METCS695 Enterprise Cybersecurity

Lab 1 Introduction to Kali Linux and Basic CLI Commands

Introduction

Brief description (purpose and overview)

The objective of this lab is to prepare the student with Kali Linux virtual machine (VM) we will use in the semester and get familiar with it as well as basic CLI commands.

Learning Objectives

After finishing this lab, students shall be able to:

1. Know basic usage of Kali Linux.
2. Master basic CLI commands

Prerequisite knowledge

- Have very basic knowledge of Linux.
- Have a basic understanding of command line interface (CLI) and be comfortable using it.

Lab Setup Requirements

The following computer resources are recommended to install and run the Virtual Machine Manager (VMM) and VM instances:

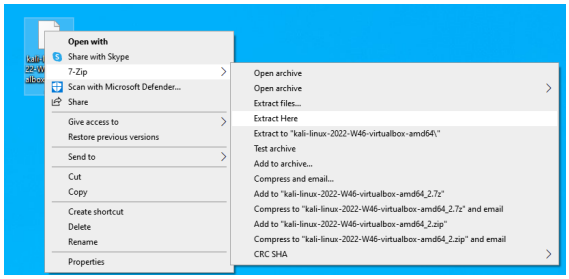
- 8 GB RAM
- 40 GB of free hard disk space
- 2GHz processor with four or more physical cores
- Windows 10 or later, MacOS 10.11 or later, Linux

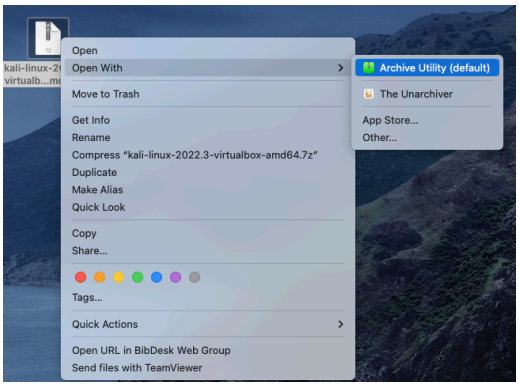
We recommend using VirtualBox. Students have successfully used other virtualization packages, for example, VMWare as well. You can use any other VMMs as long as they work.

Part 1: Set up VirtualBox and Explore Kali

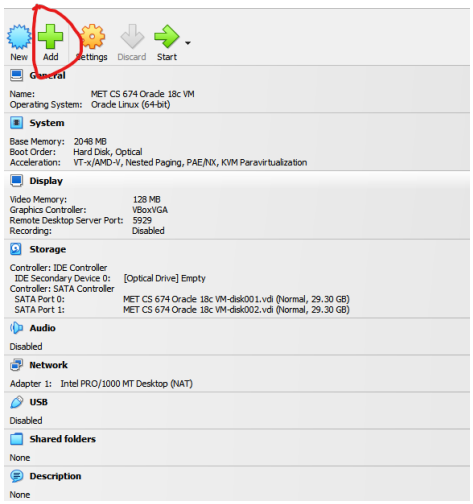
Detailed instructions

1. VirtualBox can be downloaded at:
   https://www.virtualbox.org/wiki/Downloads
   You want to choose the correct VirtualBox package to download according to your operating system.
2. Install VirtualBox on your machine. You can accept all default settings presented during the installation process.
3. Download the Kali VirtualBox image (kali-linux-2022.3-virtualbox-amd64.7z) from (https://drive.google.com/file/d/1uQKQK48-V3vGpl2lPv8h1vMbffL_w3Zm/view?usp=sharing).
4. For Windows users, you can use 7-Zip (https://www.7-zip.org/) to extract the downloaded archive. For Mac users, the pre-installed Archive Utility to extract. Make sure that your computer has enough disk space. Once the downloaded file is uncompressed, it is about 12.3GB.

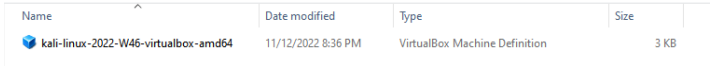




5. (1) For Windows users, open VirtualBox, and click ‘Add’

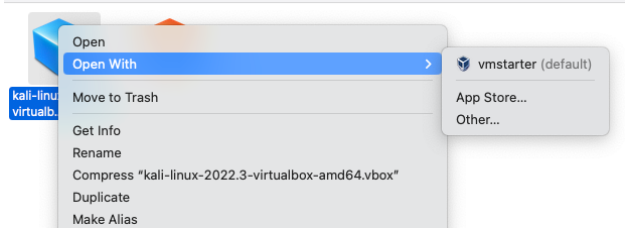


Navigate to the folder that you uncompressed in Step 4, choose the file below, and click ‘open’



You will see Kali Linux is loaded into your VirtualBox. Double click it to start Kali.

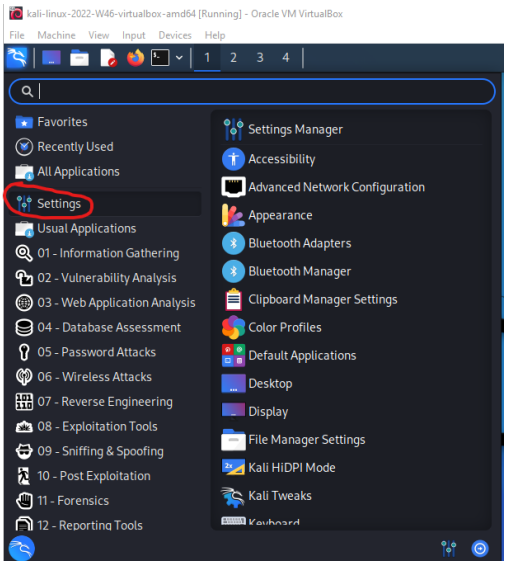
(2) For Mac users, go to the folder uncompressed from Step 4. It is named ‘kali-linux-2022.3-virtualbox-amd64’. Right click the file ‘kali-linux-2022.3-virtualbox-amd64.vbox’, choose open with, and click vmstarter to open it.

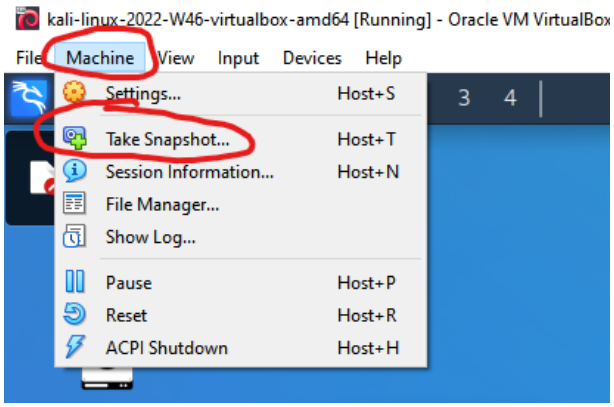


You will see Kali Linux is loaded into your VirtualBox. Double click it to start Kali.

6. Once the Kali Linux virtual machine is started, you should arrive at this connection screen, the default user is: ID: kali PASW: kali Then log in.

7. When logged in you can modify the resolution, keyboard and other settings in Settings inside the “Kali” menu. Take a snapshot of your Kali Linux. DO NOT APPLY ANY UPGRADE. If you see a window saying new packages are available and ask if you want to apply the upgrade, just cancel.





8. Below Settings there are all the preinstalled tools on kali Linux classified depending on their field of use.
9. Next to the “Kali” menu you will find a shortcut for the terminal. You will need to use the terminal to run the CLI commands asked in Part 2.

Questions:

1. What is a virtual machine? Why use a virtual machine?
2. What is a snapshot of a virtual machine?
3. What is Kali Linux? (What distribution, based OS, open source?). Why using it instead of a basic Linux distribution?
4. Navigate the Kali menu and find the following tools:
   - Nmap
   - Burpsuite
   - SQLMap
   - Mimikatz
   - Aircrack-ng
   - John
   - Wireshark

- SET (Social Engineering Toolkit)

Show which category these tools are in and give a one or two sentence summary about these tools.

Part 2: Basic Linux Command

Detailed instructions

Open the terminal. This is where you will work on for the following tasks. Take a screenshot of your command and the output for each step below.

1. *pwd*: to know which directory you are currently in (Just type *pwd* in the terminal and then hit enter. Everything you typed is after $ in the terminal. Note that you will see kali@kali instead of chival@kali on your terminal).

```
chival@kali:~$ pwd
```

2. *ls*: list the files/directories that are in your current directory.

```
chival@kali:~$ ls
```

3. *mkdir*: create a directory. Run the command below to create a directory with the name of lab1

```
chival@kali:~$ mkdir lab1
```

4. *cd*: get into a directory. Run the commands below to get into the directory of lab1 and show your current directory again. Compare it with the output of Step 1.

```
chival@kali:~$ cd lab1
chival@kali:~/lab1$ pwd
```

5. *touch*: create a new file or update the access and modification time of an existing file. Run the command below to create a file with the name of new.txt.

```
chival@kali:~/lab1$ touch new.txt
```

6. *sudo*: stands for superuser do. If you want to run any command with administrative or root privilege, you can add sudo ahead of the command. Using sudo requires you input your password. Run the commands below and compare the outputs.

```
chival@kali:~/lab1$ touch /etc/shadow
chival@kali:~/lab1$ sudo touch /etc/shadow
```

7. *apt-get*: install packages. This requires root privilege. The first command below updates your repository and the second command installs a GUI editor gedit. Running the third command, you will see the file opened (empty). Type in *CS695 lab1,* then save and close the file.

```
chival@kali:~/lab1$ sudo apt-get update
chival@kali:~/lab1$ sudo apt-get install gedit
chival@kali:~/lab1$ gedit new.txt
```

8. *cat*: display the contents of a file. Run the command below to show the content of the file new.txt.

```
chival@kali:~/lab1$ cat new.txt
```

9. *cp*: cope files. It takes two arguments: the first is the file to be copied and the second is where to copy to. Run the first command to make a backup copy of the file new.txt. Run the second command to show the files in the current directory.

```
chival@kali:~/lab1$ cp new.txt backup.txt
chival@kali:~/lab1$ ls
```

10. *mv*: move files or rename files. It also takes two arguments, the same as *cp*. Run the first command to move the file backup.txt to your Desktop. Run the following two commands to check where backup.txt is after moving. ~/ represents your home directory.

```
chival@kali:~/lab1$ mv backup.txt ~/Desktop
chival@kali:~/lab1$ ls
chival@kali:~/lab1$ ls ~/Desktop/
```

11. *rm*: delete files or directories. Run the first command to delete backup.txt in your Desktop directory, and run the second command to check if it is deleted.

```
chival@kali:~/lab1$ rm ~/Desktop/backup.txt
chival@kali:~/lab1$ ls ~/Desktop
```

12. *man*: shows the manual page of a command. Run the command below to know more details of the command *ls*. Type q to quit from the manual page to the terminal.

```
chival@kali:~/lab1$ man ls
```

13. *useradd:* add a new user. Run the command below to add a new user cs695.

```
chival@kali:~/lab1$ sudo useradd cs695
```

14. *passwd*: change the password of a user. Run the command below to setup password for cs695.

```
chival@kali:~/lab1$ sudo passwd cs695
```

15. *userdel*: delete a user. Run the command below to delete the user cs695.

```
chival@kali:~/lab1$ sudo userdel cs695
```

16. *Zip/unzip:* use zip to compress files into a zip archive, and unzip to extract files from a zip archive. Run the first command to create a zip archive called new.zip. Run the second command to delete the new.txt file. Run the last command to extract the files from the zip archive.

```
chival@kali:~/lab1$ zip -r new.zip new.txt
chival@kali:~/lab1$ rm new.txt
chival@kali:~/lab1$ unzip new.zip
```

17. Tar: compress and uncompress different types of tar archives like .tar, .tar.gz, .tar.bz2, etc. It works on the basis of the arguments given to it. Run the first command to create a tar archive. Run the second command to delete the new.txt file. Run the last command to uncompress the tar archive.

```
chival@kali:~/lab1$ tar -cvf new.tar.gz new.txt
chival@kali:~/lab1$ rm new.txt
chival@kali:~/lab1$ tar -xvf new.tar.gz
```

18. uname: get the OS version information.

```
chival@kali:~$ uname -a
```

Questions:

Using basic CLI:

a. Find the /bin and /sbin folder and show their contents (provide a screenshot of the used commands). Explain what you have found in the /bin and /sbin folder and the difference between these two folders.

b. Get the virtual machine network information using *ifconfig* (provide a screenshot of the used command). What is your IP address? Are you connected to the public network?

c. Get process information using the *ps* command. What are the 4 information printed by the *ps* command?

d. Get Linux processes information using the *top* command (type q to return to the terminal from the output of the *top* command). What is the information in the header of the result of the command?

e. What is the difference between the *ps* and the *top* commands?

Deliverables

Please submit the lab report in a single document named *CS695-LAB1-yourlastname*. Please submit a DOC document and/or a PDF file in case the format is not compatible across the platform. The lab report should include:

1. Title, author(s)
2. Table of Content
3. The detailed steps and results using text description and/or screenshots that answer the above questions and demonstrate your lab progress.
4. A summary of your own reflection of the lab exercise, such as:
   a. What is the purpose of the lab in your own words?
   b. What do you learn? Do you achieve the objectives?
   c. Is this lab hard or easy? Are the lab instructions clear?
   d. Any other feedback?