Documentation for Lab Project 1.0 (Virtual Machine setup + Hacking Lab)

August 13th, 2025

What you’ll need:

* Oracle VirtualBox + extension pack
* Ubuntu 64-bit ISO (For practice in learning how to set up a VM)
* Kali-Linux (Our hacker VM)
* mrrobot.ova (Our vulnerable machine)

**READ BEFORE STARTING**: Before installing anything, make sure Hardware Virtualization feature is toggled in the OS Bios, which can be done by hitting the ‘Delete’ key rapidly as your OS is starting up (Could be also **F2, F12, Delete, or F14** depending on the motherboard model). You can also access it by going into Update and Security in the windows settings, then click ‘Recovery’ and then ‘Restart Now’ under Advanced Startup. Then click on UEFI settings, which will take you to the OS bios. While in the bios, go into CPU configuration and then advanced settings. It will look different depending on the OS, but the settings will be consistent. Hardware Virtualization toggled on allows the user to increase the amount of ‘CPUs’ that will be allocated to the guest Virtual Machine as it runs, granting it more shared resources from the host. If you have 12-16 ‘CPUs’, then setting it to 2 or 3 in the VM configuration settings will be sufficient, but it will vary depending on what OS is being set up in your Virtual Machine. This project is also VM name-sensitive, so during configurations that require typing the respective VM’s name, use its corresponding name that shows in VirtualBox!

[If you’re using an HDMI-to-Display cord from your monitor to your PC, you WILL encounter a black screen upon booting to the bios. Make sure it’s an HDMI-to-HDMI. Try to also turn off Windows’ fast boot if you want a slower boot to see specifically which key opens the BIOS.

Lastly, at some point in the lab example, Windows Defender **WILL** alert you of various malware and severe threats in your Windows Security notifications. Those items in the threat list will be names of various pen testing tools used by Kali Linux, as Windows Defender recognizes them as malware. They are harmless and do **NOT** pose any threat to your PC or VirtualBox labs, so do not panic if you notice a Windows Defender scan picking them up. Feel free to whitelist them so that Windows Defender does not flag them.]

* Install Oracle VirtualBox, keep default settings. Then install the expansion pack, which will grant the user greater control and additional configuration settings.
* Next, test the installation of an OS ISO. First, click “**New**”. This next menu lets you customize how you want your VM in terms of specifications. We’ll start with Ubuntu 64-bit, so select the Ubuntu option from the OS drop-down arrow. Keep default settings, but it is highly recommended to check the hardware tab. If the RAM is not at **2 GB** and storage memory is not at least **10 GB**, then set them as such. If needed, you may increase the CPU allocation from your host OS for your guest OS if you want better performance or more resources to use for the scope of your activities. Make sure to avoid over-allocating resources! This is marked in red on the slider.
* Now we will set up the next VM for Kali-Linux. Click “New” just like before and configure it as a Linux-based VM with **20 GB** of memory and **2 ‘CPU’s** for the sake of stability, performance, and efficiency. Click on Kali Linux and select the Kali-Linux 64-bit ISO to mount. During the installation, retain the default settings, and make a corresponding username and password for logging in. Hold on to these!

A screenshot of a computer

AI-generated content may be incorrect.

* Make sure to use default settings for easy and basic installation. During the installation, you should use the entire disk for guided partitioning.
* Now download ‘**mrrobot.ova**’ from VulnHub and open it with VirtualBox. Windows Defender will recognize it as malicious, but the file itself is safe to use in VirtualBox.
* Go into the settings for both Kali Linux and mrrobot, and then click the Network tab. For Adapter 1, select Internal Network from the drop-down menu. The network name should be displaying with the name “**malfoy**” and will add it automatically upon entering the previous terminal commands. “Cable Connected” checkbox must be checked.

A computer screen shot of a computer

AI-generated content may be incorrect.

* Now the user shall create the isolated malfoy network:
* (NOTICE: To remove the DHCP configuration, type ‘**cd /Program Files/Oracle/VirtualBox’**, hit enter. Then type ‘**VBoxManage list dhcpservers**’ and hit enter. This will display a list of any pre-existing DHCP configurations for VirtualBox. If you see one for Malfoy, type ‘**VBoxManage dhcpserver remove –netname malfoy**’ and hit enter).
* Type ‘**VBoxManage dhcpserver add –network=Malfoy –server-ip=10.38.1.1 –netmask=255.255.255.0 –lower-ip=10.38.1.110 –upper-ip=10.38.1.120 –enable**’ and press enter.
* Now that your dhcp server is set up, we will now boot up Kali Linux! Log in, click on the Terminal and type **‘ip address’**. If you see its IP address within the **10.38.1.110-120** range (an example is **10.38.1.112**), then you successfully configured the server. But we need to also ensure that the connection is **SECURED**. First, in Kali Linux’s Terminal, ping your current host’s IP address using the **‘ping’** command followed by your actual host IP address. On your host, ping Kali Linux’s IP address through the **‘ping’** command (you can find this with **‘ipconfig’** command). If either the host or client successfully retrieves packets from each other, then the connection is NOT secure. If it times out, then the connection is isolated and secured, preventing the host from being exposed to risk and only allowing VMs on the **malfoy** network to communicate.
* Now we will use a useful network sniffing tool called **Nmap**! To make the process faster and thorough, we will elevate to Nmap’s admin privileges, allowing for more extensive network analysis. In Kali Linux’s Terminal, type **‘sudo nmap -sS -T4 10.38.1.110-120’** and hit enter.

**[TEMP SECTION]**

A screenshot of a computer

AI-generated content may be incorrect.

SOLUTION : SEARCH IN BROWSER FOR 10.38.1.112 AS MRROBOT’s IP ADDRESS (QUICK CHECK – sudo nmap -sS -sV -sC -T4 -p- 10.38.1.112)

Quick reachability: ping -c 3 10.38.1.112

curl -I http://10.38.1.112/

NEXT PHASE – Find 3 “flags” inside mrrobot