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
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 52.89 seconds
```

```
(root@kali)-[~]
# nmap -sV 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 09:49 EST
Nmap scan report for 192.168.50.102
Host is up (0.00038s latency).
Not shown: 991 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 Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
49152/tcp  open  msrpc        Microsoft Windows RPC
49153/tcp  open  msrpc        Microsoft Windows RPC
49154/tcp  open  msrpc        Microsoft Windows RPC
49155/tcp  open  msrpc        Microsoft Windows RPC
49156/tcp  open  msrpc        Microsoft Windows RPC
49157/tcp  open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:F4:83:37 (Oracle VirtualBox virtual NIC)
Service Info: Host: WINDOWS7; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/subm
Nmap done: 1 IP address (1 host up) scanned in 77.97 seconds
```

Quale potrebbe essere una valida ragione per spiegare il risultato ottenuto dalla scansione sulla macchina Windows 7? Che tipo di soluzione potreste proporre per continuare le scansioni?

Soluzione per proseguire le scansioni su Windows7

Precedentemente abbiamo come il risultato della scansione della porte non ci restituisse alcuna informazione utile dal momento che ci diceva che le mille porte tcp scansionate fossero in modalita "ignora"

```
Host is up (0.000015 latency).
All 1000 scanned ports on 192.168.50.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
```

Nella soluzione sopra abbiamo disattivato il firewall di windows per proseguire l'esercitazione, ma ciò non sarebbe possibile al di fuori del laboratorio didattico, o almeno non in questo modo. Per riuscire a proseguire la scansione potremmo:

- Tentare di effettuare un syn scan il quale è meno invasivo in quanto non completa il 3-way-handshake, rendendo le operazioni più rapide, e lasciando meno tracce.
- Timing template: è una modalità per controllare il tempo che passa tra l'invio di richieste successive, chiamata timing template. Si possono impostare 6 livelli di timing che vanno da 0 a 5. T0 e T1 sono comunemente utilizzati per bypassare gli IDS: in questa modalità gli scan sono piuttosto lenti e poco invasivi, e dunque diminuisce notevolmente la probabilità di essere intercettati
- Frammentare i pacchetti: frammentare l'header TCP su più pacchetti, in modo da rendere più difficile per un packet filter capire cosa sta succedendo.