Lazysysadmin

Lazysysadmin is another great boot2root challenge created by Togie Mcdogie.
The aim of machine is where we have to root the server and find the flag to complete the challenge.
You can get this VM from https://www.vulnhub.com/entry/lazysysadmin-1,205/).
Let's start by enumeration.

Reconnaisance

Lets start by identifying our target with the following command
netdiscover -i vboxnet0

```
Currently scanning: 172.16.222.0/16   |   Screen View: Unique Hosts

2 Captured ARP Req/Rep packets, from 2 hosts.   Total size: 84
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.56.100  08:00:27:32:dc:3f      1      42  PCS Systemtechnik GmbH
192.168.56.130  08:00:27:05:be:08      1      42  PCS Systemtechnik GmbH
```

so the IP address of the target machine is 192.168.56.130

now we can run nmap scan to find open ports, services, version
nmap - sC -sV -p- -O

```
GNU nano 4.9.2                                   nmap.txt
# Nmap 7.80 scan initiated Sun Jun 28 11:32:16 2020 as: nmap -sC -sV -p- -o nmap.txt 192.168.56.130
Nmap scan report for 192.168.56.130
Host is up (0.0071s latency).
Not shown: 65529 closed ports
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 b5:38:66:0f:a1:ee:cd:41:69:3b:82:cf:ad:a1:f7:13 (DSA)
|   2048 58:5a:63:69:d0:da:dd:51:cc:c1:6e:00:fd:7e:61:d0 (RSA)
|   256 61:30:f3:55:1a:0d:de:c8:6a:59:5b:c9:9c:b4:92:04 (ECDSA)
|_  256 1f:65:c0:dd:15:e6:e4:21:f2:c1:9b:a3:b6:55:a0:45 (ED25519)
80/tcp   open  http        Apache httpd 2.4.7 ((Ubuntu))
|_http-generator: Silex v2.2.7
| http-robots.txt: 4 disallowed entries
|_/old/ /test/ /TR2/ /Backnode_files/
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Backnode
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
3306/tcp open  mysql       MySQL (unauthorized)
6667/tcp open  irc         InspIRCd
| irc-info:
|   server: Admin.local
|   users: 1
|   servers: 1
|   chans: 0
```

From the nmap output we were able to identify different ports open and directories

Enumeration

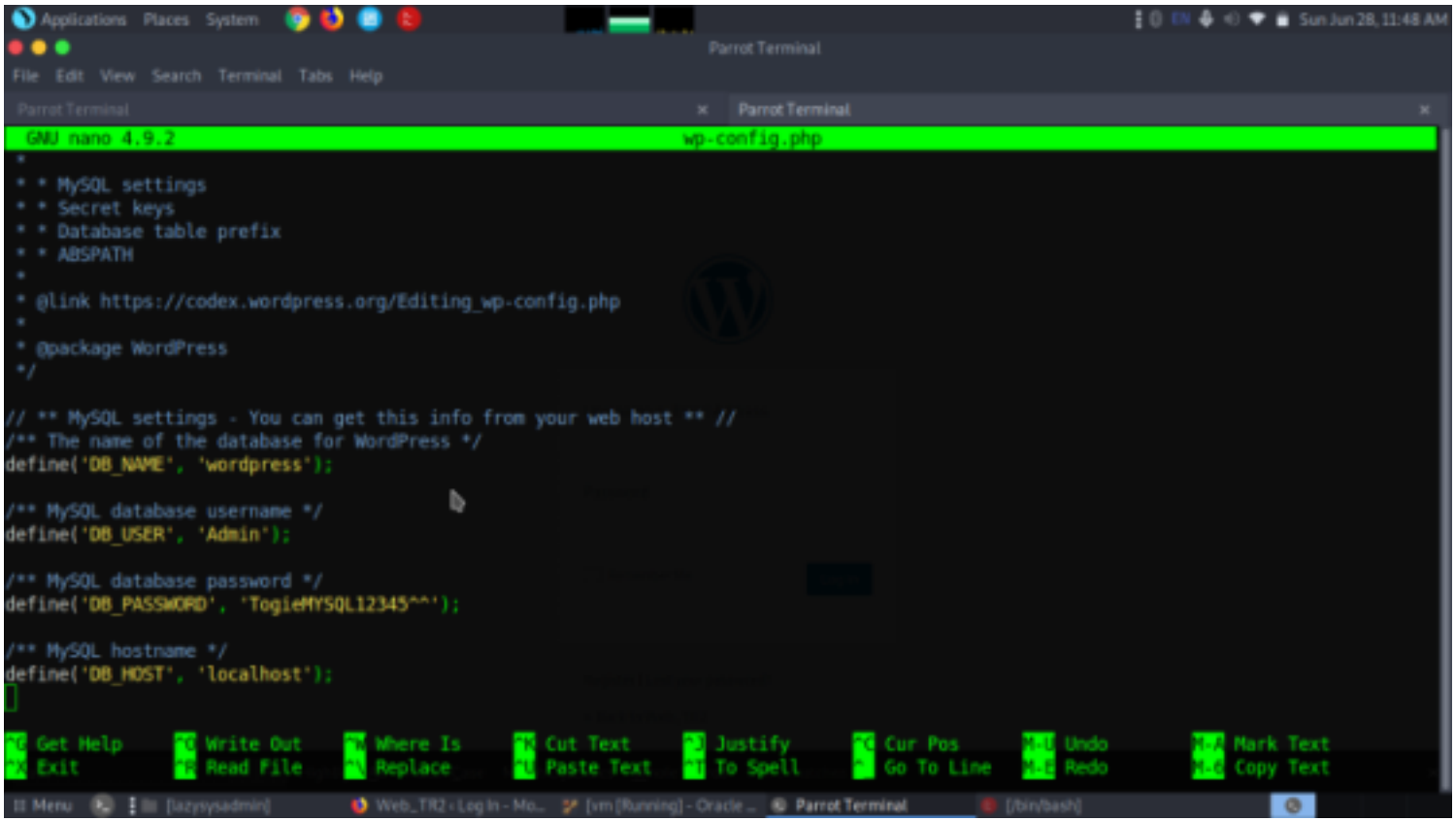
As we have port 139 and port 445 is open, so we use smbclient: smbclient is a client that can ‘talk’ to an SMB/CIFS server) to look for the shared disk. Its operations include things like getting files from the server to the local machine, putting files from the local machine to the server, retrieving directory information from the server and so on.
As you can observe with the help of smbclient we are able to view the shares of the machine. Moreover, we can use smbclient for sharing the file in the network. Here we are able to login successfully using anonymous login and now we can access the ‘share$’ drive.

In ‘share$’ we found WordPress folder as well as three txt files named deets.txt, robots.txt and todolist.txt.

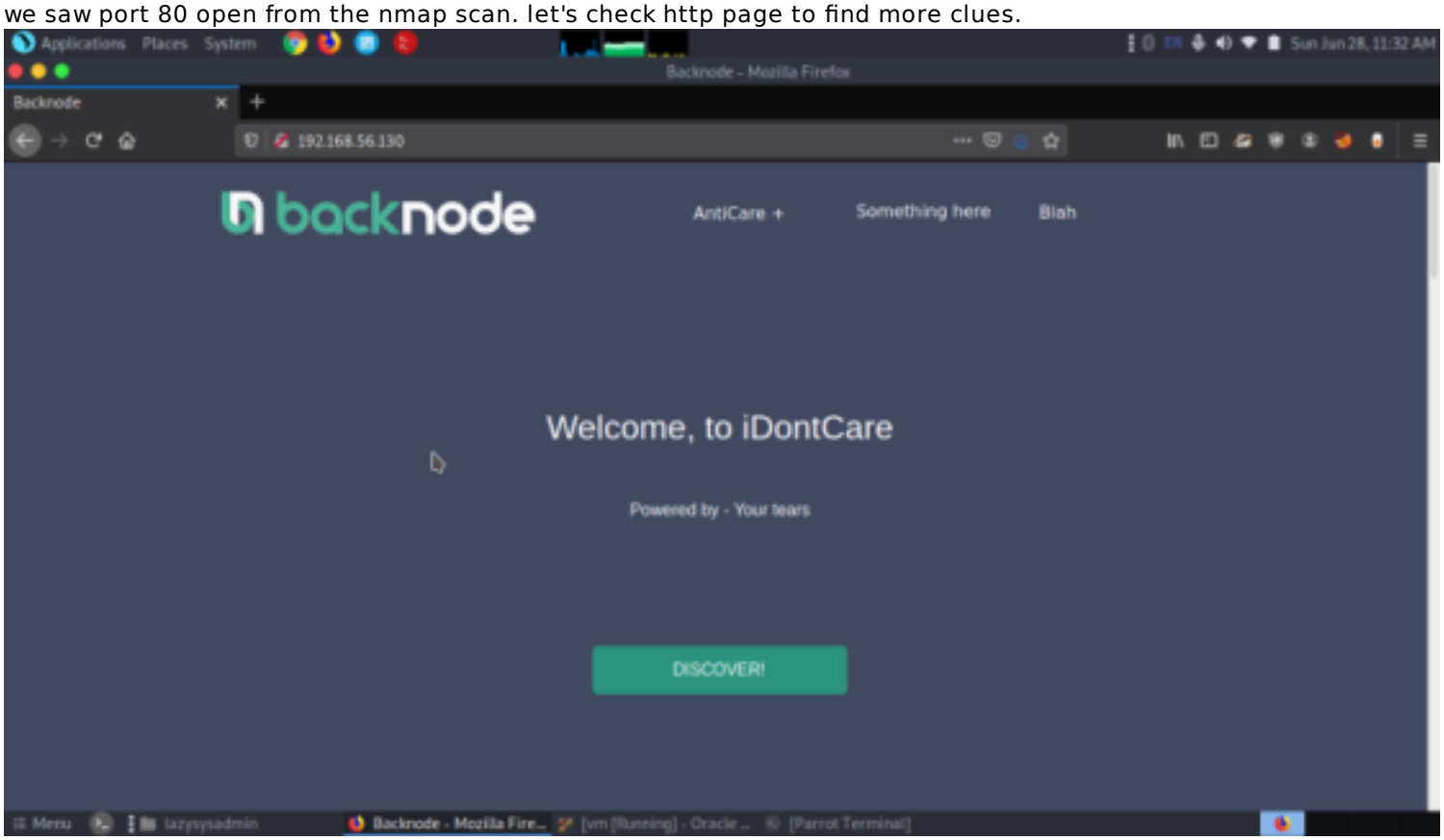
```
Applications  Places  System                                   Sun Jun 28, 11:39 AM
Parrot Terminal
File  Edit  View  Search  Terminal  Tabs  Help
Parrot Terminal                                  Parrot Terminal

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        share$          Disk      Sumshare
        IPC$            IPC       IPC Service (Web server)
SMB1 disabled -- no workgroup available
┌─[baz@parrot]─[~/comp ctf walkthroughs/lazysysadmin]
└──╼ $smbclient //192.168.56.130/share$
Enter WORKGROUP\baz's password:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Tue Aug 15 16:35:52 2017
  ..                                  D        0  Mon Aug 14 18:04:47 2017
  wordpress                           D        0  Mon Jun 15 16:16:12 2020
  Backnode_files                      D        0  Mon Aug 14 17:38:26 2017
  wp                                  D        0  Tue Aug 15 16:21:23 2017
  deets.txt                           N      139  Mon Aug 14 17:50:05 2017
  robots.txt                          N       92  Mon Aug 14 18:06:14 2017
  todolist.txt                        N       79  Mon Aug 14 18:09:56 2017
  apache                              D        0  Mon Aug 14 18:05:19 2017
  index.html                          N    36072  Sun Aug  6 10:32:15 2017
  info.php                            N       20  Tue Aug 15 16:25:19 2017
  test                                D        0  Mon Aug 14 18:05:10 2017
  old                                 D        0  Mon Aug 14 18:05:13 2017

                3029776 blocks of size 1024. 1203988 blocks available
smb: \>
Menu  lazysysadmin  [Mozilla Firefox]  [vm [Running] - Oracle ...  Parrot Terminal  [/bin/bash]
```

we downloaded the files using get command and when accessed each one we got different hints.

```
Parrot Terminal
File  Edit  View  Search  Terminal  Tabs  Help
Parrot Terminal                                  Parrot Terminal
  GNU nano 4.9.2                                          deets.txt
CBF Remembering all these passwords.

Remember to remove this file and update your password after we push out the server.

Password 12345
```



as we can see from deets.txt a password and in directory wordpress there was a file named wp-config.php and when accessed we got a username and password. This would be helpful. now let's move on
we saw port 80 open from the nmap scan. let's check http page to find more clues.

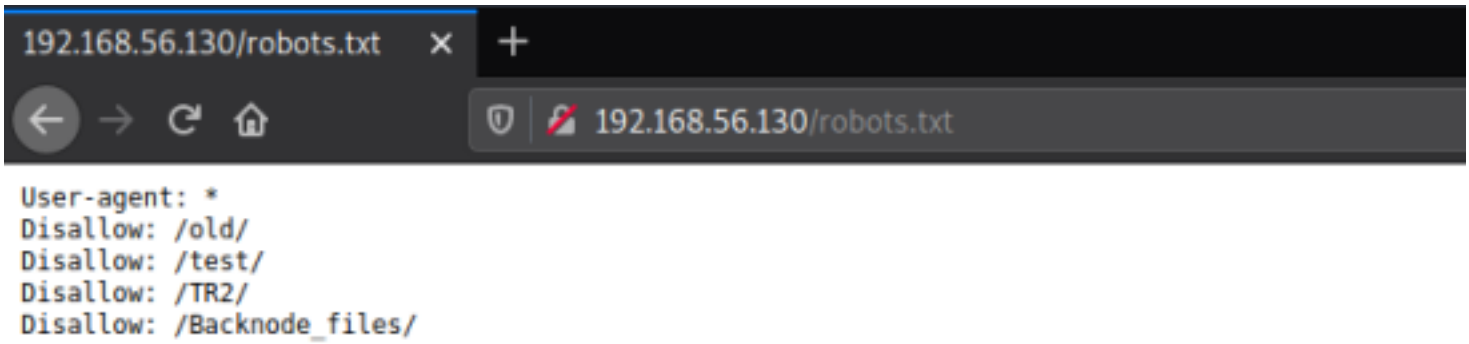


The webpage when enumerated more couldnt find much information so we did a directory scan to find all the directories linked with this webpage.
dirb http://192.168.56.130

```
GNU nano 4.9.2                                   dirb.txt
URL_BASE: http://192.168.56.130/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.56.130/ ----
==> DIRECTORY: http://192.168.56.130/apache/
+ http://192.168.56.130/index.html (CODE:200|SIZE:36072)
+ http://192.168.56.130/info.php (CODE:200|SIZE:77263)
==> DIRECTORY: http://192.168.56.130/javascript/
==> DIRECTORY: http://192.168.56.130/old/
==> DIRECTORY: http://192.168.56.130/phpmyadmin/
+ http://192.168.56.130/robots.txt (CODE:200|SIZE:92)
+ http://192.168.56.130/server-status (CODE:403|SIZE:294)
==> DIRECTORY: http://192.168.56.130/test/
==> DIRECTORY: http://192.168.56.130/wordpress/
==> DIRECTORY: http://192.168.56.130/wp/

---- Entering directory: http://192.168.56.130/apache/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.56.130/javascript/ ----
==> DIRECTORY: http://192.168.56.130/javascript/jquery/

^G Get Help   ^O Write Out   ^W Where Is   ^K Cut Text   ^J Justify   ^C Cur Pos   M-U Undo   M-A Mark Text
^X Exit       ^R Read File   ^\ Replace    ^U Paste Text ^T To Spell   ^_ Go To Line M-E Redo   M-6 Copy Text
```

From the scan we got to know lot's of important directories it contained. after examining each directories we got some more information linked to the webpage.

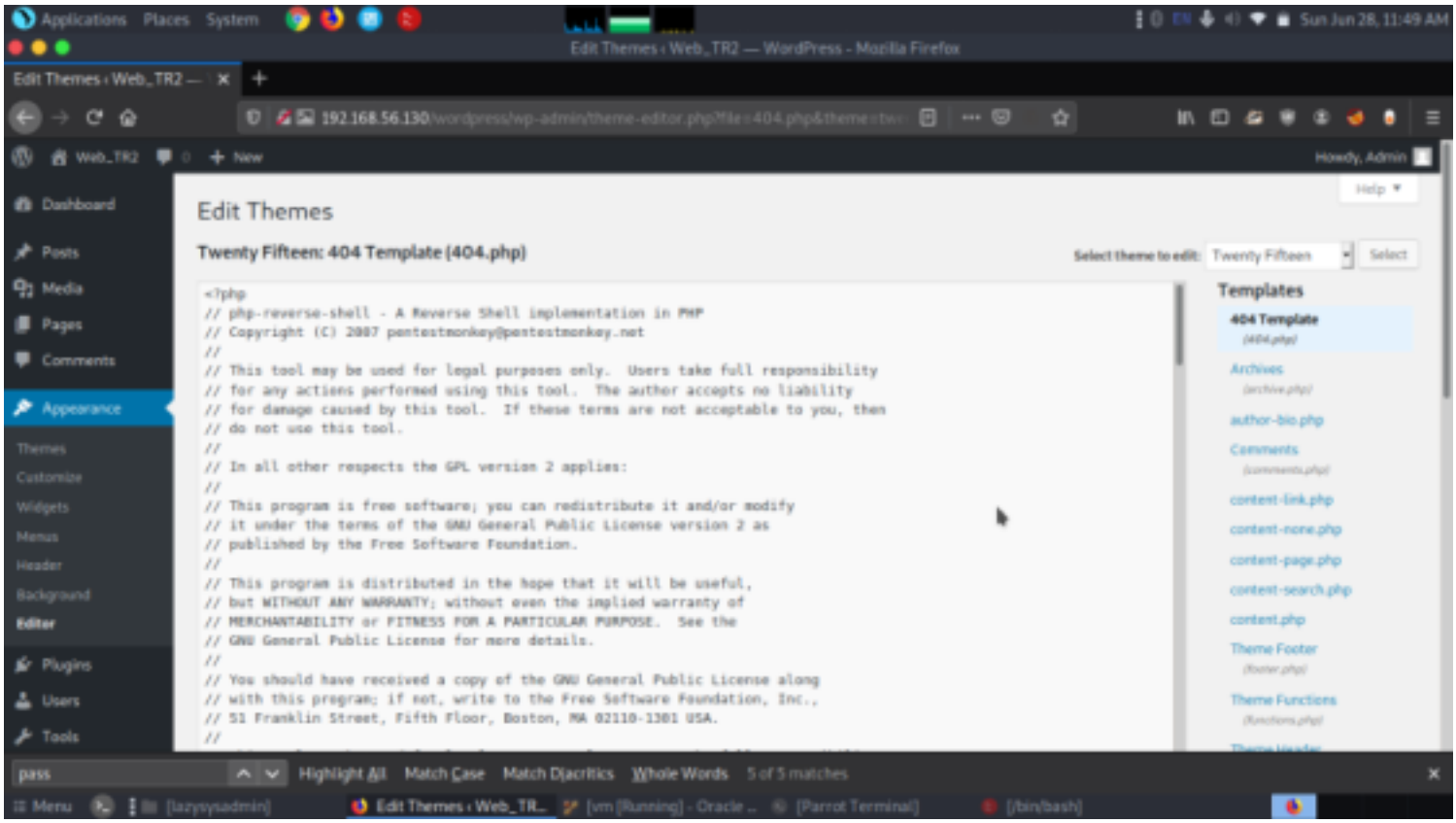
we got to know all details regarding php through the directory info.php



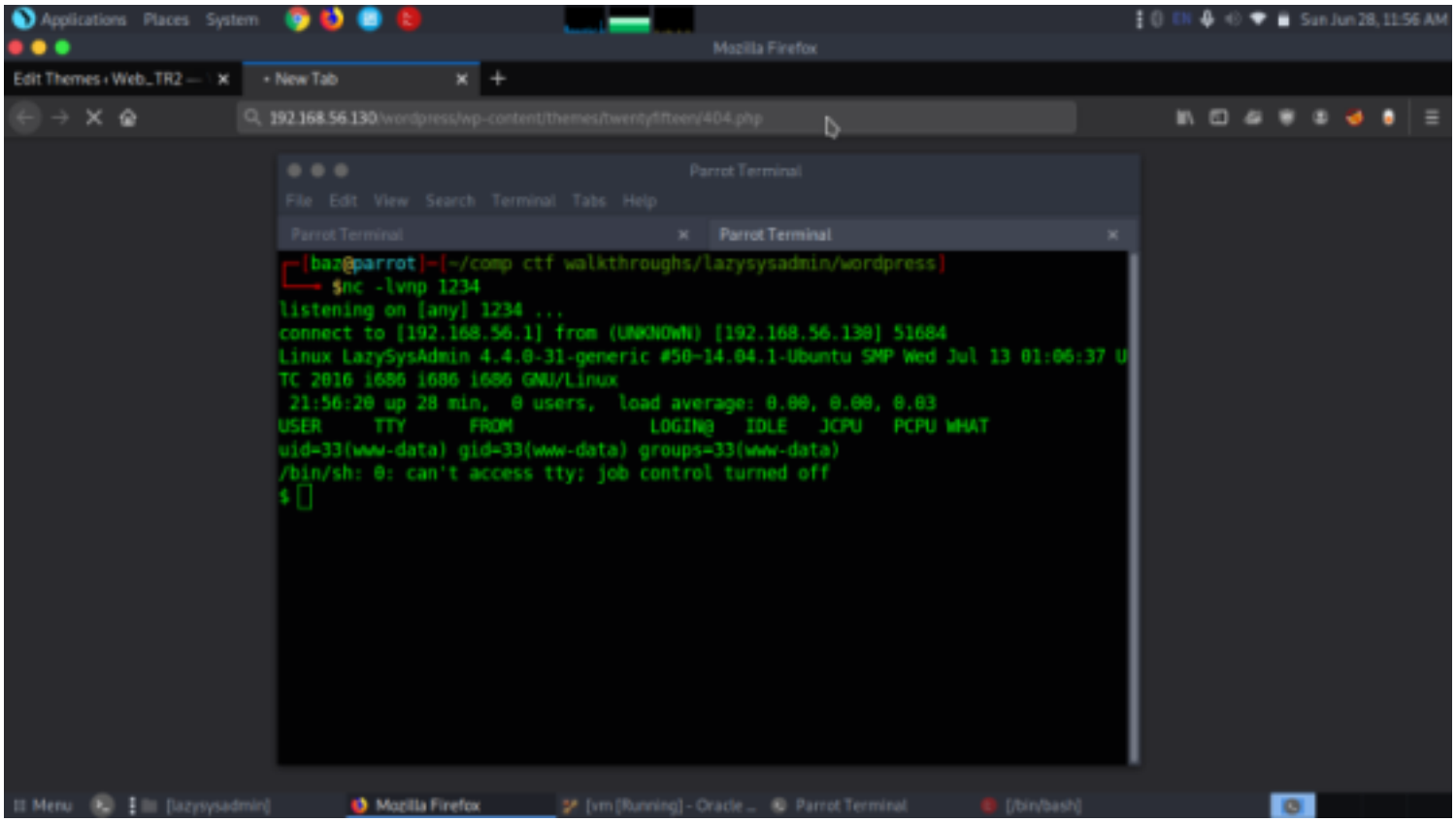
from robots.txt we got some more hidden directories which eventually didn't contain any important information so we moved on to check the login page

Exploitation

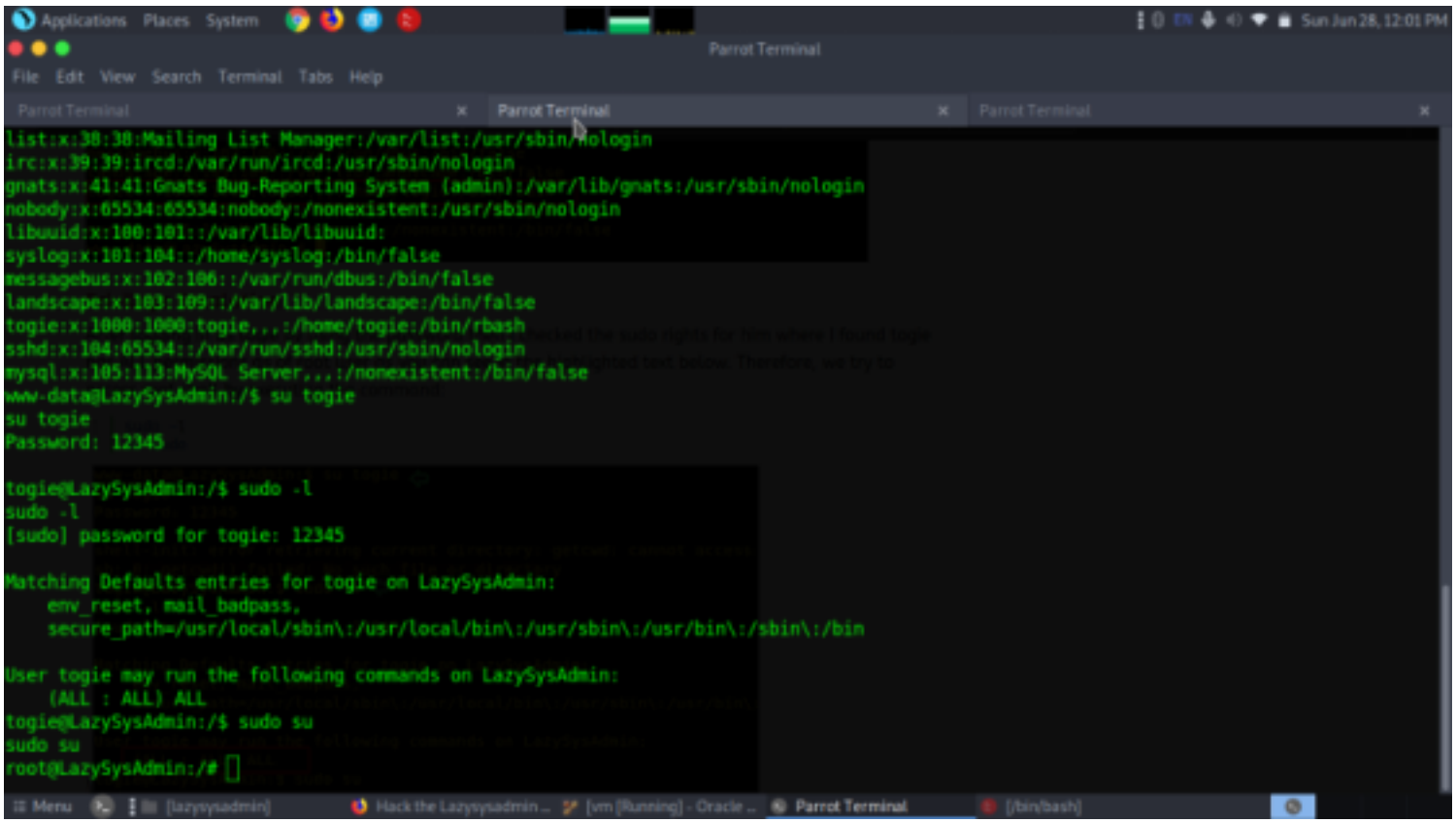
Now we had previously got the credentials of wordpress from smb port. when we tried to login with those credentials we got the admin panel



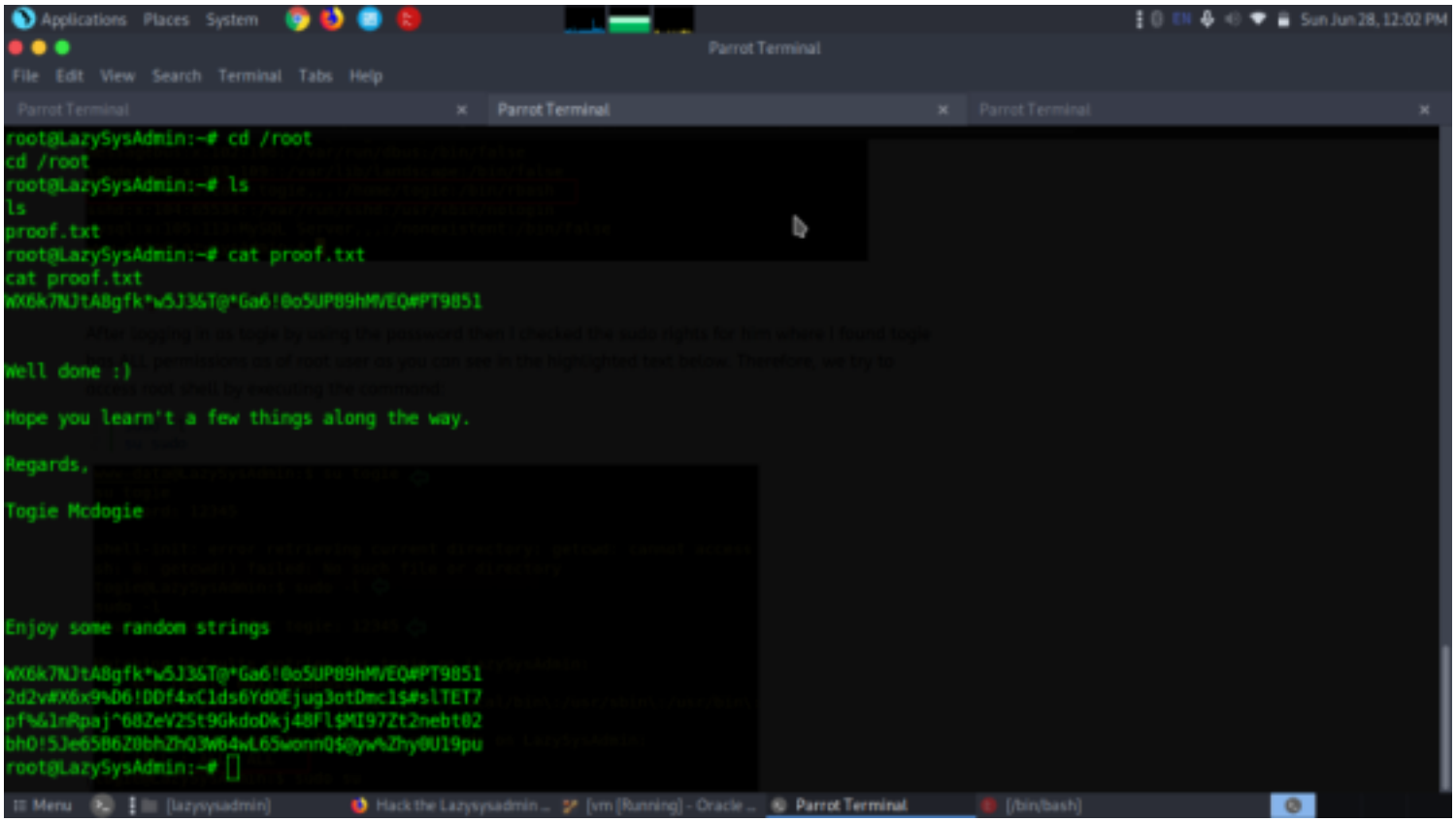
Then we inserted a php shell then started a listner



We got the reverse shell now let's exploit further more.
cat /etc/passwd
there was a user named togie and we had a password in deets.txt when tried we got access as user togie.
After logging in as togie by using the password then I checked the sudo rights for him where I found togie has ALL permissions as of root user as you can see in the highlighted text below. Therefore, we try to access root shell by executing the command:
sudo -l
pass-12345
sudo su



there we have got access as root user. Hereby going inside the root directory and listing its content we found our flag in proof.txt.



.....Have a nice day.....