Table of Content

Recon

nmap

```
Discovered open port 22/tcp on 10.10.10.121
Discovered open port 80/tcp on 10.10.10.121
Discovered open port 3000/tcp on 10.10.10.121

22/tcp   open  ssh     syn-ack ttl 63 OpenSSH 7.2p2 Ubuntu 4ubuntu2.6 (Ubuntu Linux; protocol 2.0)
80/tcp   open  http    syn-ack ttl 63 Apache httpd 2.4.18 ((Ubuntu))
3000/tcp open  http    syn-ack ttl 63 Node.js Express framework
```

Port 80 is a HelpDeskZ which suffers from a arbitraty file upload in some version Port 3000 will give you `{"message":"Hi Shiv, To get access please find the credentials with given query"}`

Initial Foothold - Get user.txt

Priv Esc - Get root.txt