

W11D1 Pratica 1

Giacomo di Giacinto



Esercizio
Scansione dei servizi

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

Modificate le impostazioni di rete delle macchine virtuali per fare in modo che i due target siano sulla stessa rete. A valle delle scansioni, per entrambi gli IP, è prevista la produzione di un **report** contenente le seguenti info (dove disponibili):

- ☐ IP
- ☐ Sistema Operativo
- ☐ Porte Aperte
- ☐ Servizi in ascolto con versione
- ☐ Descrizione dei servizi

<https://www.poftut.com/nmap-output/>

`nmap -oN report1 IP`

Di seguito elenco le scansioni sul target Metasploitable come da traccia dell'esercizio seguite da una breve descrizione delle funzioni peculiari della specifica richiesta.

Preciso che i due target si trovano sulla stessa rete.

1) OS fingerprint

Questa richiesta identifica le porte aperte del target, analizza le risposte, per mettere in evidenza il sistema operativo e la sua versione. Metasploitable ha come sistema operativo Linux alla versione 2.6.9 - 2.6.33 e di seguito vediamo tutte le porte aperte con il relativo servizio a suo fianco.

- Il comando da utilizzare è `sudo nmap -O <e l'IP target>`

```
(kali@kali)-[~]
$ sudo nmap -O 192.168.1.246
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-19 21:06 CET
Nmap scan report for 192.168.1.246
Host is up (0.00085s 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:CE:D2:42 (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
```

2) Syn scan

La scansione Syn è una scansione utilizzata per determinare le porte aperte di un indirizzo IP. La peculiarità di questa scansione sta nel fatto che la tecnica utilizzata è più silenziosa rispetto ad altri tipi di scansione .

Nella Syn scan il sistema invia i pacchetti con il flag Syn, se la porta è aperta il sistema risponde con un Syn/Ack, e la connessione si interrompe prima della risposta finale di Ack.

Se invece la porta è chiusa il sistema risponde con un Rst.

Di seguito vediamo la lista delle porte aperte con il rispettivo servizio assegnato

- il comando da utilizzare è `sudo nmap -sS <e l'IP target>`

```
(kali㉿kali)-[~]  
$ sudo nmap -sS 192.168.1.246  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-19 21:10 CET  
Nmap scan report for 192.168.1.246  
Host is up (0.0036s 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:CE:D2:42 (Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds
```

3) Tcp connect

Questa scansione a differenza della scansione Syn porta a termine la three-way-handshake e quindi porta a termine la domanda Syn, la risposta Syn/Ack e la chiusura della richiesta con Ack.

Questa scansione è meno silenziosa della precedente e potrebbe essere identificata da applicazioni che ascoltano il traffico della macchina target.

il risultato è lo stesso della precedente scansione, vengono indicate le porte e i loro servizi associati.

- il comando da utilizzare è `sudo nmap -sT <e l'IP target>`

```
(kali@kali)-[~]
$ sudo nmap -sT 192.168.1.246
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-19 21:17 CET
Nmap scan report for 192.168.1.246
Host is up (0.0016s 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:CE:D2:42 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds
```

4) Version detection

Questo tipo di scansione è la più invasiva e oltre a stabilire i three-way-handshake recupera anche le informazioni relative al servizio in ascolto dal banner del demone.

Il risultato è simile alle scansioni sopra riportate, viene integrata anche la versione di ogni singolo servizio di ogni porta aperta

- il comando da utilizzare è `sudo nmap -sV <e l'IP target>`

```
└─$ sudo nmap -sV 192.168.1.246
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-19 21:18 CET
Nmap scan report for 192.168.1.246
Host is up (0.00033s 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 rshcd
513/tcp   open  login        OpenBSD or Solaris rlogin
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:CE:D2:42 (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 12.00 seconds
```

Per concludere posso sostenere che queste tecniche di scansione sono simili ma ognuna differisce per qualche piccola peculiarità, in base alla casistica che mi troverò ad affrontare opterò per la soluzione più idonea al momento.