**Lab Report Template**

Professor's Name: Ingrid Gaviria

Course: ITT-340, Cybersecurity and Ethical Hacking, Topic 1.

Student Name: James Darling

Date: 10/30/2024

# **Title:** Secure Testing Environment: Create a Virtual Cybersecurity Sand Box

# **Overview**

# To explain the basic principles of virtualization; to contrast and evaluate the different virtualization designs; List and explain the different interfaces that exist between the hypervisors, virtual machines (VMs), hardware, networking, storage, administration tools, code execution and emulation, and external environments.

# **Details**

# First, we install Kali onto VirtualBox by opening up the program and selecting new > Name Kali ITT-340A screenshot of a computer Description automatically generated

# For type and version > Linux > Debian (64-bit) > NextA screenshot of a computer Description automatically generated

Set at 2gb > Next

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

Start Kali ITT-340 and select your Kali ISO A screenshot of a computer

Description automatically generatedSelect Graphical installation >Language > USA screenshot of a computer

Description automatically generated

Name your systemA screenshot of a computer

Description automatically generated

Finish installationA screenshot of a computer

Description automatically generated

Download Metasploitable 1 and 2 and create new vms A screenshot of a computer

Description automatically generated

Extract filesA screenshot of a computer

Description automatically generated

Create new VMs for both 1 & 2A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

AddA screenshot of a computer

Description automatically generated

Log onto both 1 & 2 with the credentials msfadmin for user and password

# **Summary**

The use of virtual environments can be advantageous not only for the organization attempting to bring in safe cash on equipment but also for the digital protection part of the IT businesses, as they provide a secure environment for testing updates, hacking, and new arrangements on an operating system.

A significant quantity of RAM should be accessible for both operating systems to use in order to lessen the possibility of sluggish operations when both the host and guest operating systems are running. The two operating systems will have a similar stockpiling unit in addition to a similar Slam. As a result, it is recommended practice to employ distributed storage for a significant percentage of the virtual work being done on the visitor operating system and to merely distribute the amount you will need on the fast device. Since the virtual machines operate on the host computer, it is likely that they share resources with it.

A great use of VMs Another is the benefits of creating previews and clones. Being able to save phases at their exact states to come back and study separate outcomes at each phase. When IT departments update their workstations, this is an essential tool. They build the updates and run them on a virtual machine (VM) to ensure that the workstations do not crash or have their security compromised, increasing the vulnerability. The fact that depictions can be employed for a long time with various clientele within the firm is another fantastic advantage. In the workplace, having a copy of an exposed operating system can save time and money. By ensuring that the sanctuary is properly configured with all the configurations required for the business to successfully restrict the security risk, creating many virtual machines (VMs) from a single VM layout can also lower human mistake rates.