TryHackMe Journal - [CJ Chairez]

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: 6/25/24
Notes During the Room: Many different things use linux as it's one of the most popular OS's in the world. Things such as home appliances and even video game consoles. Also the name Linux us just an umbrella term used for multiple OS's that use Unix. And there are many different "Flavors" of Linux, such as Ubuntu, Debian, and Kali 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 2

Room Name: Linux Fundamentals 2

Date Completed:
Notes During the Room:**Flags and Arguments:**
Extend the functionality of terminal commands.

- **Filesystem Operations:** Creating, moving, and deleting files and folders.
- **Permissions:** Understanding read, write, and execute attributes.
- **Common Directories:** Purpose and functionalities of various Linux directories.

Accessing Your Linux Machine Using SSH

- **Action:** Follow TryHackMe guide to access the Linux machine using SSH.
- **Link:** TryHackMe Linux Fundamentals Part 2

Introduction to Flags and Switches

- **Learn to Use Flags:** Explore manual pages with `man ls`.
- **Example:** Use `ls -h` for human-readable output.
- **Questions:**
    - **Manual Page of ls Command:** Explored and understood.

Filesystem Interaction Continued

- **Commands:** `touch`, `mkdir`, `rm`, `cp`, `mv`, `file`.
- **Questions:**
    - **Create a File:** `touch newnote`
    - **File Type of "unknown1":** ASCII text
    - **Move File "myfile" to "myfolder":** `mv myfile myfolder`
    - **Contents of File:** THM{FILESYSTEM}

Permissions 101

- **Permissions:** Use `ls -lh` to view.
- **Switching Users:** `su` command.
- **Questions:**
    - **Owner of "important":** user2
    - **Switch to User "user2":** `su user2`
    - **Output Contents of "important":** THM{SU_USER2}

Common Directories

- **Directories:** /etc, /var, /root, /tmp.
- **Questions:**
    - **Logs Directory Path:** /var/log
    - **Directory Similar to RAM:** /tmp
    - **Home Directory of Root User:** /root

Additional Information

- **SSH:** Secure method to access a remote machine.
- **Manual Pages (`man`):** Documentation for commands and utilities.
- **Filesystem Commands:** Essential for managing files and directories.
- **Permissions:** Crucial for security and access control.
- **Common Directories:** Important for understanding Linux system structure.

Important Takeaways: This journey through Linux fundamentals highlighted the importance of understanding flags and arguments to enhance terminal command functionalities. Mastering essential filesystem operations, such as creating, moving, and deleting files, is crucial for efficient system management. Grasping file permissions and learning to switch users ensures proper security and access control within the system. Familiarity with common directories like /etc, /var, /root, and /tmp is essential for navigating and managing a Linux environment effectively.

Entry 3

Room Name: Linux Fundamentals 3

Date Completed:
Notes During the Room:

Terminal Text Editors

So far, we have only stored text in files using a combination of the echo command and the pipe operators (> and >>). This isn't efficient for handling data in files with multiple lines.

Nano

To create or edit a file using nano.

VIM

VIM is a more advanced text editor. Some benefits of VIM include customisable keyboard shortcuts, syntax highlighting, and compatibility with all terminals. There are many resources like cheatsheets and tutorials available for learning VIM.

General/Useful Utilities

Downloading Files

You can transfer files using wget.

Transferring Files From Your Host — SCP (SSH)

Secure copy (SCP) allows you to transfer files between two computers using the SSH protocol.

Serving Files From Your Host — WEB

Ubuntu machines come pre-packaged with Python3. The HTTPServer module can turn your computer into a web server.

Processes 101

Processes are programs running on your machine, managed by the kernel, and each process has an ID (PID).

Viewing Processes

Use the ps command to list running processes

Managing Processes:

Signals you can send include SIGTERM (kill but allow cleanup), SIGKILL (kill without cleanup), and SIGSTOP (stop/suspend a process).

Starting Processes

Processes start using namespaces, which split resources available on the computer. The process with ID 0 is started when the system boots.

Getting Processes/Services to Start on Boot

Use the systemctl command to manage services.

Backgrounding and Foregrounding

Processes can run in the background or foreground. Use the & operator to run a command in the background. Use Ctrl + Z to suspend a process and fg to bring it back to the foreground.

Maintaining Your System: Automation

Crontab is a special file recognized by the cron process to execute tasks.

Maintaining Your System: Package Management

Developers submit software to an apt repository, and you can manage repositories using the apt command.

Maintaining Your System: Logs

Log files are located in the /var/log directory and contain information about the applications and services running on your system. Logs are automatically managed by a process known as “rotating.” Logs for services such as web servers contain information about every request, allowing administrators to monitor system health and investigate activities.

Important Takeaways:

In this Linux Fundamentals module, you'll learn to use terminal text editors like Nano and VIM, enhancing your ability to efficiently handle and edit files directly from the command line. You will also gain skills in downloading files with wget, transferring files using SCP, and setting up a simple web server with Python's HTTPServer module. Additionally, you will understand how to manage processes using commands like ps, top, and kill, as well as automate tasks with crontab and manage software packages with apt. Finally, you will explore maintaining system logs found in the /var/log directory, which are crucial for monitoring system health and investigating issues. These skills are essential for effective Linux system administration and troubleshooting.

Entry 4

Room Name: Linux Strength Training

Date Completed:
Notes During the Room:

Terminal Text Editors

- **Nano and VIM**: Learn to use these text editors for editing files directly from the command line.
    - **Nano**: User-friendly, basic editing.
    - **VIM**: Powerful, advanced editing capabilities.

File Management and Transfer

- **wget**: Command to download files from the internet.
- **SCP**: Securely copy files between hosts over a network.

Setting Up a Simple Web Server

- **Python HTTPServer module**: Quickly set up a basic web server.

Process Management

- **ps, top, kill**: Monitor and manage system processes.
    - **ps**: List running processes.
    - **top**: Display and update a list of processes.
    - **kill**: Terminate processes by PID.

Task Automation

- **crontab**: Schedule and automate tasks.
    - Set up recurring tasks to run at specified times.

Package Management

- **apt**: Install, update, and manage software packages.
    - Use commands like `apt-get update` and `apt-get install`.

System Logs

- **/var/log directory**: Location of system logs.
    - Essential for monitoring system health and diagnosing issues.

Important Takeaways:
This course has text editors like Nano and VIM, with Nano being user-friendly and VIM offering advanced capabilities for efficient editing. It emphasizes the importance of file management and transfer, highlighting the `wget` command for downloading files and SCP for secure file transfers between hosts. Setting up a simple web server using Python's HTTPServer module is another key takeaway, enabling users to serve files and create basic web server environments. The module also covers crucial process management commands like `ps`, `top`, and `kill` for monitoring and controlling system processes. Lastly, it underscores the importance of task automation with `crontab`, package management with APT, and the role of system logs in monitoring and diagnosing system health.

Entry 5

Room Name: Intro to Logs

Date Completed: 6/25/24
Notes During the Room: Logs serve as invaluable records of past events, and a comprehensive understanding of logs is crucial for identifying patterns and mitigating potential threats. By analyzing logs as records of historical activities, individuals and organizations can gain essential knowledge, enhancing their overall awareness and preparedness across a wide range of situations. sudo -l can be used to check what sudo privileges a user has.

- **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.

A log format defines the structure and organization 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. These formats can vary widely and may fall into three main categories: Semi-structured, Structured, and Unstructured

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

- **Syslog Message Format:** A widely adopted logging protocol for system and network logs.
- **Windows Event Log (EVTX) Format:** Proprietary Microsoft log for Windows systems.

Structured Logs: Following a strict and standardised format, these logs are conducive to parsing and analysis. Typical structured log formats include:

- **Field Delimited Formats:** Comma-Separated Values (CSV) and Tab-Separated Values (TSV) are formats often used for tabular data
- **JavaScript Object Notation (JSON):** Known for its readability and compatibility with modern programming languages.
- **W3C Extended Log Format (ELF):** Defined by the World Wide Web Consortium (W3C), customizable for web server logging. It is typically used by Microsoft Internet Information Services (IIS) Web Server.
- **eXtensible Markup Language (XML):** Flexible and customizable for creating standardized logging formats.

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

- **NCSA Common Log Format (CLF):** A standardized web server log format for client requests. It is typically used by the Apache HTTP Server by default
- **NCSA Combined Log Format (Combined):** An extension of CLF, adding fields like referrer and user agent. It is typically used by Nginx HTTP Server by default.

Important Takeaways:

Logs serve as invaluable records of past events, crucial for identifying patterns and mitigating potential threats. Various types of logs, such as application, audit, security, server, system, network, database, and web server logs, each serve specific purposes. Log formats, including semi-structured, structured, and unstructured, define the structure and organization of log data. Understanding and utilizing these logs and formats enhance security measures, regulatory compliance, and overall system preparedness, with tools like `sudo -l` aiding in managing user privileges.

Entry 6

Room Name: Wireshark Basics

Date Completed:
Notes During the Room:

Wireshark is a powerful tool for analyzing network traffic, used for detecting network problems, security anomalies, and understanding protocol details. It is not an IDS but allows in-depth packet investigation. The GUI has key sections like the toolbar, display filter bar, recent files, capture filter, interfaces, and status bar. Loading PCAP files reveals detailed packet information across panes: list, details, and bytes. Packet coloring helps quickly identify anomalies and protocols, with options for temporary and permanent rules.

Wireshark can capture live traffic using the blue shark button, stop with the red button, and restart with the green button. It can merge multiple PCAP files and provides detailed file information through the

"Statistics" menu. Packet dissection reveals detailed protocol information across OSI model layers, aiding in thorough analysis. Wireshark assigns unique numbers to packets, simplifying navigation and investigation. The "Go" menu allows for specific packet navigation, while the "Find Packet" feature supports content-based searches using various input types.

Marking packets and adding comments help analysts focus on significant packets and share insights. Exporting packets and objects allows analysts to isolate suspicious data for detailed investigation. The "Time Display Format" menu offers better timeline views, and the "Expert Info" feature suggests protocol anomalies and issues. Wireshark's packet filtering engine has capture and display filters, enabling targeted traffic analysis.

Display filters can be applied directly from packet details, and conversation filters focus on related packets. Colourising conversations highlights related packets without filtering them out. The "Prepare as Filter" option creates filters without applying them immediately. Analysts can add columns to the packet list for specific values. Following streams helps reconstruct application-level data, revealing detailed communication between clients and servers.

Important Takeaways:

Wireshark is a powerful network traffic analyzer used for troubleshooting network problems, detecting security anomalies, and understanding protocol details. Its GUI features tools for filtering, sorting, and investigating traffic, and it allows for loading and detailed examination of PCAP files. Packet coloring and filtering help quickly identify and analyze specific traffic patterns and anomalies. Wireshark also supports live traffic capture, merging multiple PCAP files, and exporting specific packets for further analysis. Additionally, its ability to follow protocol streams and reconstruct application-level data makes it invaluable for in-depth network investigations

Entry 7

Room Name: Wireshark 101

Date Completed:
Notes During the Room:

Important Takeaways:

Entry 8

Room Name: Windows Fundamentals 1

Date Completed: 8/9/24
Notes During the Room:

The Windows operating system has evolved significantly since its inception in 1985. Initially, Windows XP was widely used and had a long run before being phased out. Its successor, Windows Vista, represented a complete overhaul but was met with criticism and quickly replaced. Windows 7 emerged as a popular choice, addressing many of Vista's shortcomings, though it also faced an end-of-support deadline. Following Windows 7, Windows 8.x was introduced but had limited success, leading to the current version, Windows 10, which is available in Home and Pro editions. As of October 2021, Windows 11 is the latest operating system for end-users, while Windows Server 2019 is the current version for server environments.

The Windows desktop, or graphical user interface (GUI), is where users interact with the system. It includes the desktop area, which holds shortcuts and allows for customization. The Start Menu, accessed via the Windows logo, provides quick access to apps, settings, and power options. The Taskbar displays open applications and can be tailored to the user's preferences, while the Notification Area, located at the bottom right, shows system icons and notifications.

Windows uses the NTFS (New Technology File System) for modern installations, which supports large files, permissions, compression, and encryption. NTFS also features Alternate Data Streams (ADS), which can be used both legitimately and maliciously. Older file systems like FAT and FAT32 are still found in portable devices but are not commonly used on personal computers or servers.

System management involves critical folders such as `System32` and `C:\Windows`, which contain essential files. User accounts come in two types: Administrator and Standard User. Administrators have broader privileges to make system changes, while Standard Users are more restricted. User Account Control (UAC), introduced in Windows Vista, helps mitigate the risk of malware by requiring confirmation for actions needing elevated privileges.

System settings can be managed through the Settings Menu, which became the primary interface with Windows 8, and the Control Panel, which remains for more complex configurations. The Task Manager offers insights into running applications and system performance, allowing users to monitor and manage system resources effectively.

Important Takeaways:
Windows has evolved from XP to Windows 11, improving usability and security with each version. The desktop interface includes customizable elements like the Start Menu and Taskbar, while NTFS provides advanced file system features. User accounts are either Administrators or Standard Users, with User Account Control (UAC) enhancing security. System settings can be managed via the Settings Menu or Control Panel, and Task Manager helps monitor system performance.

Entry 9

Room Name: Windows Fundamentals 2

Date Completed: 8/9/24
Notes During the Room:

The System Configuration Utility (MSConfig) is designed for advanced troubleshooting, focusing on diagnosing startup issues. It consists of five tabs: General, Boot, Services, Startup, and Tools. To access MSConfig, you need local administrator rights. The General tab allows you to select startup options such as Normal, Diagnostic, or Selective. The Boot tab lets you define boot options for the operating system, while the Services tab lists all system services regardless of their state. The Startup tab is managed through Task Manager rather than MSConfig, which is not intended for startup management. The Tools tab provides access to various system utilities like User Account Control (UAC) settings and Computer Management.

The Computer Management Utility includes System Tools, such as Task Scheduler for automating tasks and Event Viewer for viewing system events. The Storage section features Disk Management for performing advanced storage tasks. Services and Applications allow for more detailed management of services, including WMI Control for Windows Management Instrumentation. The System Information (msinfo32) tool offers comprehensive details about hardware, system components, and software environment, divided into Hardware Resources, Components, and Software Environment sections.

Resource Monitor (resmon) provides in-depth information on CPU, memory, disk, and network usage, including advanced filtering and process analysis. The Command Prompt (cmd) allows for interaction via text commands, with useful commands like `hostname`, `whoami`, `ipconfig`, and `netstat`, and includes help manuals accessible with `/help` or `/?`. Lastly, the Windows Registry is a critical hierarchical database for system configuration, user profiles, and hardware settings, and can be accessed or edited using the Registry Editor (`regedit`), though it is recommended for advanced users.

Important Takeaways:
The System Configuration Utility (MSConfig) is essential for diagnosing startup issues, offering tabs for startup options, boot settings, services, and various tools. Key utilities include Task Scheduler for automating tasks, Event Viewer for system logs, and Resource Monitor for detailed system performance analysis. The Command Prompt allows for executing and managing system commands, while the Windows Registry contains crucial system configuration information, accessible via the Registry Editor. For startup management, Task Manager is preferred over MSConfig.

Entry 10

Room Name: Windows Fundamentals 3

Date Completed: 8/9/24
Notes During the Room:

Windows Update is a Microsoft service that provides security updates, feature enhancements, and patches for Windows and other Microsoft products, such as Microsoft Defender. Updates are generally released on the 2nd Tuesday of each month, known as Patch Tuesday, but critical updates may be pushed out sooner if necessary. Access Windows Update through the Settings menu or via the Run dialog with the command `control /name Microsoft.WindowsUpdate`.

Windows Security, accessible from Settings, manages protective tools for your device, including Virus & Threat Protection, Firewall & Network Protection, App & Browser Control, and Device Security. Virus & Threat Protection includes options for scans, settings, and updates, with features like real-time protection and cloud-delivered protection. Firewalls control network traffic, with profiles for Domain, Private, and Public networks. The SmartScreen feature guards against phishing and malware, while Exploit Protection and Core Isolation defend against attacks and code injection.

BitLocker, a data protection feature, offers encryption to secure data on devices, particularly when used with a Trusted Platform Module (TPM). The Volume Shadow Copy Service (VSS) allows for system restore points and backups, though it is important to secure these backups from malware threats by maintaining offline or off-site copies.

Important Takeaways:
Windows Update provides essential security updates and patches, typically released on Patch Tuesday, with critical updates pushed out as needed. Windows Security encompasses several protection features, including Virus & Threat Protection, firewall settings, and SmartScreen to safeguard against threats. BitLocker offers encryption to protect data, especially when combined with a TPM. The Volume Shadow Copy Service enables system restore and backups, but these should be secured against malware by keeping backups offline or off-site.

Entry 11

Room Name: Windows Forensics 1

Date Completed:
Notes During the Room:

Computer forensics is a vital subset of digital forensics, focusing on extracting and analyzing data from computer systems to support legal and corporate investigations. This field is crucial for resolving criminal cases and uncovering digital evidence. An illustrative example is the BTK serial killer case, where forensic analysis of a floppy disk led to the perpetrator's identification and arrest.

Windows, being the predominant desktop OS, is a central focus in forensic analysis. Key forensic tasks involve examining the Windows Registry, which stores critical data about system configurations and user activities. Artifacts, such as traces of user actions and system modifications, are crucial for reconstructing past events. Forensic tools like KAPE, Autopsy, and FTK Imager are used to acquire and analyze registry data from both live systems and disk images.

The Windows Registry, organized into five root keys and various hives, contains extensive information about system and user activities. Analysis involves examining keys related to system information, control sets, network interfaces, and recent files. Additionally, tools like Registry Viewer, Registry Explorer, and RegRipper assist in interpreting registry data, providing insights into user behavior and system configurations, including details about connected USB devices and other removable media

Important Takeaways:
Computer forensics involves analyzing data from computer systems to support investigations and legal cases, exemplified by the BTK serial killer case where floppy disk analysis led to the perpetrator's capture. Windows forensics focuses on examining the Windows Registry and related artifacts to reconstruct user activities and system changes. Tools like KAPE, Autopsy, and FTK Imager are essential for acquiring and analyzing registry data, which helps uncover crucial information about user behavior and system configurations.

Entry 12

Room Name: Windows Forensics 2

Date Completed:
Notes During the Room:

A storage device in a computer system, such as a hard disk drive or a USB device, is essentially a collection of bits. To transform these bits into meaningful information, they must be organized. Computer scientists and engineers have developed various file systems to standardize this organization, enabling efficient data retrieval and interpretation.

One such file system is the File Allocation Table (FAT), which has been a default for Microsoft Operating Systems since the late 1970s. The FAT system creates a table that indexes the locations of bits allocated to different files. This indexing allows for straightforward retrieval of data from storage devices.

The FAT file system is based on several key data structures. Clusters, which are the basic storage units, group together bits of information for each file. Directories store file identification details such as file name, starting cluster, and filename length. The File Allocation Table itself functions as a linked list that tracks the status and location of each cluster, ensuring proper file management on the disk.

FAT has evolved through several versions to accommodate increasing storage needs. FAT12, FAT16, and FAT32 represent different stages in this evolution. FAT12 uses 12-bit cluster addressing, supporting up to 4,096 clusters. FAT16 expanded this to 16-bit addressing, allowing up to 65,536 clusters. FAT32 introduced 28-bit addressing, which theoretically supports up to 268,435,456 clusters, though not all clusters are usable due to administrative overhead. FAT32's maximum volume size is 2TB, but Windows limits formatting to 32GB.

Important Takeaways:
File systems like FAT and NTFS organize data on storage devices, with FAT using tables to manage clusters and directories and NTFS offering advanced features like journaling and access controls. FAT12, FAT16, and FAT32 each support different cluster sizes and volume sizes, while exFAT addresses larger file and volume sizes. NTFS includes robust features for security and recovery, including the Master File Table and Volume Shadow Copies, which are crucial for forensic analysis, along with tools like MFTECmd and PECmd for detailed file and prefetch analysis

Entry 13

Room Name: Intro to Log Analysis

Date Completed: 8-10-2024
Notes During the Room:

When analyzing logs, logs are crucial for gaining insights into system activities, troubleshooting issues, and detecting security incidents. Logs, which are time-sequenced messages recording events, are analyzed to understand system interactions across a network. They provide details such as timestamps, sources, and severity levels (Informational, Warning, Error, Critical).

A timeline of logged events is fundamental for incident response, as it helps in reconstructing security incidents and understanding attacker's tactics. Tools like Plaso automate the creation of consolidated timelines from multiple log sources, while visualization tools like Kibana and Splunk aid in interpreting log data through graphical representations. Automated analysis tools, such as XPLG and SolarWinds Loggly, utilize AI and machine learning for pattern recognition but can be costly and may miss new threats. Manual analysis, using commands like `cat`, `less`, `tail`, `wc`, `cut`, `sort`, `uniq`, `sed`, `awk`, and `grep`, is essential for thorough investigation and reducing false positives. Regular expressions are invaluable for pattern matching and log parsing, and tools like Logstash and its Grok plugin help in structuring unstructured log data.

CyberChef, known as the "Cyber Swiss Army Knife," offers numerous operations for encoding, decoding, and analyzing data. It can be used to parse logs and extract useful information, leveraging regular expressions for precise searches. Understanding these tools and techniques is crucial for effective log analysis, whether through automated systems or manual methods.

Sigma is an open-source tool that describes log events in a structured format using YAML syntax. It helps in detecting events, creating SIEM searches, and identifying threats. Yara, another pattern-matching tool, uses YAML formatting to identify patterns based on binary and textual data. While Yara is commonly used in malware analysis, it is also effective for log analysis.

Important Takeaways:
Effective log analysis combines automated tools and manual methods to understand and investigate system activities. Tools like Sigma and Yara assist in pattern matching and threat detection, while CyberChef and regular expressions help parse and process log data. Understanding both the timeline of events and the key commands for log examination is essential for thorough analysis and accurate incident response.

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: