Esercitazione W10D4

Raccolta informazioni

Fabio Benevento - 10/01/2024

Traccia

Utilizzare alcuni degli strumenti indicati nel link in basso per raccogliere informazioni sulla macchina metasploitable e produrre un report. Nel report indicare sopra l'esecuzione degli strumenti e nella parte finale un riepilogo delle informazioni trovate

https://www.yeahhub.com/15-most-useful-host-scanning-commands-kalilinux/

Implementazione

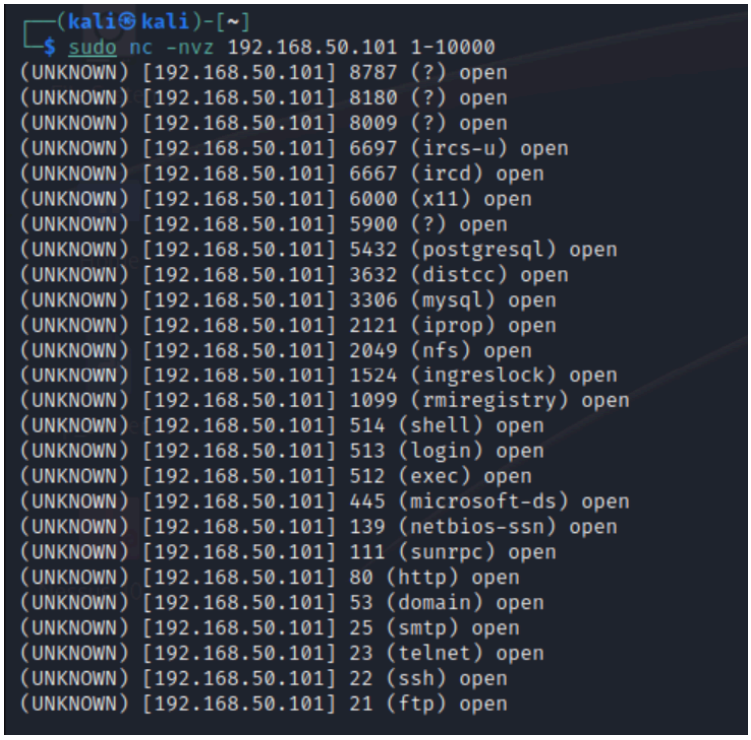
Scanning con hping3

Hping3 è uno strumento di test di rete open-source e una utility di analisi di pacchetti che può essere utilizzato per testare la connettività di rete, rilevare problemi di routing, analizzare le prestazioni della rete e condurre test di sicurezza. Alcune delle funzionalità principali di hping3 includono la possibilità di inviare pacchetti personalizzati con opzioni specifiche, generare pacchetti ICMP, TCP, UDP e altri, eseguire scansioni di porte e svolgere attività di tracciamento del percorso (traceroute). Nel caso in analisi viene usato proprio come strumento di scansione porte in alternativa a Nmap.

```
┌──(kali㉿kali)-[~]
└─$ sudo hping3 --scan known 192.168.50.101
Scanning 192.168.50.101 (192.168.50.101), port known
264 ports to scan, use -V to see all the replies
+----+------------+---------+---+-----+-----+-----+
|port| serv name  |  flags  |ttl| id  | win | len |
+----+------------+---------+---+-----+-----+-----+
All replies received. Done.
Not responding ports: (21 ftp) (22 ssh) (23 telnet) (25 smtp) (53 domain) (80 http) (111 sunrpc) (139 netbios-ssn) (445 microso
ft-d) (512 exec) (513 login) (514 shell) (1099 rmiregistry) (1524 ingreslock) (2049 nfs) (2121 iprop) (3306 mysql) (3632 distcc
) (5432 postgresql) (6000 x11) (6667 ircd) (6697 ircs-u)
```

Scanning con Netcat

In questo caso lo scanning delle porte aperte sulla rete è stato eseguito mediante il comando Netcat (nc).
La sintassi del comando è il seguente: `nc -nzv [host_remoto] [porta_iniziale-porta_finale]` dove:
-z imposta la scansione delle porte con i parametri indicati
-v abilita la modalità verbosa
-n disabilita la risoluzione dei nomi DNS



Banner grabbing con Netcat

Specificando una sola porta, netcat permette indica la versione dell'utility che offre il servizio, offrendo quindi una modalità alternativa di banner grabbing a Nmap

```
┌──(kali㉿kali)-[~]
└─$ sudo nc -nv 192.168.50.101 21
(UNKNOWN) [192.168.50.101] 21 (ftp) open
220 (vsFTPd 2.3.4)
^C

┌──(kali㉿kali)-[~]
└─$ sudo nc -nv 192.168.50.101 22
(UNKNOWN) [192.168.50.101] 22 (ssh) open
SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
^C
```

Version scanning con reason e ping disabilitato Nmap

Tramite il comando `nmap <target> -p- -sV –reason` nmap esegue la scansione di tutte le porte (opzione -p-) indicando la versione dell'utility che fornisce il servizio (opzione -sV). Tramite l'opzione –reason viene inoltre indicato il motivo per una porta viene indicata come aperta, chiusa o filtrata nella colonna STATE

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 192.168.50.101 -p- -sV --reason
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-21 11:20 EST
Nmap scan report for 192.168.50.101
Host is up, received arp-response (0.0011s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE     REASON         VERSION
21/tcp    open  ftp         syn-ack ttl 64 vsftpd 2.3.4
22/tcp    open  ssh         syn-ack ttl 64 OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet      syn-ack ttl 64 Linux telnetd
25/tcp    open  smtp        syn-ack ttl 64 Postfix smtpd
53/tcp    open  domain      syn-ack ttl 64 ISC BIND 9.4.2
80/tcp    open  http        syn-ack ttl 64 Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     syn-ack ttl 64 2 (RPC #100000)
139/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec        syn-ack ttl 64 netkit-rsh rexecd
513/tcp   open  login?      syn-ack ttl 64
514/tcp   open  shell       syn-ack ttl 64 Netkit rshd
1099/tcp  open  java-rmi    syn-ack ttl 64 GNU Classpath grmiregistry
1524/tcp  open  bindshell   syn-ack ttl 64 Metasploitable root shell
2049/tcp  open  nfs         syn-ack ttl 64 2-4 (RPC #100003)
2121/tcp  open  ftp         syn-ack ttl 64 ProFTPD 1.3.1
3306/tcp  open  mysql       syn-ack ttl 64 MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distccd     syn-ack ttl 64 distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql  syn-ack ttl 64 PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc         syn-ack ttl 64 VNC (protocol 3.3)
6000/tcp  open  X11         syn-ack ttl 64 (access denied)
6667/tcp  open  irc         syn-ack ttl 64 UnrealIRCd
6697/tcp  open  irc         syn-ack ttl 64 UnrealIRCd (Admin email admin@Metasploitable.LAN)
8009/tcp  open  ajp13       syn-ack ttl 64 Apache Jserv (Protocol v1.3)
8180/tcp  open  http        syn-ack ttl 64 Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb         syn-ack ttl 64 Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
34310/tcp open  java-rmi    syn-ack ttl 64 GNU Classpath grmiregistry
41975/tcp open  status      syn-ack ttl 64 1 (RPC #100024)
50623/tcp open  mountd      syn-ack ttl 64 1-3 (RPC #100005)
52374/tcp open  nlockmgr    syn-ack ttl 64 1-4 (RPC #100021)
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 180.06 seconds
```

Report finale

Di seguito il report in forma tabellare con le informazioni trovate

Sorgente	Kali Linux - IP: 192.168.50.100	
Target	Metasploitable - IP: 192.168.50.101	
OS	Metasploitable Linux	
MAC Address	08:00:27:10:8A:34	
Numero servizi trovati		31
Porta	**Servizio**	**Versione**
21	ftp	vsftpd 2.3.4
22	ssh	OpenSSH 4.7p1
23	telnet	Linux telnetd
25	smtp	Postfix smtpd
53	domain	ISC Bind 9.4.2
80	http	Apache 2.2.8
111	rpc-bind	2
139	netbios-ssn	Samba 3.x - 4.x
445	microsoft-ds	Samba 3.x - 4.x
512	exec	netkit-rsh rexeccd
513	login	
514	shell	netkit-rsh
1099	java-rmi	GNU classpath gmiregistry
1524	bindshell	Metasploitable root shell
2049	nfs	2-4
2121	ftp	ProFTP 1.3.1

3306	mysql	5.0.51a
3632	distccd	distccd v1
5432	postgresql	8.3.0 - 8.3.7
5900	vnc	protocol 3.3
6000	X11	
6667	irc	UnrealIRCd
6697	irc	UnrealIRCd
8009	ajp13	Apache jserv (prot. 1.3)
8081	http	Apache Tomcat 1.1
8787	drb	Ruby drb RMI 1.8
34310	java-rmi	GNU classpath gmiregistry
41975	status	1 RPC
50623	mountd	1-3 RPC
52374	nlockmgr	1-4 RPC