Assignment# 1
Final Grade: 7% (100 points)

Fundamental Linux Commands for Cybersecurity

Because this is largely a hands-on course, it is essential that you learn many of the fundamental Linux commands, an important skill for any good security practitioner.

Students are also encouraged to study YouTube videos to prepare for this lab. You will be responsible for correctly configuring your VM host to support your guest OS installations.

Recommended Specifications: - CPU: Quad-core CPU - RAM: 8GB or More - Free Storage: 40GB or more. If you do not meet these requirements but your computer is close enough, you can still complete the work; however, it may become slow sometimes.

Step 1: Enable Virtualization

Before creating virtual machines, you need to know if your computer can virtualize. There are a couple of steps you need to follow to find out the answer to this question:

Mac OS

For those using MacOS, if you have a recent Apple computer (**M1 M2 M3 chip**), you will not be able to use VirtualBox; there is another hypervisor you can use called UTM (feel free to use any other hypervisor of your choice), but I have not been able to test all of them. I have tested Ubuntu on UTM, and it works fine. You can watch and follow this YouTube **tutorial** (recommended) or this tutorial.

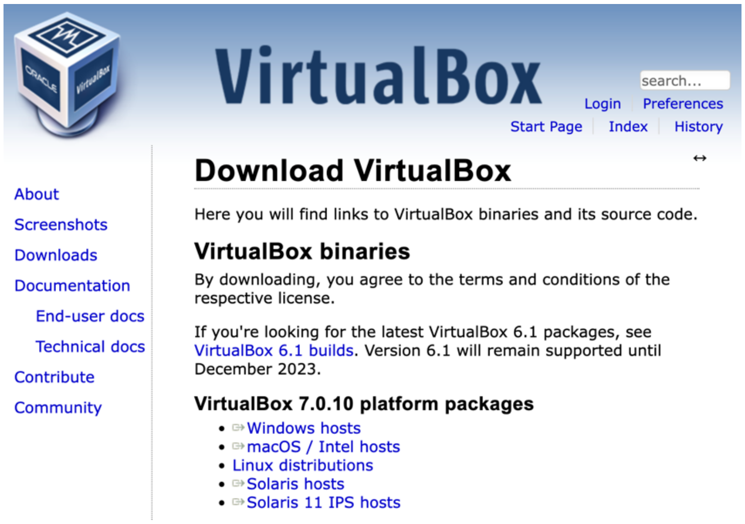
If you have a **Mac with an Intel chip**, you can use VirtualBox (recommended). Just make sure your Mac has enough resources to run virtual machines. For Intel Macs, virtualization is already enabled.

Windows OS

Important: Before you start, check if virtualization is enabled. Follow this guide to know if your computer has virtualization enabled; if not, use the same guide to learn how to enable it.

Step 2: Download and Install Virtual Box/UTM or any hypervisor.

- Virtualbox Download Page
  (There is a beta version of VirtualBox for Mac M1/M2 chip. However, it is not a stable version, not recommended)



Download VirtualBox

Here you will find links to VirtualBox binaries and its source code.

VirtualBox binaries

By downloading, you agree to the terms and conditions of the respective license.

If you're looking for the latest VirtualBox 6.1 packages, see VirtualBox 6.1 builds. Version 6.1 will remain supported until December 2023.

VirtualBox 7.0.10 platform packages

- Windows hosts
- macOS / Intel hosts
- Linux distributions
- Solaris hosts
- Solaris 11 IPS hosts

Make sure to install VirtualBox on your host computer. For Windows, follow this video. For macOS (Intel Chip), follow this video. For Mac (M1/M2), UTM installation is provided in the video recommended above. Once you have installed VirtualBox, create a virtual machine that meets these specifications:

- OS: Ubuntu or Ubuntu Server (Recommended) ISO URL
- HDD: 40 GB
- RAM: 2GB
- Video: 64 MB or Higher
- Audio Controller: Disabled (audio won't be needed)
- CPU: 2 Cores
- **Hostname:** cyber101
- **User:** student name (use your Canvas username)
- **Password:** cyber101
- Shared Clipboard: Enabled - Bidirectional
- Drag n' Drop: Enabled – Bidirectional

Install Ubuntu OS on your VirtualBox/UTM. Look for tutorials on YouTube for additional help.

Post Installation: Install Guest Additions for better performance

- Install the guest additions for VirtualBox.
- Run this command: **sudo apt install build-essential linux-headers-$(uname -r) -y**
- Use this **video** to install guest additions (Windows and Mac with Intel).
- For Mac M1/M2 chip, if you followed the YouTube video above, nothing else is required. Additional information is on this website: https://docs.getutm.app/guest-support/linux/

Step 3: Please learn and tinker with the commands below and answer the questions below. Many commands will require flags. You would be using these commands as a security practitioner so get used to these commands.

Commands: ls, rm, mkdir, rmdir, cd, wget, pwd, ln, sudo, chmod, umask, ping, cut, sort, which, grep, whereis, finger, w, who, whoami, last, file, strings, top, ps, nice, nohup, kill, signal, more, less, ifconfig, arp, nslookup, cat, uname, history, netstat, curl, ifconfig, traceroute, shred, dig, man, lsof, whois, crontab, nc, uniq, id, groups, df, du, dd, openssl, tar, clear, touch

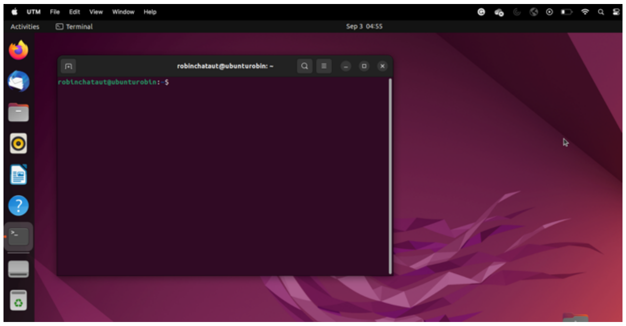
In addition, please read "The command-line, for cybersec" by Rob Graham:
https://blog.erratasec.com/2017/01/the-command-line-for-cybersec.html

Special Note

This is a demo lab for your learning. You will be making more virtual machines in the future.

Answer the questions below. Do not delete questions. Write your answer below the questions.

1. (20 Points) Include a screenshot of your VM installation with your submission. Sample below.



```
robinchataut@ubunturobin:~$
```

For each of the questions below (2–15), include a screenshot showing an example use of the command:

2. (5 Points) How would you find the path (i.e., location) to the '**gcc**' command?
3. (5 Points) What command can you use to find out your IP address and MAC address?

4. (5 Points) What command can you use to show all the processes that are running on the system?
5. (5 Points) What command can you use to get more details about running processes listening on ports?
6. (5 Points) Assume you found a file named hacked.pdf. What command could you use to find out what type of file this was?
7. (5 Points) What command can you use to find the IP address-to-MAC address mappings for systems on the local network?
8. (5 Points) What command can you use to delete a file securely?
9. (5 Points) What command can you use to see if you are a computer administrator or superuser?
10. (5 Points) What command can you use to see the list of previous commands you have entered on the command line?
11. (5 Points) Which Linux command allows to display information about files and directories contained within the current working directory?
12. (5 Points) What is the function of the Linux chmod command?
13. (5 Points) A Linux command that temporarily modifies security privileges to allow execution of a single command that requires root access permissions is called:
14. (5 Points) A Linux command-line command that enables searching files for lines containing a match to a given text pattern is known as?
15. (5 Points) Which Linux command-line utility provides a functionality similar to Windows Task Manager?
16. (10 Points) Reflecting on the fundamental concepts of cybersecurity, which area—confidentiality, integrity, or availability—do you think presents the greatest challenge for organizations today, and why? Provide a real-world example or scenario to support your perspective. Cite your sources. Minimum 150 words.

Submission Instructions:

- Submit filled pdf of this document (with all the answers). Do not delete the questions or change the order of the questions. You can download and edit this document.
- Submit electronically through D2L.
- Email or hardcopy submissions will not be accepted.