

# TryHackMe Lab Report

**Name:** Pelumi Johnson

**Date:** 01/04/2026

**Course / Platform:** TryHackMe

**Room:** Linux Fundamentals Part 1

**Operating System:** Ubuntu 20.04 LTS

## Objective

The objective of this lab was to build foundational Linux command-line skills by interacting directly with a live Linux operating system. The lab focused on understanding Linux basics, navigating the filesystem, managing files, searching logs, and controlling command execution using operators.

All tasks were completed using a real Ubuntu Linux machine deployed in-browser through TryHackMe.

## Tools & Environment Used

- Ubuntu 20.04 LTS (TryHackMe In-Browser Machine)
- Bash Shell
- Linux Command Line Utilities (echo, whoami, ls, cd, pwd, cat, grep)
- Shell Operators (>, >>, &&, &)

## Step 1: Introduction to Linux

Linux was introduced as an open-source operating system widely used across servers, cloud environments, embedded systems, websites, point-of-sale systems, and critical infrastructure. Unlike Windows and macOS, Linux is commonly interacted with through the command line, especially in professional and security-focused environments.

I learned that Linux is not a single operating system, but an umbrella term for many distributions (distros) such as Ubuntu and Debian. For this lab, Ubuntu was used.

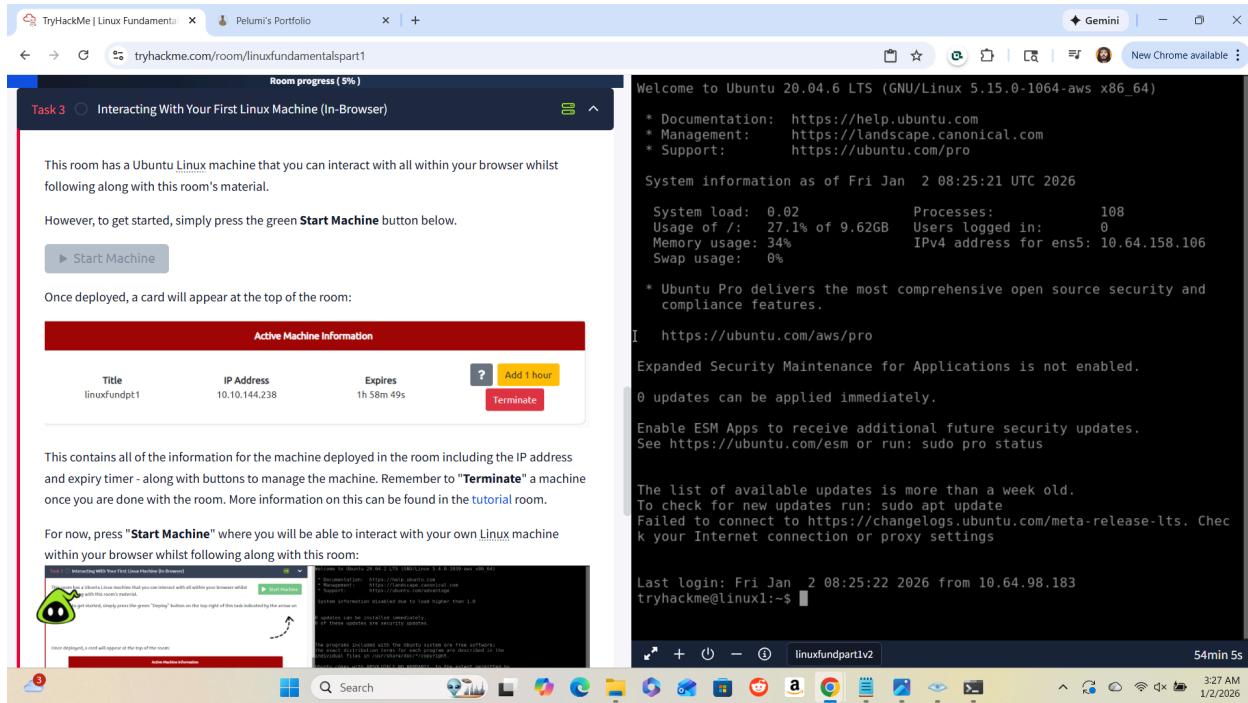
I also researched the history of Linux and confirmed that the first Linux operating system was released in 1991.

The screenshot shows a web browser window for tryhackme.com/room/linuxfundamentalspart1. At the top, there's a navigation bar with back, forward, and search icons, followed by the URL. To the right of the URL is a progress bar labeled "Room progress (5%)". Below the navigation bar, a header bar displays "Task 1" and "Introduction". A large Tux the Penguin logo is centered on the page. Below the logo, a welcome message reads: "Welcome to the first part of the "Linux Fundamentals" room series. You're most likely using a Windows or Mac machine, both are different in visual design and how they operate. Just like Windows, iOS and MacOS, Linux is just another operating system and one of the most popular in the world powering smart cars, android devices, supercomputers, home appliances, enterprise servers, and more." A note below states: "We'll be covering some of the history behind Linux and then eventually starting your journey of being a Linux-wizard! This room will have you:". A bulleted list follows: "• Running your very first commands in an interactive Linux machine in your browser  
• Teaching you some essential commands used to interact with the file system  
• Demonstrate how you can search for files and introduce shell operators". On the left side, there's a sidebar with a green alien icon and the text "Answer the questions below". Below the sidebar, a button says "Let's get started!". At the bottom, a toolbar has a "Check" button and a timestamp "2:59 AM 1/2/2026".

## Step 2: Deploying the Linux Machine

I deployed the Ubuntu Linux machine provided by TryHackMe directly in the browser. Once deployed, I was given access to a live terminal session.

This demonstrated how Linux servers are commonly accessed remotely and reinforced the importance of terminal-based interaction in real-world environments.



## Step 3: Basic Command Interaction

I practiced issuing basic commands to understand how the Linux terminal works.

### Commands used:

- Echo
- whoami

Using the echo command, I printed text to the terminal to confirm command execution.  
Using the whoami command, I identified the active user account.

The output confirmed that I was logged in as the user:

tryhackme

This step reinforced the importance of understanding user context when operating within Linux systems.

The screenshot shows a web browser window with the URL [tryhackme.com/room/linuxfundamentalspart1](https://tryhackme.com/room/linuxfundamentalspart1). The page has a header "Room progress (5%)". Below it is a table titled "Command" and "Description" with two rows: "echo" (Output any text that we provide) and "whoami" (Find out what user we're currently logged in as). A note says "See the snippets below for an example of each command being used". Two terminal snippets are shown: one for "Using echo" and another for "Using whoami to find out the username of who we're logged in as". The main content area shows system information as of Fri Jan 2 08:25:21 UTC 2026, including management and support links, system load, memory usage, swap usage, and network information. It also mentions Ubuntu Pro features and security updates. A terminal session at the bottom shows the user logging in as "tryhackme" and running "whoami" to show they are "pelumi johnson". The browser taskbar at the bottom shows various open tabs and icons.

## Step 4: Navigating the Linux Filesystem

I learned how Linux organizes files and directories and how to navigate the filesystem using terminal commands.

### Commands used:

- Pwd
- Ls
- Cd
- cd ..

Using `pwd`, I displayed the full path of my current working directory.

Using `ls`, I listed files and folders within directories.

Using `cd`, I moved into specific directories.

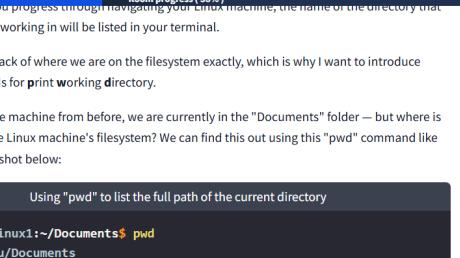
Using `cd ..`, I returned to the parent directory.

This helped me understand Linux directory structure and paths such as `/home/tryhackme`.

You'll notice as you progress through navigating your Linux machine, the name of the directory that you are currently working in will be listed in your terminal.

It's easy to lose track of where we are on the filesystem exactly, which is why I want to introduce "`pwd`". This stands for **p**rint **w**orking **d**irectory.

Using the example machine from before, we are currently in the "Documents" folder — but where is this exactly on the Linux machine's filesystem? We can find this out using this "`pwd`" command like within the screenshot below:



```
tryhackme@linux1:~/Documents$ pwd
/home/ubuntu/Documents
tryhackme@linux1:~/Documents$
```

**Let's break this down:**

1. We already know we're in "Documents" thanks to our terminal, but at this point in time, we have no idea where "Documents" is stored so that we can get back to it easily in the future.
2. I have used the "`pwd`" (print working directory) command to find the full file path of this "Documents" folder.
3. We're helpfully told by [Linux](#) that this "Documents" directory is stored at "`/home/ubuntu/Documents`" on the machine — great to know!
4. Now in the future, if we find ourselves in a different location, we can just use `cd` [/home/ubuntu/Documents](#) to change our working directory to this "Documents" directory.

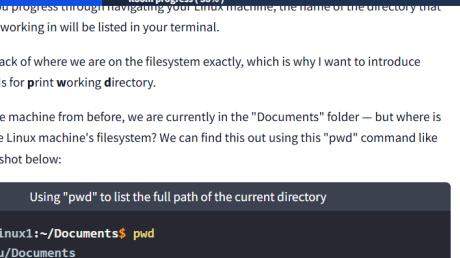
Answer the questions below

Room progress (38%)

You'll notice as you progress through navigating your Linux machine, the name of the directory that you are currently working in will be listed in your terminal.

It's easy to lose track of where we are on the filesystem exactly, which is why I want to introduce "`pwd`". This stands for **p**rint **w**orking **d**irectory.

Using the example machine from before, we are currently in the "Documents" folder — but where is this exactly on the Linux machine's filesystem? We can find this out using this "`pwd`" command like within the screenshot below:



```
tryhackme@linux1:~/Documents$ pwd
/home/ubuntu/Documents
tryhackme@linux1:~/Documents$
```

**Let's break this down:**

1. We already know we're in "Documents" thanks to our terminal, but at this point in time, we have no idea where "Documents" is stored so that we can get back to it easily in the future.
2. I have used the "`pwd`" (print working directory) command to find the full file path of this "Documents" folder.
3. We're helpfully told by [Linux](#) that this "Documents" directory is stored at "`/home/ubuntu/Documents`" on the machine — great to know!
4. Now in the future, if we find ourselves in a different location, we can just use `cd` [/home/ubuntu/Documents](#) to change our working directory to this "Documents" directory.

Answer the questions below

```
/home/tryhackme
tryhackme@linux1:~$ ls
Pelumi.txt access.log folder1 folder2 folder3 folder4 pelumi.txt
tryhackme@linux1:~$ cd ..
tryhackme@linux1:/home$ ls
tryhackme@ubuntu:~$ ls
tryhackme@ubuntu:~$ cd tryhackme
tryhackme@linux1:~$ ls
Pelumi.txt access.log folder1 folder2 folder3 folder4 pelumi.txt
tryhackme@linux1:~$ cat pelumi.txt
Pelumi
tryhackme@linux1:~$ cd ..
tryhackme@linux1:/home$ ls
tryhackme@ubuntu:~$ ls
tryhackme@ubuntu:~$ cd ubuntu
tryhackme@linux1:/home/ubuntu$ ls
tryhackme@linux1:/home/ubuntu$ ls
tryhackme@linux1:/home/ubuntu$ cd ..
tryhackme@linux1:/home$ cd tryhackme
tryhackme@linux1:~$ pwd
/home/tryhackme
tryhackme@linux1:~$ cd /home/ubuntu
tryhackme@linux1:/home/ubuntu$ cd /home/tryhackme
tryhackme@linux1:~$ ls
Pelumi.txt access.log folder1 folder2 folder3 folder4 pelumi.txt
tryhackme@linux1:~$ cd folder4
tryhackme@linux1:~/folder4$ ls
note.txt
tryhackme@linux1:~/folder4$ cat note.txt
Hello World!
tryhackme@linux1:~/folder4$ pwd
/home/tryhackme/folder4
tryhackme@linux1:~/folder4$
```

48min 32s

## **Step 5: Creating and Viewing Files**

I practiced creating files and viewing their contents directly from the command line.

## Commands used:

- echo "text" > filename
  - cat filename

Using output redirection (>), I created files and wrote text into them.

Using cat, I displayed the contents of files directly in the terminal.

This demonstrated how Linux treats nearly everything as a file and how command output can be redirected into files.

TryHackMe | Linux Fundamentals x 🔍 Pelumi's Portfolio x Gemini - New Chrome available

tryhackme.com/room/linuxfundamentalspart1

Room progress (36%) /home/ubuntu/Documents on the machine – great to know!

4. Now in the future, if we find ourselves in a different location, we can just use `cd` to change our working directory to this "Documents" directory.

Answer the questions below

On the Linux machine that you deploy, how many folders are there?

4 ✓ Correct Answer

Which directory contains a file?

folder4 ✓ Correct Answer 9

What is the contents of this file?

Hello World! ✓ Correct Answer

Use the `cd` command to navigate to this file and find out the new current working directory. What is the path?

/home/tryhackme/folder4 ✓ Correct Answer

Task 6 ⏺ Searching for Files

tryhackme@linux1:~\$ ls  
Pelumi.txt access.log folder1 folder2 folder3 folder4 pelumi.txt  
tryhackme@linux1:~\$ cd ..  
tryhackme@linux1:/home\$ ls  
**tryhackme** ubuntu  
tryhackme@linux1:/home\$ ls tryhackme  
Pelumi.txt access.log folder1 folder2 folder3 folder4 pelumi.txt  
tryhackme@linux1:~\$ cat pelumi.txt  
Pelumi  
tryhackme@linux1:~\$ cd ..  
tryhackme@linux1:/home\$ ls  
**tryhackme** ubuntu  
tryhackme@linux1:/home\$ cd ubuntu  
tryhackme@linux1:/home/ubuntu\$ ls  
tryhackme@linux1:/home/ubuntu\$ ls  
tryhackme@linux1:/home/ubuntu\$ cd ..  
tryhackme@linux1:/home\$ cd tryhackme  
tryhackme@linux1:~\$ pwd  
/home/tryhackme  
tryhackme@linux1:~\$ cd /home/ubuntu  
tryhackme@linux1:/home/ubuntu\$ cd /home/tryhackme  
tryhackme@linux1:~\$ ls  
Pelumi.txt access.log folder1 folder2 folder3 folder4 pelumi.txt  
tryhackme@linux1:~\$ cd folder4  
tryhackme@linux1:~/folder4\$ ls  
note.txt  
tryhackme@linux1:~/folder4\$ cat note.txt  
Hello World!  
tryhackme@linux1:~/folder4\$ pwd  
/home/tryhackme/folder4  
tryhackme@linux1:~/folder4\$ █

38min 19s

## Step 6: Searching Files and Logs with grep

I learned how to search through files efficiently using the grep command, which is essential when working with log files.

## **Command used:**

- grep "THM" access.log

Using grep, I searched a web server access log to find entries containing a specific pattern. This allowed me to successfully locate the embedded flag:

THM{ACCESS}

This step highlighted the importance of log analysis in cybersecurity monitoring and incident response.

The screenshot shows a web browser with two tabs: "TryHackMe | Linux Fundamentals" and "Pelumi's Portfolio". The main content area displays a challenge from TryHackMe. The challenge involves using the 'grep' command to search for an IP address in a log file. The terminal window shows the command being run and its output.

```

tryhackme@linux1:~$ grep "81.143.211.90" access.log
81.143.211.90 - - [25/Mar/2021:11:17 +0000] "GET / HTTP/1.1" 200 417 "-"
tryhackme@linux1:~$
```

"Grep" has searched through this file and has shown us any entries of what we've provided and that is contained within this log file for the IP.

**Answer the questions below**

Use grep on "access.log" to find the flag that has a prefix of "THM". What is the flag? **Note:** The "access.log" file is located in the "/home/tryhackme/" directory.

THM{ACCESS} Correct Answer 9

And I still haven't found what I'm looking for!

The terminal window shows the user attempting to find the THM flag in the access.log file. The output of the grep command is shown, indicating a successful search for the flag.

```

tryhackme@linux1:~$ ls
Pelumi.txt access.log folder1 folder2 folder3 folder4 pelumi.txt
tryhackme@linux1:~$ find -name *.txt
find: paths must precede expression: `pelumi.txt'
find: possible unquoted pattern after predicate `-name'?
tryhackme@linux1:~$ find -name *.txt
find: paths must precede expression: `pelumi.txt'
find: possible unquoted pattern after predicate `-name'?
tryhackme@linux1:~$ grep "THM" access.log
13.127.130.212 - - [04/May/2021:08:35:26 +0000] "GET THM{ACCESS}" lang=en
HTTP/1.1" 404 360 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.120 Safari/537.36"
tryhackme@linux1:~$
```

57min 20s

## Step 7: Output Redirection and Command Operators

I learned how Linux handles command output and how that output can be redirected or controlled using shell operators.

### Operators learned:

- > Overwrites file contents
- >> Appends to file contents
- ; connect multiple commands
- && Runs the next command only if the previous command succeeds
- & Runs a command in the background

### Commands used:

- echo password123 > passwords
- echo tryhackme >> passwords

Using the > operator, I replaced the contents of a file.

Using the >> operator, I appended new content without overwriting existing data.

TryHackMe | Linux Fundamentals x Pelumi's Portfolio x Gemini - +

tryhackme.com/room/linuxfundamentalspart1

Room progress (61%)

A great example of this is redirecting the output of the `echo` command that we learned in Task 4. Of course, running something such as `echo howdy` will return "howdy" back to our terminal — that isn't super useful. What we can do instead, is redirect "howdy" to something such as a new file!

Let's say we wanted to create a file named "welcome" with the message "hey". We can run `echo hey > welcome` where we want the file created with the contents "hey" like so:

Using the > Operator

```
tryhackme@linux1:~$ echo hey > welcome
```

Using cat to output the "welcome" file

```
tryhackme@linux1:~$ cat welcome
hey
```

Note: If the file i.e. "welcome" already exists, the contents will be overwritten!

### Operator ">>"

This operator is also an output redirector like in the previous operator (`>`) we discussed. However, what makes this operator different is that rather than overwriting any contents within a file, for example, it instead just puts the output at the end.

Following on with our previous example where we have the file "welcome" that has the contents of "hey". If were to use echo to add "hello" to the file using the `>>` operator, the file will now only have "hello" and not "hey".

Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.15.0-1064-aws x86\_64)

- \* Documentation: <https://help.ubuntu.com>
- \* Management: <https://landscape.canonical.com>
- \* Support: <https://ubuntu.com/pro>

System information as of Fri Jan 2 10:38:28 UTC 2026

System load:	0.01	Processes:	105
Usage of /:	27.1% of 9.62GB	Users logged in:	1
Memory usage:	33%	IPv4 address for ens5:	10.64.158.106
Swap usage:	0%		

Expanded Security Maintenance for Applications is not enabled.  
0 updates can be applied immediately.  
Enable ESM Apps to receive additional future security updates.  
See <https://ubuntu.com/esm> or run: sudo pro status

The list of available updates is more than a week old.  
To check for new updates run: sudo apt update  
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Fri Jan 2 10:36:10 2026 from 10.64.64.121  
tryhackme@linux1:~\$ echo hey > welcome  
tryhackme@linux1:~\$ cat welcome  
hey  
tryhackme@linux1:~\$

1h 17min 46s 6:03 AM 1/2/2026

TryHackMe | Linux Fundamentals x Pelumi's Portfolio x Gemini - +

tryhackme.com/room/linuxfundamentalspart1

Room progress (83%)

Answer the questions below

If we wanted to run a command in the background, what operator would we want to use?

& ✓ Correct Answer

If I wanted to replace the contents of a file named "passwords" with the word "password123", what would my command be?

echo password123 > passwords ✓ Correct Answer ?

Now if I wanted to add "tryhackme" to this file named "passwords" but also keep "password123", what would my command be?

echo tryhackme >> passwords ✓ Correct Answer ?

Now use the deployed Linux machine to put these into practice

No answer needed ✓ Correct Answer

Task 8 Conclusions & Summaries

Task 9 Linux Fundamentals Part 2

How likely are you to recommend this room to others?

Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.15.0-1064-aws x86\_64)

- \* Documentation: <https://help.ubuntu.com>
- \* Management: <https://landscape.canonical.com>
- \* Support: <https://ubuntu.com/pro>

System information as of Fri Jan 2 10:38:28 UTC 2026

System load:	0.01	Processes:	105
Usage of /:	27.1% of 9.62GB	Users logged in:	1
Memory usage:	33%	IPv4 address for ens5:	10.64.158.106
Swap usage:	0%		

Expanded Security Maintenance for Applications is not enabled.  
0 updates can be applied immediately.  
Enable ESM Apps to receive additional future security updates.  
See <https://ubuntu.com/esm> or run: sudo pro status

The list of available updates is more than a week old.  
To check for new updates run: sudo apt update  
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Fri Jan 2 10:36:10 2026 from 10.64.64.121  
tryhackme@linux1:~\$ echo hey > welcome  
tryhackme@linux1:~\$ cat welcome  
hey  
tryhackme@linux1:~\$

1h 4min 34s 6:16 AM 1/2/2026

## Step 8: Command Chaining with the Semicolon (;)

I learned how to connect multiple commands using the semicolon operator.

**Example:**

commandA ; commandB

Command A runs first, followed immediately by command B, regardless of whether command A succeeds or fails. This is useful when running independent commands sequentially.

## Step 9: Conditional Command Execution with &&

I learned how to chain commands conditionally using the && operator.

**Example:**

Command A && command B {sudo apt update && sudo apt upgrade -y}

This allows for running multiple commands on a go. With this operator, command B only runs if command A completes successfully. This ensures controlled execution and is commonly used in installations, updates, and automation scripts.

## Step 10: Background Execution with &

I learned how to run commands in the background while continuing to use the terminal.

**Example:**

command &

This allows a command to run asynchronously, meaning I could continue executing other commands while a process was running in the background. This demonstrated Linux's multitasking capabilities.

## Step 11: Practical Reinforcement

I applied all learned commands directly on the live Linux machine, reinforcing:

- User awareness

- Directory navigation
- File creation and modification
- Log searching
- Output redirection
- Command chaining and background execution

Each task was validated through TryHackMe's built-in checks.

## Completion

I successfully completed all tasks in the TryHackMe Linux Fundamentals Part 1 room. The completion screen confirmed that all exercises were validated and points were awarded.

## Key Takeaways

- Linux is precise and unforgiving, but extremely powerful when used intentionally
- The command line becomes approachable once its structure is understood
- Logs contain valuable information, and tools like grep help uncover it
- Small command-line skills form the foundation for advanced cybersecurity operations

