**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)   1. Complete the required rooms on TryHackMe, compiling notes as you work through the room. This might include:    1. Commonly used Code/Commands    2. Definitions/Explanations of important terms and concepts    3. Screenshots of useful diagrams 2. Once you’ve completed the module, capture 2-4 important takeaways. 3. After you get the hang of things, delete these instructions and the sample you were provided! |
| --- |

[Entry 1- SAMPLE](#_23drygy33cs7)

[Room Name: Linux Fundamentals 1](#_9vvz4g4ibayw)

[Entry 1](#_1hsl3npa9rfw)

[Room Name: Linux Fundamentals 1](#_qu0yyb2ejc0w)

[Entry 2](#_rssbp32e2g8m)

[Room Name: Linux Fundamentals 2](#_638z74u39hd6)

[Entry 3](#_cltwrfvb2owe)

[Room Name: Linux Fundamentals 3](#_2kl4qua7c8a1)

[Entry 4](#_2egcbux2xso7)

[Room Name: Linux Strength Training](#_5f5qjok47fjb)

[Entry 5](#_str0vgf5d80)

[Room Name: Intro to Logs](#_9ozf7tyhj2z1)

[Entry 6](#_ak1pof8ebyk6)

[Room Name: Wireshark Basics](#_w7wl7e3uwrrn)

[Entry 7](#_nzyixrmzwseg)

[Room Name: Wireshark 101](#_zdodqul745hz)

[Entry 8](#_wus2efos6bcc)

[Room Name: Windows Fundamentals 1](#_ltkwqp4he38n)

[Entry 9](#_fregcgt9agb0)

[Room Name: Windows Fundamentals 2](#_wruho7cdogl4)

[Entry 10](#_elanzhcb97j)

[Room Name: Windows Fundamentals 3](#_95wrsci0dg9e)

[Entry 11](#_g86u54ixvozg)

[Room Name: Windows Forensics 1](#_xfv515m7w632)

[Entry 12](#_atdks5ge6rk5)

[Room Name: Windows Forensics 2](#_qhosa2k0l7a6)

[Entry 13](#_v6k9voxxs4zc)

[Room Name: Intro to Log Analysis](#_1ws0odcehb3h)

[Entry 14](#_ihmevfqj73au)

[Room Name: Splunk Basics](#_8thwcuu7w9t9)

[Entry 15](#_v4ppfi3lwy10)

[Room Name: Incident Handling with Splunk](#_bm0uzj3i092e)

[Entry 16](#_3g1yj8gcyfez)

[Room Name: Splunk 2](#_wnal444q34qr)

[Entry 17](#_hb9jz3666q35)

[Room Name: Splunk 3](#_god1fagavfvg)

## 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 as the > operator but appends the output rather than replacing it (meaning nothing is overwritten). |

**Important Takeaways**

* Linux is an OS, like Windows. Many different versions of Linux serve different purposes.
* Linux systems rely more heavily on the command line to do tasks, like navigating the file system.
* The same basic commands while working with files are ls, cd, cat, and pwd

## Entry 1

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

**Date Completed**: 04/29/2024

**Notes During the Room**: Linux is one of the operating systems similar to Windows and MacOS which has different versions. Here are some Linux commands and their task

| **Commands** | **Description** |
| --- | --- |
| echo | Input the text you want to display |
| whoami | Print the user we are currently logged in as |

| **Command** | **Full form** |
| --- | --- |
| ls | Listing |
| cd | Change directory |
| pwd | Print working directory |
| cat | concatenate |

| **Symbol / Operator** | **Description** |
| --- | --- |
| & | This operator allows you to run commands in the background of your terminal |
| && | This operator allows you to combine multiple commands 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 as the > operator but appends the output rather than replacing it (meaning nothing is overwritten). |

**Important Takeaways**:

Linux is an operating system like Windows and macOS.

For security professionals, it's one of the important tools to learn.

Sometimes it makes work easier and consumes less time using Linux.

Some basic commands while working with files are ls, cd, cat, and pwd.

## Entry 2

### **Room Name**: Linux Fundamentals 2

**Date Completed**: 04/29/2024

**Notes During the Room**: Learned how to access the machine using a secure shell or SSH. SSH simply is a protocol between devices in an encrypted form. SSH allows us to remotely execute commands on another device.

| **Command** | **Description** |
| --- | --- |
| touch | Create a file |
| mkdr | Make directory |
| cp | Copy files or directory |
| mv | Move file or directory |
| rm | Remove file or directory |

Here are some common directories:

**/etc**: The etc folder (short for etcetera) is a commonplace location to store system files that are used by your operating system.

**/var**: The "/var" directory, with "var" being short for variable data, is one of the main root folders found on a Linux install. This folder stores data that is frequently accessed or written by services or applications running on the system.

**/root**: Unlike the /home directory, the /root folder is the home for the "root" system user. There isn't anything more to this folder other than just understanding that this is the home directory for the "root" user. But, it is worth mentioning as the logical presumption is that this user would have their data in a directory such as "/home/root" by default.

**/temp**: This is a unique root directory found on a Linux install. Short for "temporary", the /tmp directory is volatile and is used to store data that is only needed to be accessed once or twice.

**Important Takeaways**:

Learned how to connect to a Linux machine remotely using SSH

Advancing your use of commands by providing flags, switches, and where you can go to learn about these for each command (man pages)

Some more commands that you'll frequently be using to interact with the filesystem and its contents

A brief introduction to file permissions & switching users

A summary paragraph of the important root directories on a Ubuntu Linux install and how we may be able to use the data stored within these.

## Entry 3

### **Room Name**: Linux Fundamentals 3

**Date Completed**: 04/29/2024

**Notes During the Room**: we learned some useful utilities and applications that we are likely to use day-to-day. We also learn to deploy the tryhackme attackbox using our IP address. We learned about text editors like Nano and Vim and how t

**Important Takeaways**:

## Entry 4

### **Room Name**: Linux Strength Training

**Date Completed**: 05/06/2024

**Notes During the Room**: We learned how to find specific files/folders on the system by using the following information :

* Filename
* Size
* user/group
* Date modified
* Date accessed
* Its keyword contents

Here are some syntax:

**Find files based on the filename**

find /[directory path] -type f -name [filename]

**Find a directory based on the directory name**

find [directory path] -type d -name [filename]

**Find files based on size**

find [directory path] -type f -size [size]

**Find file based on group name**

find [directory path] -type f -group [group name]

**Find file based on group name**

find [directory path] -type f -user [user name]

**Find a file based on a specific date**

find [directory path] -type f -newermt ’[date and time]’

**Find file based on date modified**

find [directory path] -type f -newermt [ start date range]! - -newermt [end date range]

**Find a file based on a specific keyword**

Grep -iRl [directorypath/keyword]

**Read the manual for the find command**

man find

**Important Takeaways**: We learned different ways to find files and folders. We learned about hashing and its importance.

## Entry 5

### **Room Name**: Intro to Logs

**Date Completed**:

**Notes During the Room**:

**Important Takeaways**:

## Entry 6

### **Room Name**: Wireshark Basics

**Date Completed**:

**Notes During the Room**:

**Important Takeaways**:

## Entry 7

### **Room Name**: Wireshark 101

**Date Completed**:

**Notes During the Room**:

**Important Takeaways**:

## Entry 8

### **Room Name**: Windows Fundamentals 1

**Date Completed**:

**Notes During the Room**:

**Important Takeaways**:

## Entry 9

### **Room Name**: Windows Fundamentals 2

**Date Completed**:

**Notes During the Room**:

**Important Takeaways**:

## Entry 10

### **Room Name**: Windows Fundamentals 3

**Date Completed**:

**Notes During the Room**:

**Important Takeaways**:

## Entry 11

### **Room Name**: Windows Forensics 1

**Date Completed**:

**Notes During the Room**:

**Important Takeaways**:

## Entry 12

### **Room Name**: Windows Forensics 2

**Date Completed**:

**Notes During the Room**:

**Important Takeaways**:

## Entry 13

### **Room Name**: Intro to Log Analysis

**Date Completed**:

**Notes During the Room**:

**Important Takeaways**:

## Entry 14

### **Room Name**: Splunk Basics

**Date Completed**:

**Notes During the Room**:

**Important Takeaways**:

## Entry 15

### **Room Name**: Incident Handling with Splunk

**Date Completed**:

**Notes During the Room**:

**Important Takeaways**:

## Entry 16

### **Room Name**: Splunk 2

**Date Completed**:

**Notes During the Room**:

**Important Takeaways**:

## Entry 17

### **Room Name**: Splunk 3

**Date Completed**:

**Notes During the Room**:

**Important Takeaways**: