TryHackMe Journal - Anthony Awoyele

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:
Notes During the Room:
Task 1 - Introduction:

- Linux is a popular operating system used in various devices and systems worldwide.
- This room covers some Linux history and helps start the journey as a Linux user.
- Mentions essential commands to interact with the file system and understand users and groups in Linux.

Task 2 - A bit of background on Linux:

- Linux is more intimidating than Windows but has its advantages.
- Linux powers websites, car entertainment systems, PoS systems, and critical infrastructures.
- There are many distributions (flavors) of Linux, such as Ubuntu and Debian, which are open-source and highly extensible.
- Ubuntu Server can run on systems with only 512MB of RAM.

Task 3 - Interacting with your first Linux machine:

- This room provides an Ubuntu Linux machine that can be interacted with in the browser.
- To start the machine, click the "Start Machine" button on the top-right of the task.
- A card will appear with the machine's information, including the IP address and expiry timer.
- Remember to "Terminate" the machine once done with the room.

Important Takeaways:

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: Linux Strength Training

Date Completed: July 29th, 2024
Notes During the Room:
I will return to the training to take notes. My initial goal was to enjoy the moment and immerse myself in figuring it out the first time around without any distractions. The second time around, i will take notes and try to recall what i learned the first time around.

Important Takeaways:

Entry 5

Room Name: Intro to Logs

Date Completed:
Notes During the Room:
Task 1 - Introduction:

- Logs are invaluable records of past events that provide essential insights for identifying and mitigating potential threats.
- Understanding logs is crucial for detecting patterns and threats, but manually examining vast amounts of log data can be challenging.
- Log analysis tools and methods streamline the processing and scrutiny of log data, facilitating prompt detection and response to potential incidents.

- This room covers the importance of logs, various types of logs, logging mechanisms, collection methods, and hands-on experience detecting and defeating adversaries through log analysis.

Task 2 - Expanding Perspectives: Logs as Evidence of Historical Activity:

- Logs provide a historical record of system activity, capturing user interactions, system errors, network connections, and changes to data or configurations.
- Log entries typically include a timestamp, the name of the system or application, the type of event, and additional details about the event.
- When log data is aggregated, analyzed, and cross-referenced with other sources, it becomes a powerful investigation tool, answering critical questions about an event (what, when, where, who, success, and result).
- Logs are instrumental in piecing together a complete picture of an event, enhancing understanding and the ability to respond effectively.

Task 3 - Types, Formats and Standards:

- Common log types include application, audit, security, server, system, network, database, and web server logs.
- Log formats define the structure and organization of data within a log file and can be categorized as semi-structured, structured, or unstructured.
- Semi-structured logs may contain structured and unstructured data (e.g., Syslog, Windows Event Log).
- Structured logs follow a strict and standardized format (e.g., CSV, JSON, W3C Extended Log Format, XML).
- Unstructured logs comprise free-form text and can be rich in context but challenging to parse systematically (e.g., NCSA Common Log Format, NCSA Combined Log Format).
- Log standards provide guidelines or specifications for generating, transmitting, and storing logs (e.g., CEE, OWASP Logging Cheat Sheet, Syslog Protocol, NIST SP 800-92).

Important Takeaways:

Entry 6

Room Name: Wireshark Basics

Date Completed: july 29th, 2024
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: