**TryHackMe Journal - Michael Hermann**

| **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 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**: 04/23/24

**Notes During the Room**:

| Command | Description |
| --- | --- |
| echo | Prints input text after echo IE echo “hello World” prints “hello World” |
| whoami | Prints current user |

| Command | Full Name |
| --- | --- |
| ls | List’s files. |
| cd | Change into a specific directory IE cd /Home/User/Downloads will put you into the downloads folder of the user in the Terminal |
| cat | Will print the file into the terminal. |
| pwd | Prints directory of current location OR will print the directory of the specified file/folder. |

| Symbol / Operator | Description |
| --- | --- |
| & | Tell commands to run in the background. |
| && | Tells your CLI to use multiple commands, must successfully complete to move to the next command. |
| > | Redirector - meaning that we can take the output from a command and direct it elsewhere. IE cat hello > hey will print hey when you use “cat hello” |
| >> | This operator does the same function of the > operator but adds the output rather than replacing, will print both. |

**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 2

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

**Date Completed**: 04/23/2024

**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 |
| --- | --- |
| ssh | Secure Shell - Connect remotely to another device, a protocol between devices in an encrypted form. Using cryptography, any input we send in a human-readable format is encrypted for traveling over a network -- where it is then unencrypted once it reaches the remote machine  ssh user@IPADDRESS > Password |
| Switches & Flags | Argument provided to command “nano -help” would show all arguments for nano. |

| Command | Full Name |
| --- | --- |
| Man (man pages) | List of all flags/switches for a particular command. |
| File system commands | Touch - Create file, Mkdir - create folder, cp - copy, mv - move, rm - remove, file - file |
| su | Switch between available users |
| Directories | /etc, /var, /root, /home,/tmp |

**Important Takeaways**:

* SSH is great for working inside of a server or remote host.
* Directories and Remote connections are easy to use with the CLI
* Already well versed in linux CLI commands.

## Entry 3

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

**Date Completed**: 04/23/2024

**Notes During the Room**:

| Command | Description |
| --- | --- |
| nano | Simple easy to use text editor |
| vim | My preferred Text editor, many more features and uses CLI |

| scp | Securely copy a file over SSH from one host to another. |
| --- | --- |
| wget/curl | Package installer - Just two of many |
| Systemctl | Systemctl <arg> <program> (Enable/Start/Stop) |
| Ctrl + Z OR fg | Sends a program to run in the background/Foreground. |

| Crontabs | Command and program automation on a schedule. Backing up files using a date/time format. |
| --- | --- |

**Important Takeaways**:

* Scp is super easy to use while your ssh into another machine, and fast.
* CLI makes handling linux connections and files easy.

## Entry 4

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

**Date Completed**:

**Notes During the Room**:

**Important Takeaways**:

## 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**: