TryHackMe Journal - [Name]

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: 04/28/2024
Notes During the Room:

- Linux is lightweight and used in many systems such as websites, POS systems, traffic light controllers, and car control panels.
- Linux is an umbrella term.
- Ubuntu and Debian are common distributions of Linux

Name of Commands	**Description**
echo	Output any text that we provide
whoami	Currently logged in user
ls	Provides a list of whats in the directory or file you are in
cd	Changes directory
cat	Concatenate, seeing the contents of text files
pwd	Print working directory
find	Look for specific files
grep	To search the contents of files for specific values

Symbol/Operator	**Description**
&	Allows you to run commands in the background of your terminal.
&&	Allows you to combine multiple commands together in one line of your terminal; make a list of commands to follow.
>	This is a redirector which means you can take the output from a command and direct it elsewhere.
>>	Does the same function as the > command but appends the output rather than replacing it.
*	Wildcard, search for anything that has the speciffied

Important Takeaways:

- Linux is widely used throught various industries.
- *ls*, *cd*, and *pwd* are common commands.

Entry 2

Room Name: Linux Fundamentals 2

Date Completed: 04/28/2024
Notes During the Room:

- What is the SSH? The common means of connecting to and interacting with the command line of a remote Linux machine.
- How does SSH work? A protocol between devices in an encrypted form.
- SSH is short for secure shell
- drwx/-rwx meaning *d* for directory - meaning no directory *r* for read *w* for write and *x* for execute.
- Arguments are identified by a hyphen and a certain keyword known as flags or switches.

Command	Full Name	Purpose
touch	touch	Create file
mkdir	make directory	Create 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
ls -a		Shows hidden files
Ls -l		Shows 10 lines
su	Substitute user	Temporary root privilage
man	manual	Read documentation for

Common root directories

Name	**Full name**	**Description**
/etc	etcetera	Store system files that are used by your OS
/var	Variable data	Stores frequently accessed data
/root	root	Home for root system
/tmp	temporary	Sort term storage, until system restart

Important Takeaways:

- The function of SSH.
- How to move and examine things within the command line

Entry 3

Room Name: Linux Fundamentals 3

Date Completed: 04/29/2024
Notes During the Room:

- A few features of nano are that you can search for text, there's copying and pasting, jumping to a specific line number, and finding what number you are on.
- Ctrl is represented by ^ on Linux.
- VIM is more likely to be installed over nano.
- Ubuntu machines come pre-packaged with python3.
- Signals that we can send to a process when its killed; SIGTERM, SIGKILL, SIGSTOP
- Options for systemctl: start, stop, enable, disable
- Crontabs is one of the processes that is started at boot

Terminal text editors

Command	**Description**	**How to execute**
nano	To create or edit a file	nano filename
VIM	Alternative to nano, more advanced text editor	

General/Useful Utilities

Command	**Description**	**How to execute**
wget	Allows you to download files from the web via HTTP	`wget`
scp	Secure copy	Source destination
curl		
python3	Starting a webserver	python3 -m http.server
ps	Provides a list of running processes	ps
aux	To see the processes run by other users and those that dont run from a session	ps aux
top	Gives you real-time statistics	top

	about the processes running on your system that refreshses every 10 seconds	
kill	Terminate a process	Kill associated PID
systemd	One of the first processes that starts once a system boots	systemd
systemctl	Allows you to interact with the systemd	systemctl [option] [service]
Ctrl + z	To background a process	Ctrl + z
fg	Bring to the forground	fg
crontab -e	To edit the users crontab file	
add-apt-repository	Adds additional repositories	
apt	Can use to install software onto Ubuntu system	apt
dpkg	Type of package installler	dpkg
apt update	Update the apt	
apt remove	remove	apt remove [software-name-here]

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 actuall command that will be executed.
*	Doesn’t matter when its executed

Important Takeaways:

- Processes can run in the background and in the foreground.

- Overall all the notes taken in this section are important to continuously review.

Entry 4

Room Name: Linux Strength Training

Date Completed:
Notes During the Room:

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: