Lab 01 – Building a Virtual Network Security Test Lab

A lab environment, otherwise known as a sand box, is crucial when working with vulnerable, exploitable, and malicious software. Although a physical environment could be used as a lab environment, a more typical environment is now built using virtualization software known as a hypervisor. This helps protect the campus, corporate or home network from the potentially unsafe lab environment. This also helps establish a portable lab environment where you are able to test advanced functionality from the ease of your own desktop, or laptop.

For this particular lab, there is nothing particularly unsafe about it, so there's no need to worry about completely isolating this environment as we will have to do later this semester when dealing with malware.

We will need to be able to create several VMs (known as virtual machines) as the semester progresses. Some of these VMs will use guest Operating Systems (OSs) such as Windows or Linux variants whereas others will be prebuilt VMs. In order to ensure you have the proper Windows software at your disposal, you should have an account available for you to access Microsoft Azure for Education portal. This will allow you to gain access to a licensed copy of the Windows Operating Systems you will need access to in order to complete this lab and future ones.

Complete the following steps:

TASK ONE: Hypervisor Configuration

1. Install your Hypervisor of choice: VMware Workstation, VMware Fusion, or Oracle Virtualbox. If you have a full VMware ESXi, Hyper-V, or KVM implementation at your disposal, you may use that as well; however, please keep in mind that some of the software we will use this semester may not be ready for primetime and may contain bugs that should NOT be implemented within a production environment.

TASK TWO: Windows Lab Environment Configuration

1. The goal of this task is to create a VM of a Windows Domain Controller using either Windows Server 2022, 2019, 2016, or 2012 R2. You will also create a VM of a Windows client. The Windows client version is up to you: Windows 11, 10, 8.1, or 7. Please know that Windows Server is unable to run on ARM right now. This means that if you have a newer macbook with an M1, M2, or M3 processor, you will be unable to run an x86 or x64 operating system. You will need to use another computer to complete this lab. *If you do not have another computer to complete this step of the lab and are not able to use a computer lab on campus, please let me know.*

2. A lab walkthrough using older Windows versions can be found at http://thehackerplaybook.com/Windows_Domain.htm Complete the tasks displayed in this walk-through.

TASK THREE: Kali Linux Download

1. We will be utilizing other VMs throughout this course. From an offensive perspective, you should download a Kali Linux .iso, or virtual appliance from: https://www.kali.org. This will be used as your attack VM at a later date in this course. Create a Kali Linux VM and show that you are able to login to this VM. There is nothing else that needs to be completed with Kali for this initial lab.

DELIVERABLE:

1. Complete a professional write-up and include the following information:

    a. **Description:** Brief description, such as an executive summary, depicting an overall view of what topic or technology you are concentrating on within this lab. Keep this short and to the point. Think like a consultant and be mindful that what you are providing should represent you as a professional in the industry.

    b. **Topology:** Use Microsoft Visio, or Lucid Chart, to create an aesthetically pleasing network topology. This should include devices, network connections, virtual NIC labels, IP Addresses, subnet masks, domain information, credential used, and anything else you feel would be beneficial to add.

    c. **Key Syntax:** Sometimes it's nice to include key syntax used. For instance, if you're not a Linux guru, it might be nice to include how you configured a static IP Address in the Linux CLI, or what files you needed to modify in order to configure a primary DNS server IP Address or domain suffix.

    d. **Verification:** Provide key screenshots that display verification that the lab was completed. For instance, if the lab required you to login from a windows client to a domain controller, show the screenshot or multiple screenshots verifying this action was achieved successfully. Make sure you provide a description of what the screenshot is showing. Do not simply add the screenshot and state, "here is the screenshot". These descriptions and screenshots should paint a story of the work you put into this lab and verify you have successfully completed the virtual environment configuration. Be thorough and professional!

    e. **Conclusion:** Wrap up your lab report with a short conclusion. If something did not work, state it. If everything did work successfully, state that as well.

    f. **References:** Make sure you include any works cited here as well as throughout your lab report. If you looked something up, include it.

2. Upload the following file(s) to the assignment within Brightspace:
    a. your .docx or .pdf file (please do NOT zip your files)

Good Luck with your first lab!