**TryHackMe Journal - Ampith Anderson**

| **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! |
| --- |

[Instructions](#_slg4z2fxyog6)

[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](#_str0vgf5d80)

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

[Entry 5](#_ak1pof8ebyk6)

[Room Name: Wireshark Basics](#_w7wl7e3uwrrn)

[Entry 6](#_wus2efos6bcc)

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

[Entry 7](#_fregcgt9agb0)

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

[Entry 8](#_elanzhcb97j)

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

[Entry 9](#_g86u54ixvozg)

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

[Entry 10](#_atdks5ge6rk5)

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

[Entry 11](#_v6k9voxxs4zc)

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

[Entry 12](#_ihmevfqj73au)

[Room Name: Splunk Basics](#_8thwcuu7w9t9)

[Entry 13](#_v4ppfi3lwy10)

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

[Entry 14](#_3g1yj8gcyfez)

[Room Name: Splunk 2](#_wnal444q34qr)

[Entry 15](#_hb9jz3666q35)

[Room Name: Splunk 3](#_god1fagavfvg)

## Entry 1- SAMPLE

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

**Date Completed**: 03/22/2025

**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**: 03/22/2025

**Notes During the Room**:

* **Application Logs:** Messages about specific applications, including status, errors, warnings, etc.
* **Audit Logs:** Activities related to operational procedures crucial for regulatory compliance.
* **Security Logs:** Security events such as logins, permissions changes, firewall activity, etc.
* **Server Logs:** Various logs a server generates, including system, event, error, and access logs.
* **System Logs:** Kernel activities, system errors, boot sequences, and hardware status.
* **Network Logs:** Network traffic, connections, and other network-related events.
* **Database Logs:** Activities within a database system, such as queries and updates.
* **Web Server Logs:** Requests processed by a web server, including URLs, response codes, etc.

**Semi-structured Logs:** These logs may contain structured and unstructured data, with predictable components accommodating free-form text.

**Structured Logs:** Following a strict and standardised format, these logs are conducive to parsing and analysis.

**Unstructured Logs:** Comprising free-form text, these logs can be rich in context but may pose challenges in systematic parsing

**Log collection:** is an essential component of log analysis, involving the aggregation of logs from diverse sources such as servers, network devices, software, and databases.

**Important Takeaways**:

A log format defines the structure and organisation of data within a log file. It specifies how the data is encoded, how each entry is delimited, and what fields are included in each row.Utilising the **Network Time Protocol (NTP)** is a method to achieve this synchronisation and ensure the integrity of the timeline stored in the logs.

Efficient Log Management ensures that every gathered log is stored securely, organised systematically, and is ready for swift retrieval.

## Entry 2

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

**Date Completed**:

**Notes During the Room**:

**Important Takeaways**:

## Entry 3

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

**Date Completed**:

**Notes During the Room**:

**Important Takeaways**:

## Entry 4

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

**Date Completed**:

**Notes During the Room**:

**Important Takeaways**:

## Entry 5

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

**Date Completed**:

**Notes During the Room**:

**Important Takeaways**:

## Entry 6

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

**Date Completed**:

**Notes During the Room**:

**Important Takeaways**:

## Entry 7

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

**Date Completed**:

**Notes During the Room**:

**Important Takeaways**:

## Entry 8

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

**Date Completed**:

**Notes During the Room**:

**Important Takeaways**:

## Entry 9

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

**Date Completed**:

**Notes During the Room**:

**Important Takeaways**:

## Entry 10

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

**Date Completed**:

**Notes During the Room**:

**Important Takeaways**:

## Entry 11

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

**Date Completed**:

**Notes During the Room**:

**Important Takeaways**:

## Entry 12

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

**Date Completed**:

**Notes During the Room**:

**Important Takeaways**:

## Entry 13

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

**Date Completed**:

**Notes During the Room**:

**Important Takeaways**:

## Entry 14

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

**Date Completed**:

**Notes During the Room**:

**Important Takeaways**:

## Entry 15

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

**Date Completed**:

**Notes During the Room**:

**Important Takeaways**: