EXPLOIT TELNET CON METASPLOIT

ESERCIZIO S7/L2

Scopo dell’esercizio:

Utilizzare Metasploit per sfruttare la vulnerabilità relativa a Telnet con il modulo auxiliary telnet_version sulla macchina Metasploitable

Configuriamo le macchine con gli eventuali indirizzi IP richiesti nella traccia

IP Kali 192.168.1.25 e IP Meta 192.168.1.40

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
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:fecb:7ef5  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:cb:7e:f5  txqueuelen 1000  (Ethernet)
        RX packets 44  bytes 4092 (3.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 18  bytes 2564 (2.5 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 0x10<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


┌──(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=1.32 ms
64 bytes from 192.168.1.40: icmp_seq=2 ttl=64 time=0.912 ms
64 bytes from 192.168.1.40: icmp_seq=3 ttl=64 time=0.933 ms
64 bytes from 192.168.1.40: icmp_seq=4 ttl=64 time=1.00 ms
64 bytes from 192.168.1.40: icmp_seq=5 ttl=64 time=0.882 ms
^C
── 192.168.1.40 ping statistics ──
5 packets transmitted, 5 received, 0% packet loss, time 4116ms
rtt min/avg/max/mdev = 0.882/1.009/1.318/0.159 ms
```

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:64:48:1b
          inet addr:192.168.1.40  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe64:481b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:84 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:5592 (5.4 KB)
          Base address:0xd020 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:125 errors:0 dropped:0 overruns:0 frame:0
          TX packets:125 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:24365 (23.7 KB)  TX bytes:24365 (23.7 KB)

msfadmin@metasploitable:~$
```

Con un ping ci assicuriamo che comunicano tra di loro

Facciamo partire il servizio «msfconsole»

Facciamo una ricerca del modulo auxiliary telnet_version

Eccola qui l'exploit che ci serve, andiamo a utilizzare il modulo 3 con il comando «use»

```
msf6 > search telnet scanner

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

   #  Name                                                  Disclosure Date  Rank    Check  Description
   -  ----                                                  ---------------  ----    -----  -----------
   0  auxiliary/scanner/telnet/brocade_enable_login                          normal  No     Brocade Enable Login Check Scanner
   1  auxiliary/scanner/ssh/juniper_backdoor                2015-12-20       normal  No     Juniper SSH Backdoor Scanner
   2  auxiliary/scanner/telnet/lantronix_telnet_password                     normal  No     Lantronix Telnet Password Recovery
   3  auxiliary/scanner/telnet/lantronix_telnet_version                      normal  No     Lantronix Telnet Service Banner Detection
   4  auxiliary/admin/http/netgear_pnpx_getsharefolderlist_auth_bypass  2021-09-06       normal  Yes    Netgear PNPX_GetShareFolderList Authentication Bypass
   5  auxiliary/scanner/telnet/telnet_ruggedcom                              normal  No     RuggedCom Telnet Password Generator
   6  auxiliary/scanner/telnet/satel_cmd_exec               2017-04-07       normal  No     Satel Iberia SenNet Data Logger and Electricity Meters Command Injection Vulnerability
   7  auxiliary/scanner/telnet/telnet_login                                  normal  No     Telnet Login Check Scanner
   8  auxiliary/scanner/telnet/telnet_version                                normal  No     Telnet Service Banner Detection
   9  auxiliary/scanner/telnet/telnet_encrypt_overflow                       normal  No     Telnet Service Encryption Key ID Overflow Detection


Interact with a module by name or index. For example info 9, use 9 or use auxiliary/scanner/telnet/telnet_encrypt_overflow
```

Bene ora che possiamo configurare i parametri specifici del modulo

Aggiungiamo l’IP di Meta 192.168.1.40 nella sezione «rhosts»

```
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 specified username
   RHOSTS                     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT     23               yes       The target port (TCP)
   THREADS   1                yes       The number of concurrent threads (max one per host)
   TIMEOUT   30               yes       Timeout for the Telnet probe
   USERNAME                   no        The username to authenticate as


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

msf6 auxiliary(scanner/telnet/telnet_version) > set rhosts 192.168.1.40
rhosts => 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 specified username
   RHOSTS    192.168.1.40     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT     23               yes       The target port (TCP)
   THREADS   1                yes       The number of concurrent threads (max one per host)
   TIMEOUT   30               yes       Timeout for the Telnet probe
   USERNAME                   no        The username to authenticate as
```

Possiamo eseguire l'attacco utilizzando il comando "exploit".

```
msf6 auxiliary(scanner/telnet/telnet_version) > exploit

[+] 192.168.1.40:23       - 192.168.1.40:23 TELNET _                  _     _ _   _     _         ____   \x0a _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ \x0a| '_ ` _ \ / _ \ __/ _` /
_/ _` | '_ \| |/ _ \ __) |\x0a| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ \x0a|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|\x0a                                                  |_|
                      \x0a\x0a\x0aWarning: Never expose this VM to an untrusted network!\x0a\x0aContact: msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin to get started\x0a\x0a\x0ametasploitable login:
[*] 192.168.1.40:23       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) >
```

Facciamo partire il servizio telnet sulla macchina target Meta

Otteniamo l’accesso tramite il servizio telnet nella shell di Meta

```
msf6 auxiliary(scanner/telnet/telnet_version) > 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: Tue Jan 16 03:31:37 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:~$
```

EXPLOIT

Un exploit è un metodo che sfrutta le vulnerabilità di sicurezzain un sistema informatico, un'applicazione o un protocollo eseguire azioni non autorizzate.

Gli hacker utilizzano gli exploit per penetrare nei sistemi e ottenere accesso non consentito o causare danni.

PROTOCOLLO TELNET

Telnet è un modo per controllare un computer da un altro luogo tramite la rete.

Questo protocollo è progettato per consentire agli utenti di accedere e controllare un computer da remoto. Telnet trasmette i dati in modo non sicuro, inclusi nomi utente e password, rendendolo vulnerabile. A causa di problemi di sicurezza, viene spesso sostituito da protocolli più sicuri come SSH.