

Esercitazione W11D1 - Pratica 1

Nmap

Fabio Benevento - 16/01/2024

Traccia

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

Implementazione

Nelle seguenti pagine sono illustrati i comandi utilizzati per ricavare le informazioni richieste.

Entrambe le macchine sono collocate sulla stessa sottorete (192.168.50.x) con indirizzi rispettivamente di 192.168.50.100 per Kali Linux e di 192.168.50.101 per Metasploitable

OS Fingerprinting (-O)

Tramite l'opzione -O è possibile individuare la versione del sistema operativo che viene stampata in basso al termine della scansione dei servizi come mostrato nell'immagine sottostante.

```
(kali㉿kali)-[~]  
└─$ sudo nmap -O 192.168.50.101  
[sudo] password for kali:  
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 05:46 EST  
Nmap scan report for 192.168.50.101  
Host is up (0.0019s 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: 08:00:27:10:8A:34 (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 15.55 seconds
```

Syn Scan (-S)

Tramite l'opzione -S è possibile effettuare la scansione senza effettuare la connessione completa con three-way handshake

```
(kali㉿kali)-[~]  
└─$ sudo nmap -sS 192.168.50.101  
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 05:50 EST  
Nmap scan report for 192.168.50.101  
Host is up (0.0030s 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: 08:00:27:10:8A:34 (Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 13.41 seconds  
  
(kali㉿kali)-[~]  
└─$
```

TCP Connect (-T)

Con l'opzione -T invece la scansione viene effettuata instaurando una connessione con three-way handshake e risulta quindi più invasiva.

```
(kali㉿kali)-[~]  
$ sudo nmap -sT 192.168.50.101  
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 06:06 EST  
Nmap scan report for 192.168.50.101  
Host is up (0.010s 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: 08:00:27:10:8A:34 (Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 13.43 seconds
```

Version detection (-V)

Per il version detection ho utilizzato l'opzione specifica -V. In questo caso, ove possibile, nmap indica la versione del tool che espone il servizio.

```
(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-19 06:09 EST
Nmap scan report for 192.168.50.101
Host is up (0.0013s 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
MAC Address: 08:00:27:10:8A:34 (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 70.64 seconds
```

Report finale

Di seguito il report in forma tabellare con le informazioni trovate

Fonte	Kali Linux - IP: 192.168.50.100		
Target	Metasploitable - IP: 192.168.50.101		
Tipo di scan	Nmap (varie modalità)		
Numero servizi trovati		12	
Porta	Servizio	Versione	Descrizione
21	ftp	vsftpd 2.3.4	server FTP per scambio file
22	ssh	OpenSSH 4.7p1	connessione sicura remota

23	telnet	Linux telnetd	connessione host remoto
25	smtp	Postfix smtpd	invio posta elettronica
53	domain	ISC Bind 9.4.2	dns
80	http	Apache 2.2.8	server web
111	rpc-bind	2	comunicazione tra processi RPC
139	netbios-ssn	Samba 3.x - 4.x	com. reti locali - sessione
445	microsoft-ds	Samba 3.x - 4.x	condivisione risorse
512	exec	netkit-rsh rexecd	remote shell (progetto netkit)
513	login		remote shell (progetto netkit)
514	shell	netkit-rsh	remote shell (progetto netkit)
1099	java-rmi	GNU classpath gmiregistry	invocazione metodi remoti
1524	bindshell	Metasploitable root shell	shell remota (hacking)
2049	nfs	2-4	condivisione file
2121	ftp	ProFTP 1.3.1	server FTP per scambio file
3306	mysql	5.0.51a	database relazionale
5432	postgresql	8.3.0 - 8.3.7	database relazionale
5900	vnc	protocol 3.3	controllo desktop remoto
6000	X11		motore grafico di Linux
6667	irc	UnrealIRCd	chat
8009	ajp13	Apache jserv (prot. 1.3)	servlet
8081	http	Apache Tomcat 1.1	server web