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:
The Linux Fundamentals module covers essential skills such as using terminal 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:
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: