

# TryHackMe Lab Report

**Name:** Pelumi Johnson

**Platform:** TryHackMe

**Room:** Linux Fundamentals (Part 2)

**Operating System:** Ubuntu Linux (TryHackMe AttackBox)

**Date:** January 2026

## Objective

The objective of this documentation is to record and explain my hands-on progress through the **TryHackMe Linux Fundamentals** room. This lab focuses on strengthening foundational Linux command-line skills by practicing filesystem navigation, file management, permissions awareness, and command execution within a live Linux environment.

All activities were performed using the TryHackMe in-browser Ubuntu Linux machine.

## Environment & Tools Used

- Ubuntu Linux (TryHackMe AttackBox)
- Bash Shell
- Linux Command-Line Utilities:
  - ls, pwd, cd
  - touch, mkdir, rm
  - cp, mv
  - cat, file
  - grep

- Shell Operators:

- `>`, `>>`
  - `;`, `&&`, `&`

## Section 1: Creating Files and Directories

I practiced creating files and directories using basic Linux commands.

### Commands Used

- `touch` — create empty files
- `mkdir` — create directories
- `ls` — verify file and directory creation

## What I Did

- Created new files such as `security`, `data`, and `myfile`
- Created directories such as `myblog` and `myfolder`
- Verified creation using `ls`

This reinforced how Linux treats files and directories as fundamental objects and how quickly structure can be created from the terminal.

 *Screenshot: Creating files and directories*

---

## Section 2: Writing to and Viewing Files

I practiced writing data to files and displaying file contents directly from the terminal.

### Commands Used

- `echo "text" > filename`
- `echo "text" >> filename`
- `cat filename`

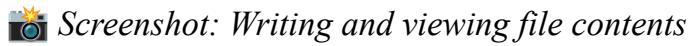
## What I Learned

- The `>` operator overwrites file contents

- The `>>` operator appends content without removing existing data
- `cat` allows quick inspection of file contents

Example:

- Added “access control” and “asset inventory” into the `security` file
- Verified contents using `cat security`



*Screenshot: Writing and viewing file contents*

---

## Section 3: Removing Files and Directories

I learned how to safely remove files and directories.

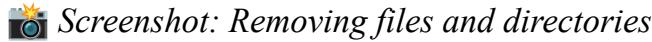
### Commands Used

- `rm filename`
- `rm -R directory`

### What I Did

- Removed files such as `security`
- Removed directories such as `myblog`
- Confirmed removal using `ls`

This reinforced the importance of caution when using `rm`, especially with recursive deletion.



*Screenshot: Removing files and directories*

---

## Section 4: Copying and Moving Files

I practiced duplicating and renaming files.

### Commands Used

- `cp source destination`
- `mv oldname newname`

### What I Did

- Copied `data` to `data2`
- Renamed `data2` to `data3`
- Verified changes using `ls`

This demonstrated how Linux handles file duplication and renaming without needing a graphical interface.

 *Screenshot: Copying and moving files*

---

## Section 5: Determining File Types

I used Linux utilities to determine file types rather than relying on file extensions.

### Command Used

- `file filename`

### What I Learned

- Files such as `unknown1` were identified as **ASCII text**
- Linux determines file type based on content, not extension

This reinforced a key Linux and security concept: file extensions cannot be trusted.

 *Screenshot: File type identification*

---

## Section 6: Permissions and Ownership

I examined file permissions and ownership.

### Commands Used

- `ls -l`
- `ls -a`

### What I Observed

- File ownership varies by user
- Permissions control read, write, and execute access
- Ownership determines who can modify or access files

This helped me understand how Linux enforces access control at the filesystem level.

 *Screenshot: File permissions and ownership*

---

## Section 7: Users and Privilege Context

I practiced switching users and understanding privilege boundaries.

## Commands Used

- `su user2`
- `su -l user2`

## What I Learned

- User context matters when accessing files
- Authentication failures occur when incorrect credentials are used
- Certain files are only readable by specific users

I successfully accessed restricted content once in the correct user context.

 *Screenshot: User switching and permissions*

---

## Section 8: Important Linux Directories

I explored core Linux directories and their purpose.

### Key Directories Studied

- `/var` — variable data such as logs
- `/var/log` — system and application logs
- `/tmp` — temporary storage (similar to RAM behavior)
- `/root` — home directory for the root user

Understanding these directories is essential for system administration and security monitoring.

 *Screenshot: Exploring system directories*

---

## Section 9: Practical Reinforcement

I applied all learned commands directly on the live Linux machine and validated each task through TryHackMe's built-in checks.

This included:

- Navigating directories
  - Creating, modifying, and deleting files
  - Searching file contents
  - Understanding permissions
  - Executing commands safely and intentionally
- 

## Progress Status

- Linux Fundamentals tasks completed progressively
- Multiple sections validated with correct answers
- Practical skills reinforced through repetition and real output

 *Screenshot: Task completion and progress indicators*

---

## Key Takeaways

- Linux rewards precision and intentional action
- The command line becomes intuitive with structured practice
- Files, permissions, and users form the foundation of system security
- These fundamentals directly support future cybersecurity tasks such as log analysis, incident response, and system hardening