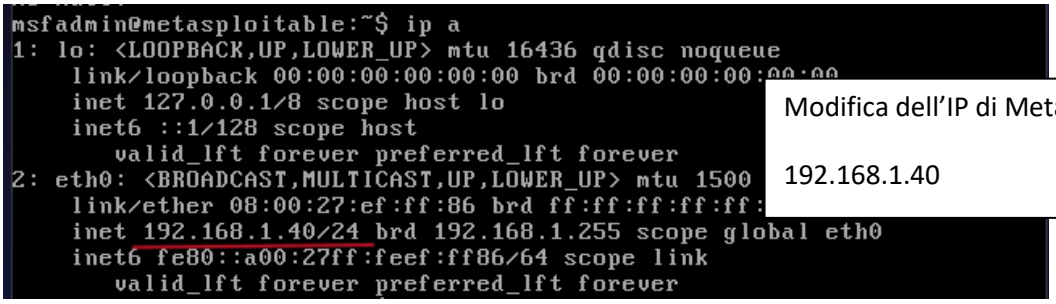
Esercizio 07-03

Traccia: configurare IP Kali come 192.168.1.25 e IP Metasploitable come 192.168.1.40. Eseguire un exploit della vulnerabilità relativa a Telnet con il modulo auxiliary telnet_version sulla macchina Metasploitable.

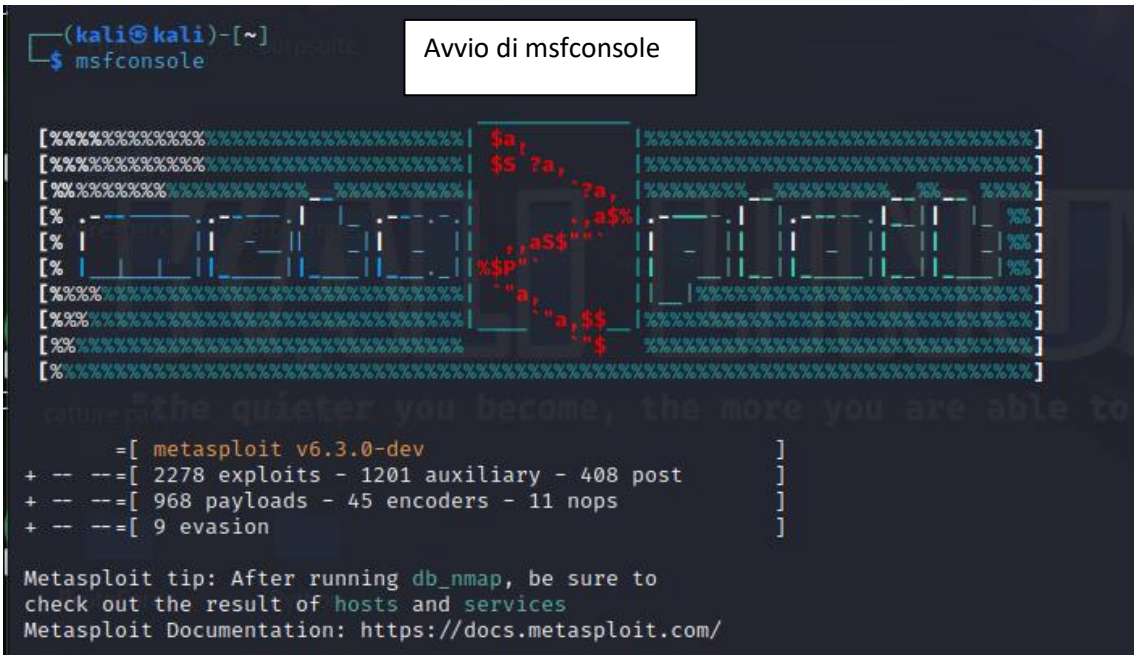
Modifica dell'IP di Kali:

192.168.1.25



Modifica dell'IP di Metasploitable:

192.168.1.40



Avvio di msfconsole

```
msf6 > search telnet

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

   #   Name                                                  Disclosure Date  Rank
Check  Description
   -   ----                                                  ---------------  ----
   0   exploit/linux/misc/asus_infosvr_auth_bypass_exec      2015-01-04       excellent
No     ASUS infosvr Auth Bypass Command Execution
   1   exploit/linux/http/asuswrt_lan_rce                    2018-01-22       excellent
No     AsusWRT LAN Unauthenticated Remote Code Execution
   2   auxiliary/server/capture/telnet                                        normal
No     Authentication Capture: Telnet
   3   auxiliary/scanner/telnet/brocade_enable_login                          normal
No     Brocade Enable Login Check Scanner
   4   exploit/windows/proxy/ccproxy_telnet_ping             2004-11-11       average
Yes    CCProxy Telnet Proxy Ping Overflow
   5   auxiliary/dos/cisco/ios_telnet_rocem                  2017-03-17       normal
No     Cisco IOS Telnet Denial of Service
   6   auxiliary/admin/http/dlink_dir_300_600_exec_noauth    2013-02-04       normal
No     D-Link DIR-600 / DIR-300 Unauthenticated Remote Command Execution
   7   exploit/linux/http/dlink_diagnostic_exec_noauth       2013-03-05       excellent
```

Utilizzo del comando search con riferimento a telnet

```
msf6 > use 35
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://github.com/rapid7/metasploit
                                        -framework/wiki/Using-Metasploit
   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.

msf6 auxiliary(scanner/telnet/telnet_version) > set rhosts 192.168.1.40
rhosts ⇒ 192.168.1.40
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    192.168.1.40     yes       The target host(s), see https://github.com/rapid7/metasploit
                                        -framework/wiki/Using-Metasploit
   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.
```

Impostazione dell'IP target con set RHOSTS

Utilizzo del comando exploit e ottenimento delle credenziali

```
msf6 auxiliary(scanner/telnet/telnet_version) > exploit

[+] 192.168.1.40:23       - 192.168.1.40:23 TELNET _                  _       _ _        _     _      ____  \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 g
[*] 192.168.1.40:23       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

```
msf6 > 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 Mar  7 07:03:39 EST 2023 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:~$ id
uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip)
,44(video),46(plugdev),107(fuse),111(lpadmin),112(admin),119(sambashare),1000(msfadmin)
msfadmin@metasploitable:~$ 
```

Utilizzo del comando telnet con IP di Metasploitable per caricare la schermata di login.

Test delle credenziali per verificarne la correttezza.