Esercizio

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 IP Metasploitable2 e Kali Linux.

Modifico l'indirizzo IP di Metasploitable2. Metto la scheda di rete su rete interna e assegno l'indirizzo IP statico 192.168.1.40.

sudo su

nano /etc/network/interfaces

sostituisco iface eth0 con:

auto eth0

iface eth0 inet static

address 192.168.1.40

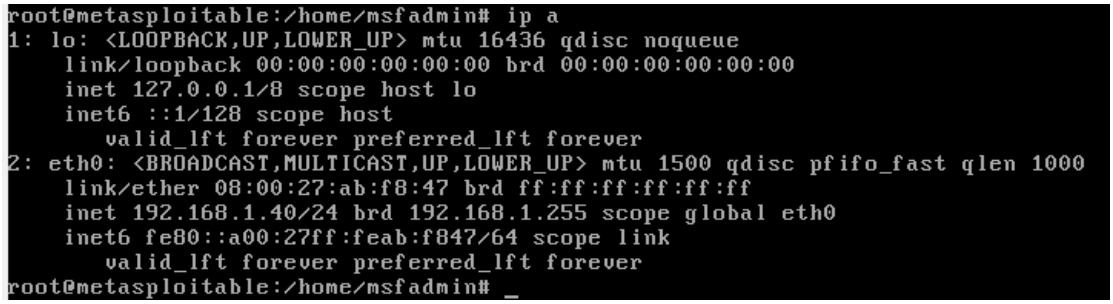
netmask 255.255.255.0

gateway 192.168.1.1

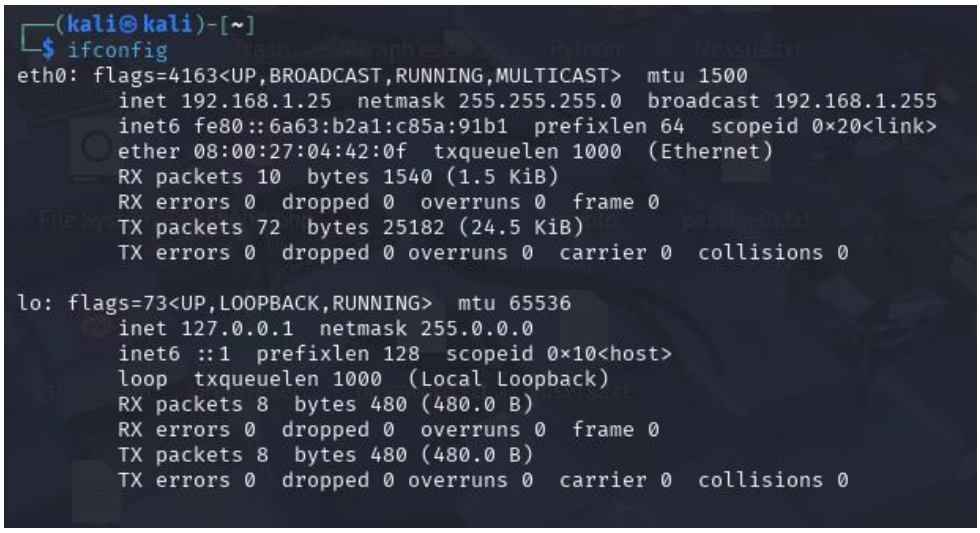
Riavvio l'interfaccia di rete:

ifdown eth0 && ifup eth0

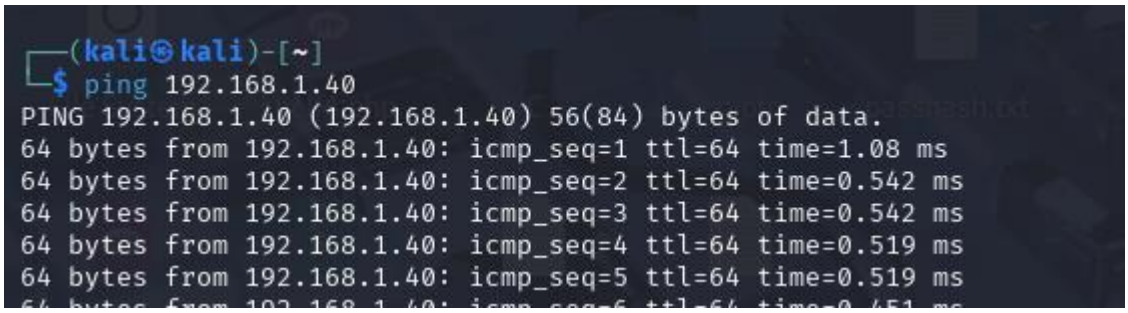
Verifico ora indirizzo IP:



Configuro la rete statica anche sulla Kali:

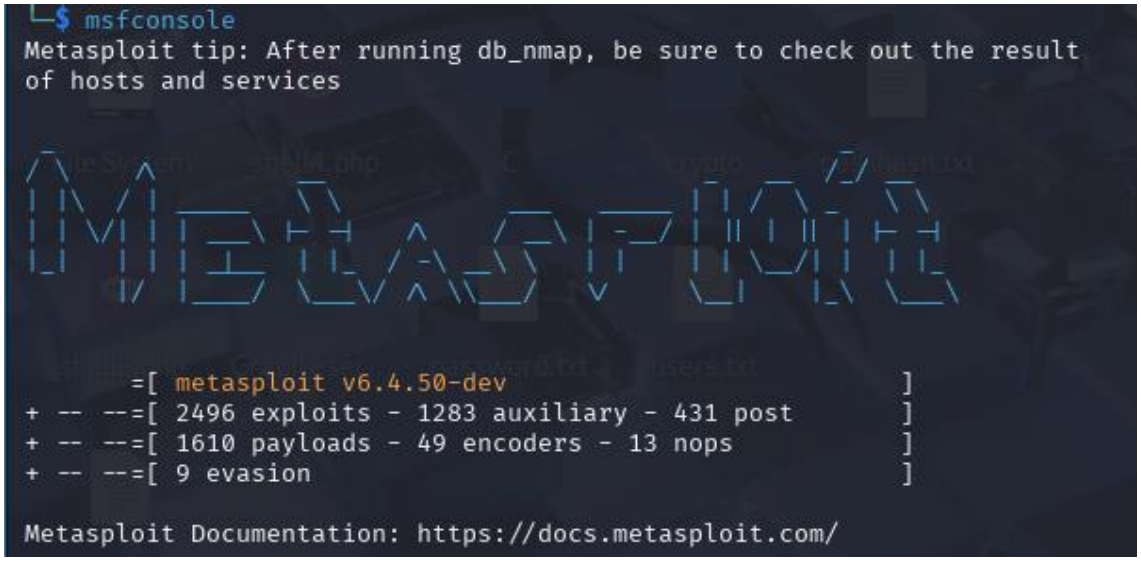


Faccio una prova di connettività



Sfrutto la vulnerabilità relativa a Telnet

Avvio msfconsole



Digito search telnet_version

```
msf6 > search telnet_version

Matching Modules
================

   #  Name                                                  Disclosure Date  Rank    Check  Description
   -  ----                                                  ---------------  ----    -----  -----------
   0  auxiliary/scanner/telnet/lantronix_telnet_version     .                normal  No     Lantronix Telnet Service Banner Detection
   1  auxiliary/scanner/telnet/telnet_version               .                normal  No     Telnet Service Banner Detection

Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/telnet/telnet_version
```

Digito use 1

```
msf6 > use 1
msf6 auxiliary(scanner/telnet/telnet_version) >
```

Digito OPTIONS

```
msf6 auxiliary(scanner/telnet/telnet_version) > 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/using-metasploit/basics/using-m
                                        etasploit.html
   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
```

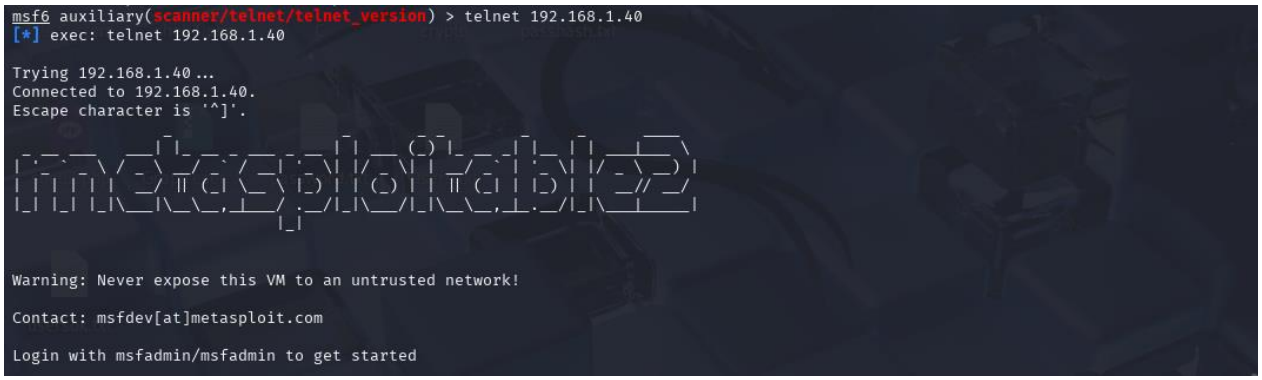
Digito set RHOSTS 192.168.1.40

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

Digito exploit

```
msf6 auxiliary(scanner/telnet/telnet_version) > exploit
[+] 192.168.1.40:23       - 192.168.1.40:23 TELNET _                                                  ___  \x0a _ __ ___   ___| |
_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ \x0a| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| __/ _ \ '_ \| |/ _ \ __)
 |\x0a| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ \x0a|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\_
_\__,_|_.__/|_|\___|_____|\x0a                                    |_|                                          \x0a\x0a\x0aWarning: Never
expose this VM to an untrusted network!\x0a\x0aContact: msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin to get starte
d\x0a\x0a\x0ametasploitable login:
[*] 192.168.1.40:23       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) >
```

Digito il comando telnet 192.168.1.40



Entro con le credenziali