TryHackMe Journal - Rowan King

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

Room Name: Linux Fundamentals 1

Date Completed: 4/27/2024
Notes During the Room: The basics of Linux and the CLI

Introduced several commands;

Command	**Description**
echo	Output any text that we provide
whoami	Find out what user we're currently logged in as!
ls	listing
cd	change directory
cat	concatenate
pwd	print working directory
find	search for a specified file or folder
grep	search the contents of files for specific values that we are looking for

As well as Operators:

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:

Entry 2

Room Name: Linux Fundamentals 2

Date Completed: 4/27/2024
Notes During the Room:
Introduced remote login using the SSH command

SSH *	The syntax to use SSH is very simple. We only need to provide two things: 1. The IP address of the remote machine

	2. Correct credentials to a valid account to login with on the remote machine

Other Filesystem Commands

Command	**Full Name**	**Purpose**
touch	touch	Create file
mkdir	make directory	Create a folder
cp	copy	Copy a file or folder
mv	move	Move a file or folder
rm	remove	Remove a file or folder
file	file	Determine the type of a file

Covered common directories such as /ect, /var, /root, & /tmp

Important Takeaways:

Entry 3

Room Name: Linux Fundamentals 3

Date Completed: 4/27/2024
Notes During the Room:

Learned about nano and vim.

Learned about wget and its variables;

Variable	**Value**
The IP address of the remote system	192.168.1.30
User on the remote system	ubuntu
Name of the file on the local system	important.txt
Name that we wish to store the file as on the remote system	transferred.txt

Learned about running and killing processes

Learned about cron files used to automate tasks;

Value	**Description**
MIN	What minute to execute at
HOUR	What hour to execute at
DOM	What day of the month to execute at
MON	What month of the year to execute at
DOW	What day of the week to execute at
CMD	The actual command that will be executed.

Learned about adding and removing repositories

Learned how to pull system logs

Important Takeaways:

Entry 4

Room Name: Linux Strength Training

Date Completed: 4/27/2024
Notes During the Room:
Learned about nano and vim.

Learned about wget and its variables;

Variable	**Value**
The IP address of the remote system	192.168.1.30
User on the remote system	ubuntu
Name of the file on the local system	important.txt
Name that we wish to store the file as on the remote system	transferred.txt

Learned about running and killing processes

Learned about cron files used to automate tasks;

Value	**Description**
MIN	What minute to execute at

HOUR	What hour to execute at
DOM	What day of the month to execute at
MON	What month of the year to execute at
DOW	What day of the week to execute at
CMD	The actual command that will be executed.

Learned about adding and removing repositories

Learned how to pull system logs

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: