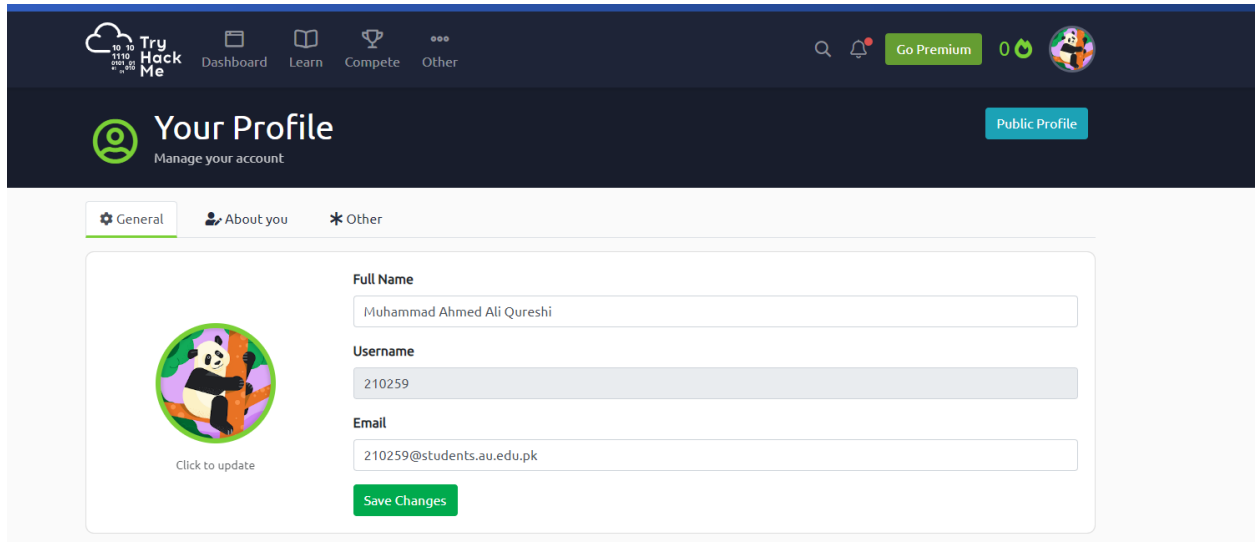


## Lab -Task-1 Solution

### 1. Account on Tryhackme:

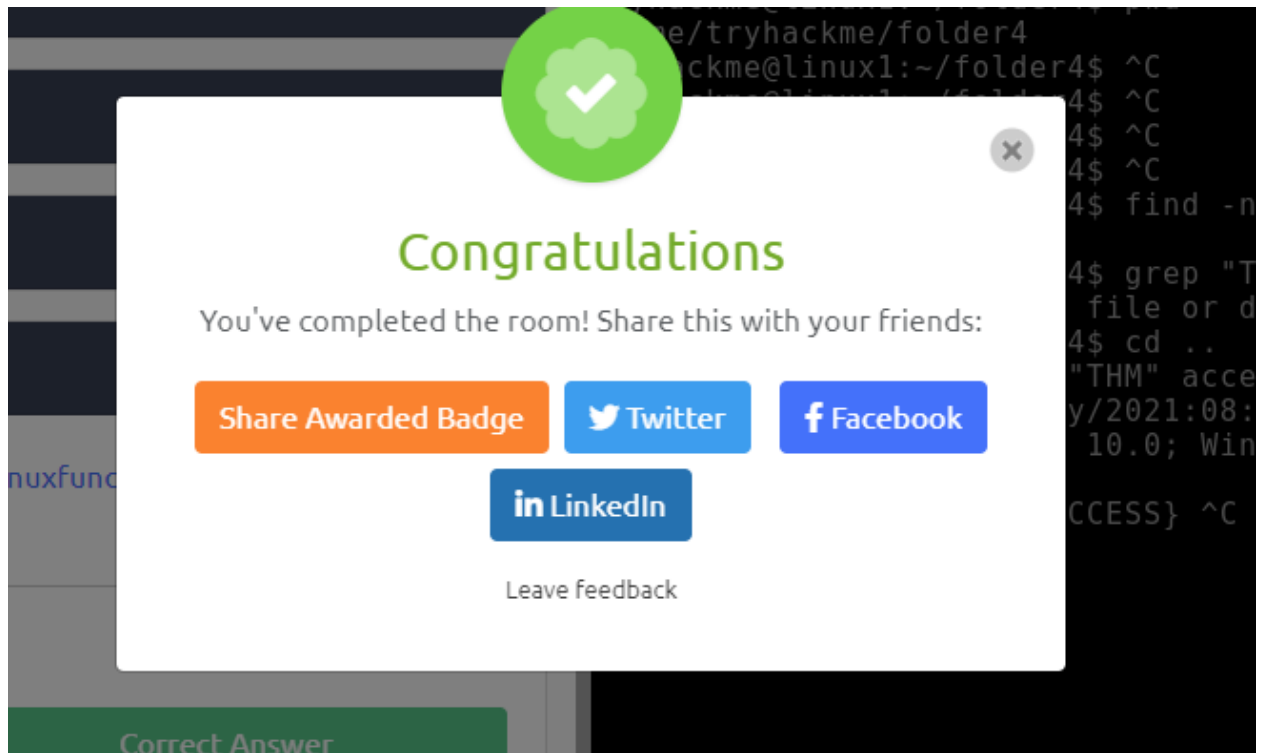


The screenshot displays the 'Your Profile' page on the TryHackMe platform. The page is divided into a header section and a main content area. The header section includes the TryHackMe logo, navigation links (Dashboard, Learn, Compete, Other), a search icon, a notification bell, a 'Go Premium' button, and a user avatar. The main content area features a 'Your Profile' section with a profile picture of a panda, a 'Click to update' button, and a 'Public Profile' button. Below this, there are tabs for 'General', 'About you', and 'Other'. The 'General' tab is active, showing the user's full name, username, and email address. A 'Save Changes' button is located at the bottom of the form.


**Task 1: Write down complete paths for file1-file10 in form of a table.**

Files	Path
File1	C:\file1
File2	C:\file2
File3	C:\b\file3
File4	C:\b\file4
File5	C:\b\c\file5
File6	C:\users\user1\file6
File7	C:\b\c\file7
File8	C:\b\c\file8
File9	C:\users\user1\Documents\file9
File10	C:\users\user1\Documents\file10

### Task 3:



8015





# Linux Fundamentals Part 1

Embark on the journey of learning the fundamentals of Linux. Learn to run some of the first essential commands on an interactive terminal.

Awards

Help









Learn the Linux Fundamentals Part 1 | TryHackMe • May 27, 2021


Source: YouTube


100%


Task 1  Introduction


Task 2  A Bit of Background on Linux


Task 3  Interacting With Your First Linux Machine (In-Browser) 


Task 4  Running Your First few Commands

Task 5  Interacting With the Filesystem!

Task 6  Searching For Files

Task 7  An Introduction to Shell Operators

Task 8  Conclusions & Summaries

Task 9  Linux Fundamentals Part 2

Activate Windows

## Task 4:

- **List all `.log` files in the current directory:**

```
ls *.log
```

This command lists all files in the current directory that have the `.log` extension.

- **Read the contents of the file `/etc/group`:**

```
cat /etc/group
```

This command displays the contents of the `/etc/group` file, which contains information about the system's groups.

- **Search for the string "Failed" in all files in the `/var/log` directory:**

```
grep -r "Failed" /var/log
```

The `-r` option searches recursively in all files within the `/var/log` directory.

- **Calculate MD5 and SHA1 hashes of the file `/etc/passwd`:**

```
md5sum /etc/passwd
shasum /etc/passwd
```

These commands compute the MD5 and SHA1 checksums of the `/etc/passwd` file, useful for verifying file integrity.

- **Use the `file` command to determine the type of the file `/usr/bin/whoami`:**

```
file /usr/bin/whoami
```

### **Explanation:**

The output will typically indicate that it's an ELF 64-bit executable for Linux systems. It might also mention that the file is dynamically linked, the interpreter being used, and whether the binary is stripped of debugging information.

- **Display all printable strings of length  $\geq 10$  in the file `/bin/echo`:**

```
strings -n 10 /bin/echo
```

The `strings` command extracts printable text from binary files, and `-n 10` ensures that only strings of at least 10 characters are displayed.

- **Determine what's wrong with the `image.jpg` file:**

- The file is identified as an ELF 64-bit executable instead of a valid JPEG image. This indicates the file might be malicious, potentially disguised as an image to deceive users.

- **Find files modified in the last 10 minutes in the `/tmp` directory:**

```
find /tmp -type f -mmin -10
```

This command finds all files (`-type f`) in `/tmp` that have been modified within the last 10 minutes.

- **Display all active UDP connections on the system:**

```
netstat -tunap | grep udp
```

```
o
```

```
ss -tunap | grep udp
```

These commands display active UDP connections along with the associated application.