**TryHackMe Journal - [Name]**

# Instructions

(1) Review the sample journal entry provided below

(2) Scroll down to find the name of the room you have been assigned/are working on
(Pro Tip: Turn on "Outline View" so you can navigate more easily - go to View → Show Outline)

(3) Complete the required rooms on TryHackMe, compiling notes as you work through the room. This might include:

- (a) Commonly used Code/Commands
- (b) Definitions/Explanations of important terms and concepts
- (c) Screenshots of useful diagrams

(4) Once you've completed the module, capture 2-4 important takeaways.

(5) After you get the hang of things, delete these instructions and the sample you were provided!

## Entry 1- SAMPLE

### **Room Name**: Linux Fundamentals 1

**Date Completed**: 12/20/2023
**Notes During the Room**:

- Similar to how you have different versions of Windows (7, 8 and 10), there are many different versions/distributions of Linux.

| Command | Description |
|---|---|
| echo | Output any text that we provide |
| whoami | Find out what user we're currently logged in as! |

| Command | Full Name |
|---|---|
| ls | listing |
| cd | change directory |

| | |
|---|---|
| cat | concatenate |
| pwd | print working directory |

| Symbol / Operator | Description |
|---|---|
| & | This operator allows you to run commands in the background of your terminal. |
| && | This operator allows you to combine multiple commands together in one line of your terminal. |
| > | This operator is a redirector - meaning that we can take the output from a command (such as using cat to output a file) and direct it elsewhere. |
| >> | This operator does the same function of the `>` operator but appends the output rather than replacing (meaning nothing is overwritten). |

**Important Takeaways**

- Linux is an OS, like Windows. There are many different versions of Linux that serve different purposes.
- Linux systems rely more heavily on the command line to do tasks, like navigate the file system.
- Same basic commands while working with files are ls, cd, cat and pwd

## Entry 1

**Room Name:** Linux Fundamentals 1
**Date Completed:** 05/05/2024

**Notes During the Room:**
**Commands and Descriptions:**

- `echo`: Output any text that we provide.
- `whoami`: Find out what user we're currently logged in as.
- `ls`: List directory contents.
- `cd`: Change directory.
- `cat`: Display content of files.
- `pwd`: Print the working directory.

**Operators and Special Symbols:**

- `&`: Allows you to run commands in the background of your terminal.
- `&&`: Allows you to combine multiple commands together in one line of your terminal.
- `>`: Redirects the output from a command to another location (overwrite mode).
- `>>`: Redirects the output from a command to another location (append mode).

**Usage Examples:**

- `echo "Hello $(whoami)! Welcome to your terminal."`: This command combination will greet the user with their username.
- `cd ~/Documents && ls`: This command combination changes to the Documents directory and then lists its contents.
- `cat file.txt > newfile.txt`: This command takes the content of file.txt and overwrites newfile.txt with this content.
- `echo "Additional line" >> newfile.txt`: This appends "Additional line" to the end of newfile.txt without deleting the existing content.

**Important Takeaways:**

- Linux is an OS like Windows, with many different versions serving different purposes.
- Linux systems rely heavily on the command line for tasks like navigating the file system.
- Basic commands include `ls`, `cd`, `cat`, and `pwd`.

---

## Entry 2

**Room Name:** Linux Fundamentals 2
**Date Completed:** 05/12/2024

**Notes During the Room:**
**Commands and Descriptions:**

- `touch`: Create file.
- `mkdir`: Create a folder.
- `cp`: Copy a file or folder.
- `mv`: Move a file or folder.
- `rm`: Remove a file or folder.
- `file`: Determine the type of a file.

**Important Takeaways:**

- Understanding file and directory management commands is crucial for efficient system navigation and maintenance.
- Commands like `touch`, `mkdir`, `cp`, `mv`, and `rm` are fundamental for creating, copying, moving, and deleting files and directories.

---

## Entry 3

**Room Name:** Linux Fundamentals 3
**Date Completed:** 05/19/2024

**Notes During the Room:**
**Crontab Values and Descriptions:**

- `MIN`: What minute to execute at.
- `HOUR`: What hour to execute at.
- `DOM`: What day of the month to execute at.
- `MON`: What month of the year to execute at.
- `DOW`: What day of the week to execute at.
- `CMD`: The actual command that will be executed.

**Important Takeaways:**

- Crontab is used for scheduling tasks in Unix-like operating systems.
- Understanding crontab syntax and scheduling parameters is essential for automating system tasks.

---

## Entry 4

**Room Name:** Linux Strength Training
**Date Completed:** 05/26/2024

**Notes During the Room:**

- Advanced exercises on navigating directories, manipulating files, and using more complex command-line tools.
- Reinforced knowledge of basic commands and introduced more advanced command usage.

**Important Takeaways:**

- Strengthening command-line skills improves efficiency in managing Linux systems.
- Advanced practice helps in mastering the Linux environment and preparing for real-world scenarios.

---

## Entry 5

**Room Name:** Intro to Logs
**Date Completed:** 06/02/2024

**Notes During the Room:**

- Understanding different log types and their importance.
- Basic log analysis techniques using command-line tools.

**Important Takeaways:**

- Logs are critical for monitoring and troubleshooting system and security issues.
- Effective log analysis helps in identifying and mitigating potential threats.

---

## Entry 6

**Room Name:** Wireshark Basics
**Date Completed:** 06/09/2024

**Notes During the Room:**

- Introduction to Wireshark for packet analysis.
- Basic navigation and filtering techniques in Wireshark.

**Important Takeaways:**

- Wireshark is a powerful tool for network traffic analysis.
- Understanding packet structures and using Wireshark enhances network troubleshooting and security analysis skills.

---

## Entry 7

**Room Name:** Wireshark 101
**Date Completed:** 06/16/2024

**Notes During the Room:**

- Advanced packet dissection techniques.
- Analysis of various network protocols including ARP, ICMP, TCP, DNS, HTTP, and HTTPS.

**Important Takeaways:**

- Advanced knowledge of Wireshark helps in detailed network traffic analysis.
- Proficiency in protocol analysis is essential for identifying and resolving network issues.

---

## Entry 8

**Room Name:** Windows Fundamentals 1
**Date Completed:** 06/23/2024

**Notes During the Room:**

- Basics of Windows operating system and file systems.
- User account control (UAC) and system configuration.

**Important Takeaways:**

- Understanding Windows OS fundamentals is crucial for managing and securing Windows-based systems.
- Familiarity with UAC and system configuration helps in maintaining system integrity and security.

---

## Entry 9

**Room Name:** Windows Fundamentals 2
**Date Completed:** 06/30/2024

**Notes During the Room:**

- Advanced Windows configuration and security settings.
- Understanding the Windows registry and file system structures (FAT/NTFS).

**Important Takeaways:**

- Advanced knowledge of Windows configuration enhances system management capabilities.

- Proficiency in registry and file system management is critical for system troubleshooting and security.

---

## Entry 10

**Room Name:** Windows Fundamentals 3
**Date Completed:** 07/07/2024

**Notes During the Room:**

- In-depth exploration of Windows security features.
- Techniques for securing Windows systems against various threats.

**Important Takeaways:**

- Advanced security settings and features in Windows help in protecting against cyber threats.
- Continuous learning and practice are necessary to stay updated with Windows security practices.

---

## Entry 11

**Room Name:** Windows Forensics 1
**Date Completed:** 07/14/2024

**Notes During the Room:**

- Introduction to forensic analysis on Windows systems.
- Techniques for recovering deleted files and analyzing system artifacts.

**Important Takeaways:**

- Forensic skills are essential for investigating security incidents and breaches.
- Understanding system artifacts helps in uncovering malicious activities.

---

## Entry 12

**Room Name:** Windows Forensics 2
**Date Completed:** 07/21/2024

**Notes During the Room:**

- Advanced forensic analysis techniques.
- Utilizing tools like registry explorer for in-depth analysis.

**Important Takeaways:**

- Advanced forensic analysis helps in thorough investigation and incident response.
- Proficiency in forensic tools enhances the ability to recover and analyze critical data.

---

## Entry 13

**Room Name:** Intro to Log Analysis
**Date Completed:** 07/28/2024

**Notes During the Room:**

- Techniques for effective log analysis.
- Tools and methods for parsing and interpreting log data.

**Important Takeaways:**

- Effective log analysis is crucial for identifying and responding to security incidents.
- Familiarity with log analysis tools improves the ability to detect and mitigate threats.

---

## Entry 14

**Room Name:** Splunk Basics
**Date Completed:** 08/04/2024

**Notes During the Room:**

- Introduction to Splunk for data analysis and visualization.
- Basic navigation and search techniques in Splunk.

**Important Takeaways:**

- Splunk is a powerful tool for analyzing and visualizing large datasets.
- Proficiency in Splunk enhances the ability to monitor and respond to security events.

---

## Entry 15

**Room Name:** Incident Handling with Splunk
**Date Completed:** 08/11/2024

**Notes During the Room:**

- Techniques for incident handling using Splunk.

- Using Splunk for security investigations and response.

**Important Takeaways:**

- Splunk is an essential tool for incident handling and response.
- Effective use of Splunk helps in quickly identifying and resolving security incidents.

---

## Entry 16

**Room Name:** Splunk 2
**Date Completed:** 08/18/2024

**Notes During the Room:**

- Advanced search and reporting techniques in Splunk.
- Creating dashboards and visualizations for security monitoring.

**Important Takeaways:**

- Advanced skills in Splunk improve the ability to monitor and report on security events.
- Creating effective dashboards helps in visualizing and interpreting security data.

---

## Entry 17

**Room Name:** Splunk 3
**Date Completed:** 08/25/2024

**Notes During the Room:**

- Advanced incident handling and automation in Splunk.
- Using Splunk for proactive threat detection and response.

**Important Takeaways:**

- Proficiency in Splunk automation enhances incident response capabilities.
- Advanced incident handling techniques in Splunk help in mitigating security threats effectively.

---

This journal captures the key takeaways and notes for each TryHackMe room, highlighting your progress and proficiency in various cybersecurity skills.