

## Lab 4: Linux File Permissions and Ownership

### Objectives

In this lab, you will:

- Understand Linux file permissions and their implications.
- Learn to modify permissions and ownership of files and directories.
- Practice using permission-related commands with hands-on exercises.

### Background / Scenario

Linux employs a robust permission system that controls access to files and directories. Understanding and managing these permissions is crucial for system security. Each file and directory has an owner and a group associated with it, determining who can read, write, or execute the file.

### Required Resources

- Kali Linux VM
- Terminal access

### Concepts

#### 1. File Permissions

Linux file permissions determine who can read, write, or execute files. Permissions are divided into three types:

- **Read (r)**: Permission to read the file.
- **Write (w)**: Permission to modify or delete the file.
- **Execute (x)**: Permission to run the file as a program.

#### 2. User Types

- **Owner**: The user who created the file.
- **Group**: Users who belong to the same group as the file's group.
- **Others**: All other users.

#### 3. Permission Representation

Permissions are displayed as a string of ten characters:

- Example: `-rwxr-xr--`

- The first character indicates the type (- for file, d for directory).
- The next three characters are for the owner, the following three for the group, and the last three for others.

#### 4. Permission Codes Table

Symbol	Meaning	Octal Value
<b>r</b>	Read permission	4
<b>w</b>	Write permission	2
<b>x</b>	Execute permission	1
-	No permission	0

#### 5. Permissions Breakdown Table

Permissions String	Owner	Group	Others
<b>Rwxrwxrwx</b>	<b>rwx</b>	<b>rwx</b>	<b>rwx</b>
<b>Octal Equivalent</b>	<b>777</b>		

#### Commands to Learn

- **ls -l**: List files with permissions.
- **chmod**: Change file permissions.
- **chown**: Change file ownership.
- **chgrp**: Change group ownership.

---

## Instructions

### Part 1: Viewing File Permissions

#### Step 1: Check Current Permissions

1. Open your terminal.
2. Create a new directory:

```
mkdir PermissionTest
```

3. Navigate into the directory:

```
cd PermissionTest
```

4. Create a new file:

```
touch testfile.txt
```

5. List the permissions:

```
ls -l
```

#### **What to Observe:**

- Notice the output showing permissions for testfile.txt.

### **Part 2: Modifying Permissions**

#### **Step 2: Change File Permissions**

1. Change the permissions of testfile.txt to 777 (full permissions for everyone):

```
chmod 777 testfile.txt
```

2. Verify the changes:

```
ls -l
```

#### **Explanation:**

- 777 means that the owner, group, and others all have read (r), write (w), and execute (x) permissions.
- This is useful for sharing files, but it poses security risks, as anyone can modify or delete the file.

#### **Step 3: Revert Permissions**

1. Revert the permissions to 644 (owner can read/write, group and others can read):

```
chmod 644 testfile.txt
```

2. Check permissions again:

```
ls -l
```

### **Exercise 1: Experiment with Permissions**

- Change the permissions of testfile.txt back to 777:

```
chmod 777 testfile.txt
```

- Verify the permissions again.

---

### **Part 3: Changing Ownership**

#### Step 4: Change File Ownership

1. Create a new user for testing (this may require sudo privileges):

```
sudo adduser testuser
```

2. Change the ownership of testfile.txt to testuser:

```
sudo chown testuser:testuser testfile.txt
```

3. Verify ownership:

```
ls -l
```

#### Exercise 2: Group Ownership

- Change the group ownership of testfile.txt to another group (e.g., staff):

```
sudo chgrp staff testfile.txt
```

- Check the ownership and permissions again.

---

### Part 4: Practical Exercises

#### Exercise 3: Create and Modify Permissions

1. Create three new files:

```
touch file1.txt file2.txt file3.txt
```

2. Set permissions as follows:

- file1.txt: Full permissions for owner, read and execute for group and others (755).
- file2.txt: Read and write for the owner, read for group and others (644).
- file3.txt: Full permissions for everyone (777).

3. `chmod 755 file1.txt`

4. `chmod 644 file2.txt`

```
chmod 777 file3.txt
```

5. Verify permissions for all files:

```
ls -l
```

#### Exercise 4: Ownership Challenge

1. Create a directory named Project and set your current user as the owner:
2. `mkdir Project`

`sudo chown $USER:$USER Project`

3. Verify the ownership:

`ls -ld Project`

---

#### Conclusion

In this lab, you learned about file permissions and ownership in Linux. Understanding these concepts is vital for securing your files and managing access in a multi-user environment. Mastery of permission commands will enable you to maintain control over your system's resources.

# Lab 5: Individual Research on Linux

## Objectives

In this lab, you will:

- Conduct individual research on various aspects of Linux.
- Analyze and present your findings in a structured format.
- Fill in a research table based on your findings.

## Background

Linux is a versatile, open-source operating system widely used in various domains, from personal computers to servers and embedded systems. Understanding its features, distributions, and applications is essential for anyone pursuing a career in cybersecurity or IT.

## Required Resources

- Access to the internet for research.
- Document editor (e.g., Google Docs, Microsoft Word).

## Instructions

### Part 1: Research Topics

Choose one of the following research topics related to Linux:

1. **Linux Distributions:** Research different Linux distributions, their features, and typical use cases.
2. **Linux Kernel:** Explore the architecture of the Linux kernel and its functions.
3. **Common Linux Commands:** Investigate essential Linux commands and their practical applications.
4. **Linux Security Features:** Analyze the security features in Linux, including user permissions and firewalls.
5. **Linux in Cloud Computing:** Examine the role of Linux in cloud services and infrastructures.

## Part 2: Research Process

1. **Gather Information:** Use reliable sources such as official documentation, educational websites, and community forums.
2. **Take Notes:** Document important findings, including facts, figures, and quotes.

## Part 3: Fill Out the Research Table

Use the table below to organize your research findings. Fill in each section based on your selected topic.

Topic	Key Findings	Source(s)	Additional Notes
-------	--------------	-----------	------------------

## Part 4: Submit Your Research

1. Compile your findings in a report format, including:
  - An overview of your chosen topic.
  - Detailed key findings, properly cited.
  - Any additional notes or insights you gathered during your research.
2. Submit your report through the portal.

## Conclusion

Through this individual research lab, you will deepen your understanding of Linux and its various components. This knowledge is vital for your development in cybersecurity and IT fields, enhancing your skills and readiness for real-world applications.

## Additional Resources

- [Linux Documentation Project](#)
- [How Linux Works: What Every Superuser Should Know](#)
- [Linux Journal](#)