



**EncryptEdge Labs**

# **Cybersecurity Analyst Internship**

## **Task Report**

atalmamun@gmail.com

Task No: 03



Copyright © 2024 EncryptEdge Labs. All rights reserved

Credit: Offensive Security



## Table of Contents

<b>1.0 EncryptEdge Labs Internship Task Report</b>	<b>3</b>
<i>1.1 Introduction</i>	3
<i>1.2 Objective</i>	3
<i>1.3 Requirements</i>	3
<b>2.0 Command-Line Navigation</b>	<b>4</b>
<b>3.0 File Operations</b>	<b>6</b>
<b>4.0 Text Manipulation</b>	<b>9</b>
<b>5.0 Hands-on Labs (TryHackMe: Linux Fundamentals)</b>	<b>15</b>
<b>6.0 Reflection</b>	<b>21</b>



## 1.0 EncryptEdge Labs Internship Task Report

### 1.1 Introduction

Linux is a powerful and widely used operating system in cybersecurity and penetration testing. Proficiency in Linux commands is essential for security professionals, as many cybersecurity tools and techniques are designed for Linux-based environments.

This report outlines my learning experience with fundamental Linux commands, focusing on command-line navigation, file operations, text manipulation, and hands-on labs. The goal of this task is to develop confidence in operating within a Linux environment, which is crucial for cybersecurity roles, especially in penetration testing and system administration.

### 1.2 Objective

The primary objectives of this task are:

- To gain proficiency in navigating the Linux file system using command-line tools.
- To understand and execute essential file operations such as creation, copying, moving, and deletion.
- To manage file permissions and ownership using `chmod` and `chown` commands.
- To practice text manipulation commands, including `cat`, `grep`, `awk`, and `sed`.
- To complete hands-on labs in TryHackMe's Linux Fundamentals, reinforcing theoretical knowledge with practical exercises.

### 1.3 Requirements

To successfully complete this task, the following requirements must be met:

- Access to a Linux-based system (preferably Kali Linux or Ubuntu).

- Basic understanding of the Linux command-line interface.
  - Execution of command-line navigation tasks, including `pwd`, `cd`, and `ls`.
  - Completion of file operations using commands such as `touch`, `cp`, `mv`, and `rm`.
  - Application of file permission and ownership changes using `chmod` and `chown`.
  - Familiarity with text manipulation commands like `cat`, `grep`, `awk`, and `sed`.
  - Hands-on experience through TryHackMe's Linux Fundamentals lab.

## 2.0 Command-Line Navigation

Gain familiarity with the Linux file system and master essential commands for directory exploration.

## **Commands Practiced:**

- `pwd` – Displays the current working directory.
  - `cd` – Changes directories (e.g., `cd /etc`).
  - `ls` – Lists directory contents (`ls -l` for detailed view).

## Screenshots:

```
kali㉿kali:~$ cd /etc  
kali㉿kali:~/etc$ ls  
Desktop Documents Downloads Music Pictures Public Templates Videos received_file.txt  
kali㉿kali:~/etc$ cd ..  
kali㉿kali:~$ ls  
Desktop Documents Downloads Music Pictures Public Templates Videos received_file.txt  
kali㉿kali:~$ cd /etc  
kali㉿kali:~/etc$ ls  
ImageMagick-6 firebird libccid_Info.plist papersize smartmontools  
ModemManager firefox-esr libibusverbs.d passwd smi.conf  
NetworkManager fonts libibusvbus.d passwd- smp  
ODBCDataSources freeds libpaper.d perl speech-dispatcher  
OpenCL fstab lightdm pmstrongswan  
OpenSC gnutls libpam.d plymouth polkit-1 ssl  
X11 gai.conf locale.alias postgresql salsplit  
adduser.conf geoclue locale.conf postgresql-common strongswan.conf  
alsa ghostscript locale.gen powershell-empire strongswan.d  
alternatives glibvnc liblzo2.so profile stunnel  
apache2 gnuTLS liblzo2.so.1 ppp stunnel-grid  
apt-mirror gpmish liblogrotate.d profile.d subgid  
aparmor.d groff liblogrotate.d protocols subuid  
apt groff liblogrotate.d proxychains4.conf subuid  
arp-scan group macchanger pulse subversion  
avahi group machine-id python2.7 sudo  
bash bashrc grub.d magisk python3.7 sudo_10gsrvd.conf  
bash_completion gshadow magic.mime python3.11 sudoers  
bash_completion.d gshadow-mailcap pythontest.11 sudoers.d  
bindresvport.blacklist gss mailcap.order qemu  
binfmt_d gtk-2.0 manpath.config radcli sv  
bluetooth gtk-3.0 matplotlibrc rc0.d sysctl.conf  
ca-certificates guymager mime.types rc1.d sysctl.d  
certmonger.conf hdparm.conf minicom rc2.d sysstat  
cifs-utils host.conf miredo.conf rc3.d sysvinit  
cifs-utils host.conf miredo.conf rc4.d terminfo
```



```
kali@kali: /etc
$ ls -l
total 1484
drwxr-xr-x  2 root    root    4096 Oct 20  2023 ImageMagick-6
drwxr-xr-x  4 root    root    4096 Oct 20  2023 ModemManager
drwxr-xr-x  7 root    root    4096 Oct 20  2023 NetworkManager
drwxr-xr-x  2 root    root    4096 Jun 16  2023 ODBCDataSources
drwxr-xr-x  3 root    root    4096 Oct 20  2023 OpenCL
drwxr-xr-x  2 root    root    4096 Oct 20  2023 UPower
drwxr-xr-x  11 root   root    3386 Jun 27  2023 adduser.conf
drwxr-xr-x  3 root    root    4096 Oct 20  2023 alsamixer
drwxr-xr-x  2 root    root    20480 Oct 20  2023 alternatives
drwxr-xr-x  8 root    root    4096 Oct 20  2023 apache2
drwxr-xr-x  2 root    root    4096 Oct 20  2023 apparmor
drwxr-xr-x  2 root    root    4096 Oct 20  2023 apparmor.d
drwxr-xr-x  9 root    root    4096 Oct 20  2023 apt
drwxr-xr-x  8 root    root    4096 Oct 20  2023 arp-scan
drwxr-xr-x  3 root    root    4096 Oct 20  2023 avahi
drwxr-xr-x  1 root    root    1994 Aug  5  2023 bash.bashrc
drwxr-xr-x  1 root    root    45 Jan 24  2020 bash_completion
drwxr-xr-x  2 root    root    4096 Oct 20  2023 bash_completion.d
drwxr-xr-x  1 root    root    367 Sep 22  2022 bindnfsport.blacklist
drwxr-xr-x  2 root    root    4096 Jul 28  2023 binfmt.d
drwxr-xr-x  2 root    root    4096 Oct 20  2023 bluetooth
drwxr-xr-x  3 root    root    4096 Oct 20  2023 ca-certificates
drwxr-xr-x  1 root    root    5989 Oct 20  2023 ca-certificates.conf
drwxr-s---  2 root    dip     4096 Oct 20  2023 chatscripts
drwxr-xr-x  2 root    root    4096 Oct 20  2023 cifs-utils
drwxr-xr-x  3 root    root    4096 Oct 20  2023 cloud
drwxr-xr-x  2 root    root    4096 Oct 20  2023 console-setup
drwx----- 2 root    root    4096 Jul 28  2023 credstore
drwx----- 2 root    root    4096 Jul 28  2023 credstore.encrypted
drwxr-xr-x  2 root    root    4096 Oct 20  2023 cron.d
drwxr-xr-x  2 root    root    4096 Oct 20  2023 cron.daily
drwxr-xr-x  2 root    root    4096 Oct 20  2023 cron.hourly
drwxr-xr-x  2 root    root    4096 Oct 20  2023 cron.monthly
drwxr-xr-x  2 root    root    4096 Oct 20  2023 cron.weekly
drwxr-xr-x  2 root    root    4096 Oct 20  2023 cron.yearly
drwxr-xr-x  1 root    root    1042 Jul 26  2023 crontab
drwxr-xr-x  2 root    root    4096 Oct 20  2023 cryptsetup-initramfs
drwxr-xr-x  2 root    root    4096 Aug 14  2023 cryptsetup-nuke-password
drwxr-xr-x  1 root    root    54 Oct 20  2023 crypttab
```

```
kali@kali: /var
$ cd /home
(kali㉿kali)-[~/]
$ cd /home
(kali㉿kali)-[~/]
$ ls -l
total 4
drwxr----- 16 kali kali 4096 Mar 18 17:05 kali
(kali㉿kali)-[~/]
$ ls
kali
(kali㉿kali)-[~/]
$ cd
(kali㉿kali)-[~]
$ pwd
/home/kali
(kali㉿kali)-[~]
$ cd /var
(kali㉿kali)-[/var]
$ ls -l
total 40
drwxr-xr-x  2 root root  4096 Mar 18 15:15 backups
drwxr-xr-x  17 root root  4096 Oct 20  2023 cache
drwxr-xr-x  76 root root  4096 Oct 20  2023 lib
drwxrwsr-x  2 root staff 4096 Aug  8  2023 local
lrwxrwxrwx  1 root root   9 Oct 20  2023 lock → /run/lock
drwxr-xr-x  21 root root  4096 Mar 18 17:04 log
drwxrwsr-x  2 root mail  4096 Oct 20  2023 mail
drwxr-xr-x  2 root root  4096 Oct 20  2023 opt
lrwxrwxrwx  1 root root   4 Oct 20  2023 run → /run
```



### Observations:

Understanding the Linux file system hierarchy, including `/home`, `/etc`, and `/var`, helped in navigating directories efficiently.

## 3.0 File Operations

Learn to create, copy, move, delete files, and manage permissions.

### Commands Practiced:

#### File Creation & Management:

- `touch myfile.txt` – Creates a new file.
- `cp myfile.txt /tmp/` – Copies the file to `/tmp/`.
- `mv myfile.txt mynewfile.txt` – Renames/moves the file.
- `rm mynewfile.txt` – Deletes the file.

#### File Permissions & Ownership:

- `chmod 755 myfile.txt` – Changes file permissions.
- `chown user:user myfile.txt` – Changes file ownership.

### Screenshots:



A screenshot of a Kali Linux desktop environment. On the left, there's a dock with icons for Trash, File System (with Home selected), share, and wireshark. A terminal window is open in the center, showing the following session:

```
(kali㉿kali)-[~]
└─$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos
(kali㉿kali)-[~]
└─$ touch myfile.txt
(kali㉿kali)-[~]
└─$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos myfile.txt
(kali㉿kali)-[~]
└─$ cp myfile.txt /tmp
(kali㉿kali)-[~]
└─$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos myfile.txt
(kali㉿kali)-[~]
└─$ cd /tmp
(kali㉿kali)-[/tmp]
└─$ pwd
/tmp
(kali㉿kali)-[/tmp]
└─$ ls
Temp-7fa55c02-8bf7-4c8f-808c-ea7ad3b4c80c
myfile.txt
ssh-BouRQu0P4Trx
ssh-q90rD65Hk68m
systemd-private-7ef05700ff4347f5a88d807cf42ec5cc-ModemManager.service-7Ew7mY
systemd-private-7ef05700ff4347f5a88d807cf42ec5cc-colord.service-lCnCQ6
systemd-private-7ef05700ff4347f5a88d807cf42ec5cc-haveged.service-sdtbSM
systemd-private-7ef05700ff4347f5a88d807cf42ec5cc-polkit.service-JONGNK
systemd-private-7ef05700ff4347f5a88d807cf42ec5cc-spice-vdagentd.service-71EPaQ
systemd-private-7ef05700ff4347f5a88d807cf42ec5cc-systemd-logind.service-icEr9B
systemd-private-7ef05700ff4347f5a88d807cf42ec5cc-upower.service-EN0s0r
systemd-private-d6518a04f74d480b87056e74f132a99e-ModemManager.service-NiKr62
systemd-private-d6518a04f74d480b87056e74f132a99e-colord.service-y85LRG
systemd-private-d6518a04f74d480b87056e74f132a99e-polkit.service-VyNXP
systemd-private-d6518a04f74d480b87056e74f132a99e-spice-vdagentd.service-3DkX8H
```

A screenshot of a Kali Linux desktop environment. On the left, there's a dock with icons for share and wireshark. A terminal window is open in the center, showing the following session:

```
(kali㉿kali)-[/tmp]
└─$ mv myfile.txt mynewfile.txt
(kali㉿kali)-[/tmp]
└─$ ls
Temp-7fa55c02-8bf7-4c8f-808c-ea7ad3b4c80c
mynewfile.txt
ssh-BouRQu0P4Trx
ssh-q90rD65Hk68m
systemd-private-7ef05700ff4347f5a88d807cf42ec5cc-ModemManager.service-7Ew7mY
systemd-private-7ef05700ff4347f5a88d807cf42ec5cc-colord.service-lCnCQ6
systemd-private-7ef05700ff4347f5a88d807cf42ec5cc-haveged.service-sdtbSM
systemd-private-7ef05700ff4347f5a88d807cf42ec5cc-polkit.service-JONGNK
systemd-private-7ef05700ff4347f5a88d807cf42ec5cc-spice-vdagentd.service-71EPaQ
systemd-private-7ef05700ff4347f5a88d807cf42ec5cc-systemd-logind.service-icEr9B
systemd-private-7ef05700ff4347f5a88d807cf42ec5cc-upower.service-EN0s0r
systemd-private-d6518a04f74d480b87056e74f132a99e-ModemManager.service-NiKr62
systemd-private-d6518a04f74d480b87056e74f132a99e-colord.service-y85LRG
systemd-private-d6518a04f74d480b87056e74f132a99e-polkit.service-VyNXP
systemd-private-d6518a04f74d480b87056e74f132a99e-spice-vdagentd.service-3DkX8H
systemd-private-d6518a04f74d480b87056e74f132a99e-systemd-logind.service-C2rup5
systemd-private-d6518a04f74d480b87056e74f132a99e-upower.service-xat2ch
wireshark_eth0.pcapng
(kali㉿kali)-[/tmp]
└─$
```





The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window displays the following command-line session:

```
(kali㉿kali)-[~]
$ id newuser
id: 'newuser': no such user

(kali㉿kali)-[~]
$ sudo useradd newuser
[sudo] password for kali:

(kali㉿kali)-[~]
$ chown kali:newuser myfile.txt
chown: changing ownership of 'myfile.txt': Operation not permitted

(kali㉿kali)-[~]
$ ls -l
total 32
drwxr-xr-x 2 kali kali 4096 Mar 18 14:34 Desktop
drwxr-xr-x 2 kali kali 4096 Oct 20 2023 Documents
drwxr-xr-x 2 kali kali 4096 Oct 20 2023 Downloads
drwxr-xr-x 2 kali kali 4096 Oct 20 2023 Music
drwxr-xr-x 2 kali kali 4096 Oct 20 2023 Pictures
drwxr-xr-x 2 kali kali 4096 Oct 20 2023 Public
drwxr-xr-x 2 kali kali 4096 Oct 20 2023 Templates
drwxr-xr-x 2 kali kali 4096 Oct 20 2023 Videos
-rw-r--r-- 1 kali kali 0 Mar 18 17:13 myfile.txt

(kali㉿kali)-[~]
$ sudo chown kali:newuser myfile.txt
[kali㉿kali]-[~]
$ ls -l
total 32
drwxr-xr-x 2 kali kali 4096 Mar 18 14:34 Desktop
drwxr-xr-x 2 kali kali 4096 Oct 20 2023 Documents
drwxr-xr-x 2 kali kali 4096 Oct 20 2023 Downloads
drwxr-xr-x 2 kali kali 4096 Oct 20 2023 Music
drwxr-xr-x 2 kali kali 4096 Oct 20 2023 Pictures
drwxr-xr-x 2 kali kali 4096 Oct 20 2023 Public
drwxr-xr-x 2 kali kali 4096 Oct 20 2023 Templates
drwxr-xr-x 2 kali kali 4096 Oct 20 2023 Videos
-rw-r--r-- 1 kali newuser 0 Mar 18 17:13 myfile.txt

(kali㉿kali)-[~]
```

## Observations:

Understanding permissions and ownership is crucial for security and access control in Linux systems.

## 4.0 Text Manipulation

Gain experience in viewing, editing, and manipulating text files.

### Commands Practiced:

#### Viewing Files:

- `cat myfile.txt` – Displays file content.



- `more myfile.txt / less myfile.txt` – Paginated file viewing.

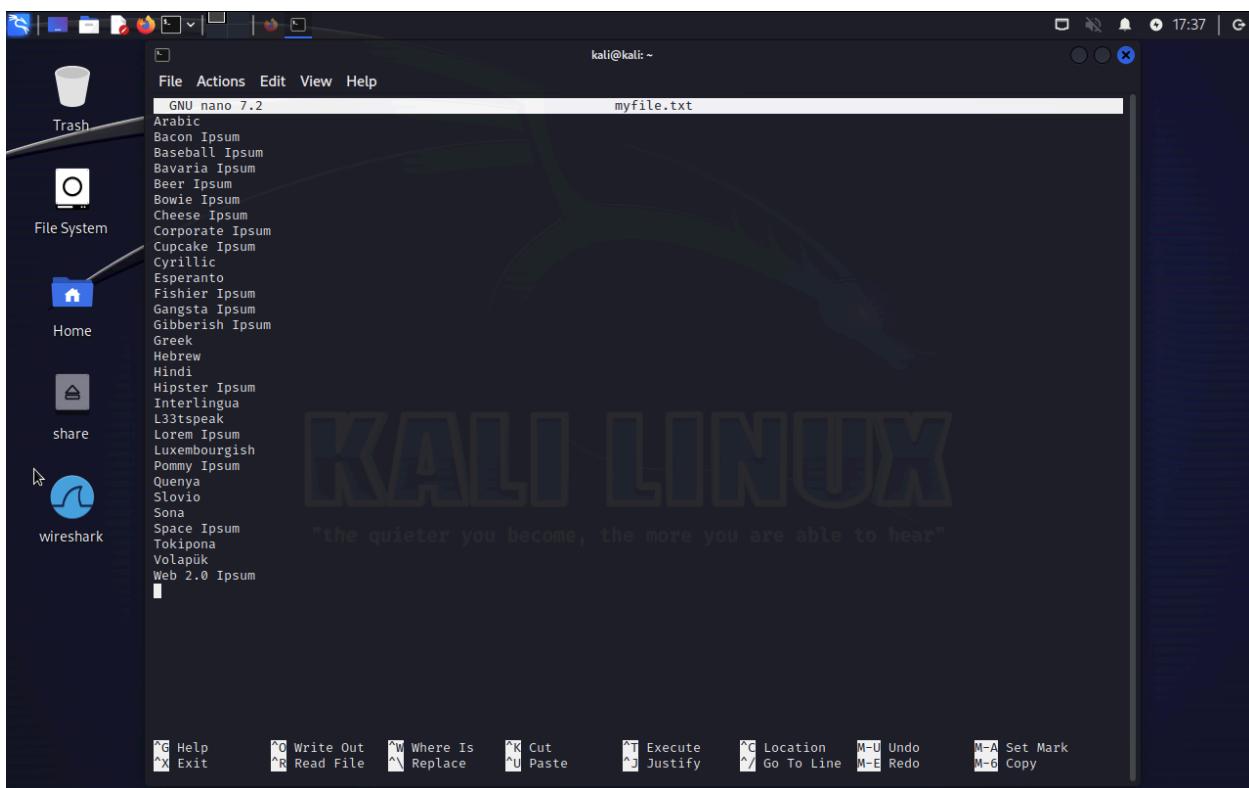
## Editing Files:

- `nano myfile.txt` – Edits a file using Nano.
- `vim myfile.txt` – Edits a file using Vim.

## Text Manipulation:

- `grep "search_term" myfile.txt` – Searches for specific text.
- `awk -F: '{print $1}' /etc/passwd` – Extracts specific fields.
- `sed 's/old/new/g' myfile.txt` – Replaces text in a file.

## Screenshots:

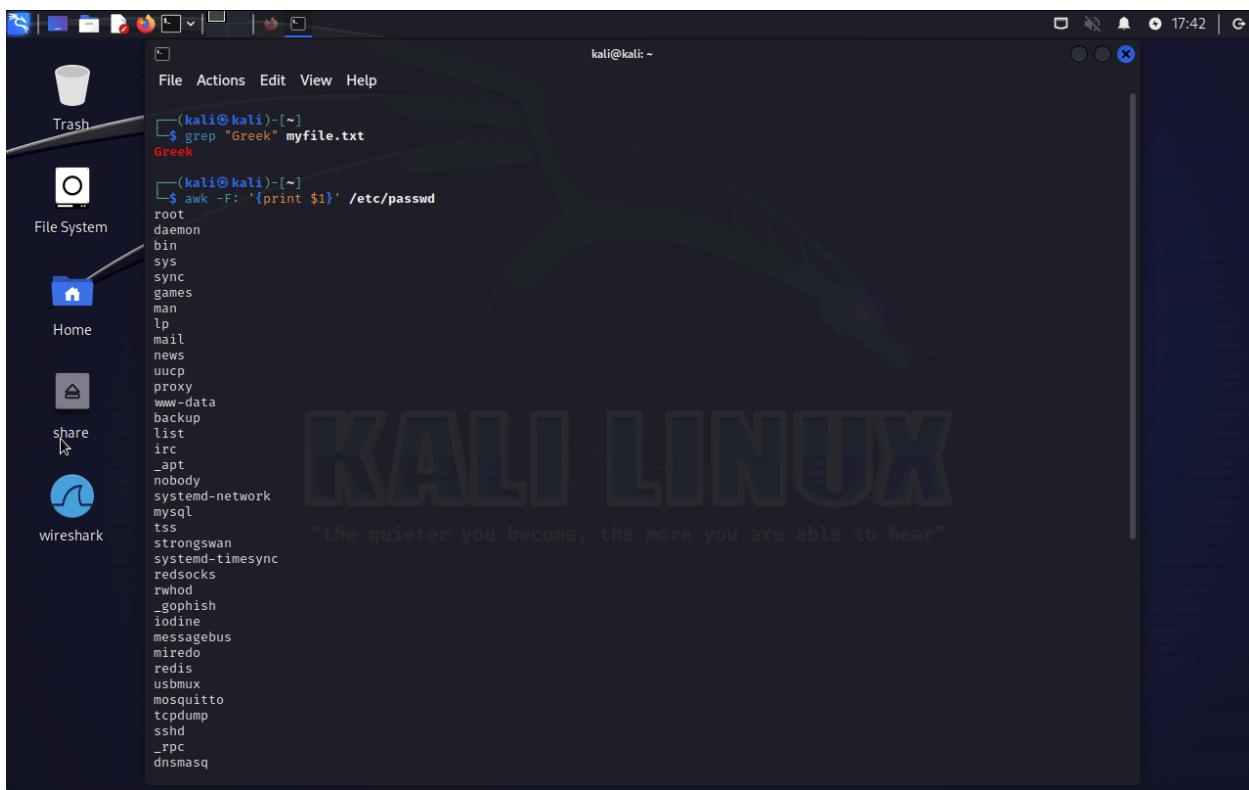


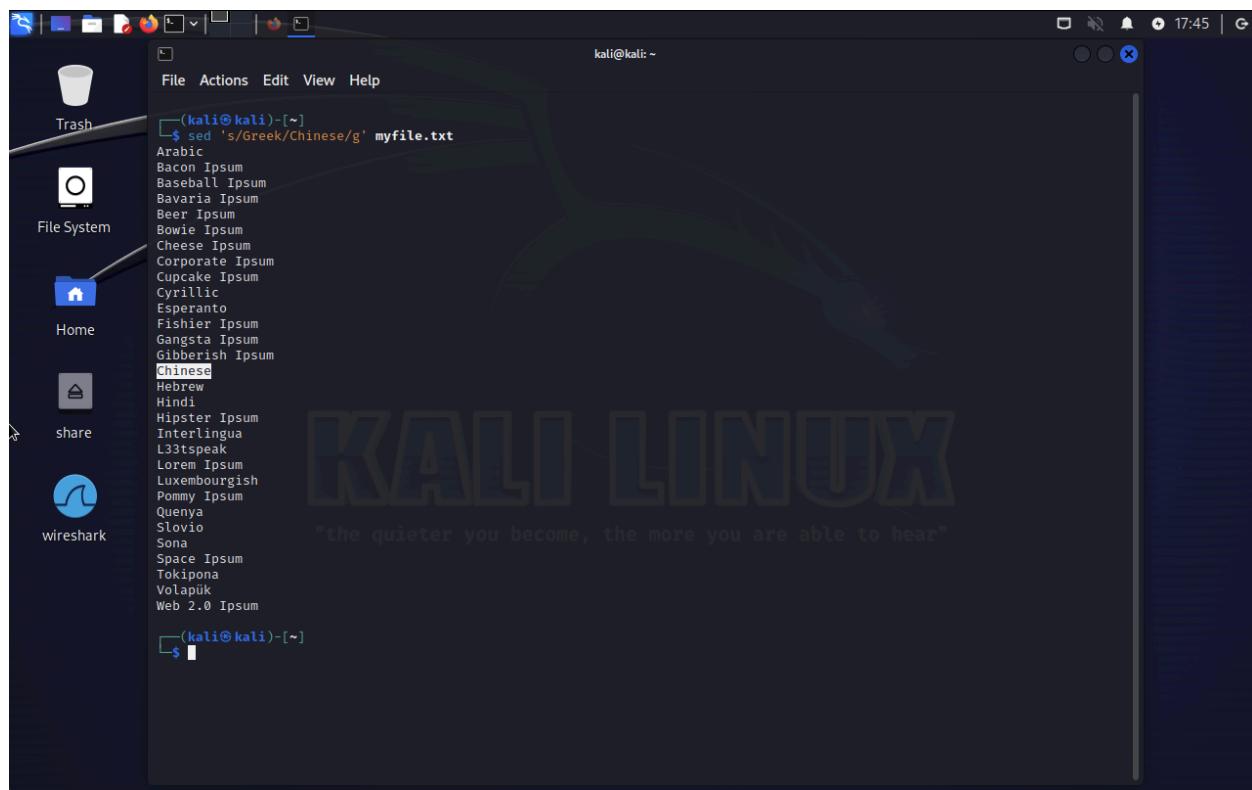




**EncryptEdge Labs**









## Observations:

These commands are useful for analyzing logs, processing files, and automating text-related tasks.

## 5.0 Hands-on Labs (TryHackMe: Linux Fundamentals)

Gain foundational knowledge of Linux systems by completing hands-on exercises.

### Lab Completion Screenshots:



- **Linux Fundamentals Part 1:**

The screenshot shows the TryHackMe platform interface for the 'Linux Fundamentals Part 1' room. At the top, there's a navigation bar with tabs for 'Dashboard', 'Learn', 'Compete', and 'Other'. A search bar and a notification bell icon are also present. The main content area has a dark background with a large cartoon penguin illustration. The title 'Linux Fundamentals Part 1' is displayed, along with a brief description: 'Embark on the journey of learning the fundamentals of Linux. Learn to run some of the first essential commands on an interactive terminal.' Below the title are 'Info' and '10 min' duration indicators. A green button labeled 'Share your achievement' is visible. The video player section shows a thumbnail for a YouTube video titled 'Learn the Linux Fundamentals - Part 1' from TryHackMe, dated May 26, 2021. The video player includes controls like play/pause and volume, and a 'Source: YouTube' link. The bottom section lists nine tasks with green checkmarks: 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), and Task 9 (Linux Fundamentals Part 2). A feedback section at the bottom asks 'How likely are you to recommend this room to others?' with a scale from 1 to 10.



tryhackme.com/room/linuxfundamentalspart1 Room completed (100%)

**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**

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

4 ✓ Correct Answer

Which directory contains a file?

folder4 ✓ Correct Answer 💡 Hint

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

- **Linux Fundamentals Part 2 (Optional):**



Screenshot of the TryHackMe website showing the Linux Fundamentals Part 2 room. The room is completed at 100%. The interface includes a navigation bar with 'Dashboard', 'Learn', 'Compete', and 'Other' tabs, and a sidebar with 'Access Machines', a search bar, a notification bell with 17 notifications, and a user profile icon.

**Cyber Security 101 > Linux Fundamentals > Linux Fundamentals Part 2**

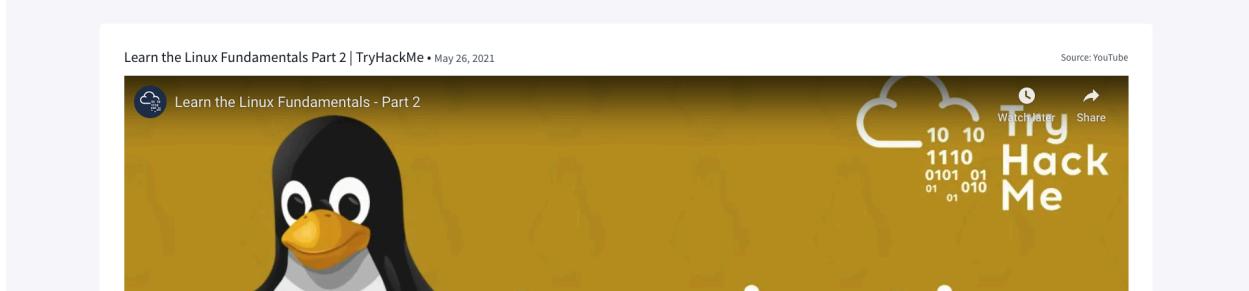
**Linux Fundamentals Part 2**

Continue your learning Linux journey with part two. You will be learning how to log in to a Linux machine using SSH, how to advance your commands, file system interaction.

**Info** 20 min

Share your achievement Start AttackBox Badge Help Save Room 8484 Options

Room completed (100%)



Screenshot of the TryHackMe website showing the completed Linux Fundamentals Part 2 room. The room is completed at 100%. The interface displays a list of tasks:

- Task 1 ✓ Introduction
- Task 2 ✓ Accessing Your Linux Machine Using SSH (Deploy)
- Task 3 ✓ Introduction to Flags and Switches
- Task 4 ✓ Filesystem Interaction Continued
- Task 5 ✓ Permissions 101
- Task 6 ✓ Common Directories
- Task 7 ✓ Conclusions and Summaries
- Task 8 ✓ Linux Fundamentals Part 3

How likely are you to recommend this room to others?

1 2 3 4 5 6 7 8 9 10

Submit now



The screenshot shows a web browser window for TryHackMe. The title bar says "tryhackme.com/room/linuxfundamentalspart2". The main content area displays a terminal session with the command "file note" and output "note: ASCII text". Below the terminal, there's a section titled "Answer the questions below" with several questions and input fields:

- How would you create the file named "newnote"? Input: "touch newnote" (marked as correct)
- On the deployable machine, what is the file type of "unknown1" in "tryhackme's" home directory? Input: "ASCII text" (marked as correct)
- How would we move the file "myfile" to the directory "myfolder"? Input: "mv myfile myfolder" (marked as correct)
- What are the contents of this file? Input: "THM{FILESYSTEM}" (marked as correct)
- Continue to apply your knowledge and practice the commands from this task. Input: "No answer needed" (marked as correct)

At the bottom, it says "Task 5 100% Complete".

- **Linux Fundamentals Part 3 (Optional):**



Screenshot of the TryHackMe platform showing the 'Linux Fundamentals Part 3' room. The room is completed at 100%. The interface includes a navigation bar with 'Dashboard', 'Learn', 'Compete', and 'Other' tabs, and a sidebar with 'Access Machines', a search bar, a notification bell, and a user icon. The main content area features a penguin icon, a brief description of the room, and various interaction buttons like 'Share your achievement', 'Start AttackBox', 'Badge', 'Help', 'Save Room', and 'Options'. A video player window titled 'Learn the Linux Fundamentals - Part 3' is embedded in the page, showing a video thumbnail with a penguin and binary code.

Screenshot of the TryHackMe platform showing the 'Linux Fundamentals Part 3' room. The room is completed at 100%. The interface includes a navigation bar with 'Dashboard', 'Learn', 'Compete', and 'Other' tabs, and a sidebar with 'Access Machines', a search bar, a notification bell, and a user icon. The main content area displays a list of tasks: Task 1 (Introduction), Task 2 (Deploy Your Linux Machine), Task 3 (Terminal Text Editors), Task 4 (General/Useful Utilities), Task 5 (Processes 101), Task 6 (Maintaining Your System: Automation), Task 7 (Maintaining Your System: Package Management), Task 8 (Maintaining Your System: Logs), and Task 9 (Conclusions & Summaries). Below the tasks is a feedback section asking 'How likely are you to recommend this room to others?' with a scale from 1 to 10.

A screenshot of a web browser showing a completed room on TryHackMe. The title bar says "tryhackme.com/room/linuxfundamentalspart3". The main content area displays several questions and their answers. Each question has a text input field and a "Correct Answer" button. Some answers are marked as correct (e.g., "301", "SIGTERM", "THM[PROCESSES]", "systemctl stop myservice", "systemctl enable myservice", "fg"). Other answers like "301" and "SIGTERM" have "Hint" buttons next to them. At the bottom, there are two collapsed sections: "Task 6" and "Task 7", both labeled "Maintaining Your System: Automation".

If we were to launch a process where the previous ID was "300", what would the ID of this new process be?  
301 ✓ Correct Answer

If we wanted to **cleanly** kill a process, what signal would we send it?  
SIGTERM ✓ Correct Answer

Locate the process that is running on the deployed instance (MACHINE\_IP). What flag is given?  
THM[PROCESSES] ✓ Correct Answer ⚡ Hint

What command would we use to stop the service "myservice"?  
systemctl stop myservice ✓ Correct Answer ⚡ Hint

What command would we use to start the same service on the boot-up of the system?  
systemctl enable myservice ✓ Correct Answer ⚡ Hint

What command would we use to bring a previously backgrounded process back to the foreground?  
fg ✓ Correct Answer

Task 6 ✓ Maintaining Your System: Automation

Task 7 ✓ Maintaining Your System: Package Management

## Observations:

The labs reinforced my understanding of Linux system administration, security configurations, and user management.

## 6.0 Reflection

### Key Learnings:

- Gained confidence in navigating the Linux file system and performing file operations.
- Understood file permissions and ownership, crucial for system security.
- Learned how to manipulate text files, search logs, and automate tasks using command-line utilities.



- Completed hands-on labs that enhanced my practical knowledge of Linux systems.

### **Challenges Faced:**

- Understanding file permissions (`chmod` and `chown`) initially required extra research.
- Editing with `vim` had a learning curve due to its different modes.
- Some TryHackMe labs required troubleshooting issues related to user privileges.

### **Application to Penetration Testing:**

- Mastering Linux commands is essential for ethical hacking, as most security tools run on Linux.
- Navigating directories, modifying files, and handling permissions are critical for penetration testing scenarios.
- Text manipulation skills help in analyzing logs and extracting useful information from security data.



**EncryptEdge Labs**

**This Internship Task report was developed on [Mar, 19, 2025]**

**By:**

**atalmamun@gmail.com**