**https://www.youtube.com/watch?v=5OessbOgyEo**

**ACTIVE DIRECTORY HOMELAB**

P R O J E C T

**Fall 2024**

**Khang Nguyen**

**Active Directory HomeLab Project**

Being in the IT industry, we are exposed to new technologies and equipment everyday. Not everyone is able to get hands-on experience with industry-leading tools, but you can certainly read about it online. Learning how to implement what you’ve learned from a textbook into the real world can be challenging, especially when there is a limit on tools and resources.

Thanks to virtualized environments, you do not need to go out and buy production-grade equipment in order to get real experience.

In the I.T. / Cybersecurity space, you may have heard of people using the term homelab and building one to gain experience. Beginners may be completely lost on what they need or what to do… this is for them.

**What is a HomeLab in I.T. / Cybersecurity?**

A home lab is a safe environment where you can practice and experiment with tools in order to gain experience, primarily dealing with common techniques and components in IT.

The main purpose and goal of the lab is to learn how to install, configure, and manage these industry-leading tools on a small scale in order to apply similar processes to the real-world.

Homelabs could be very diverse and can be fit to satisfy a variety of different functions. It can be simple or complex with your choice to provide additional equipment. As long as you have a scope and guide in mind, it will be easy to accomplish.

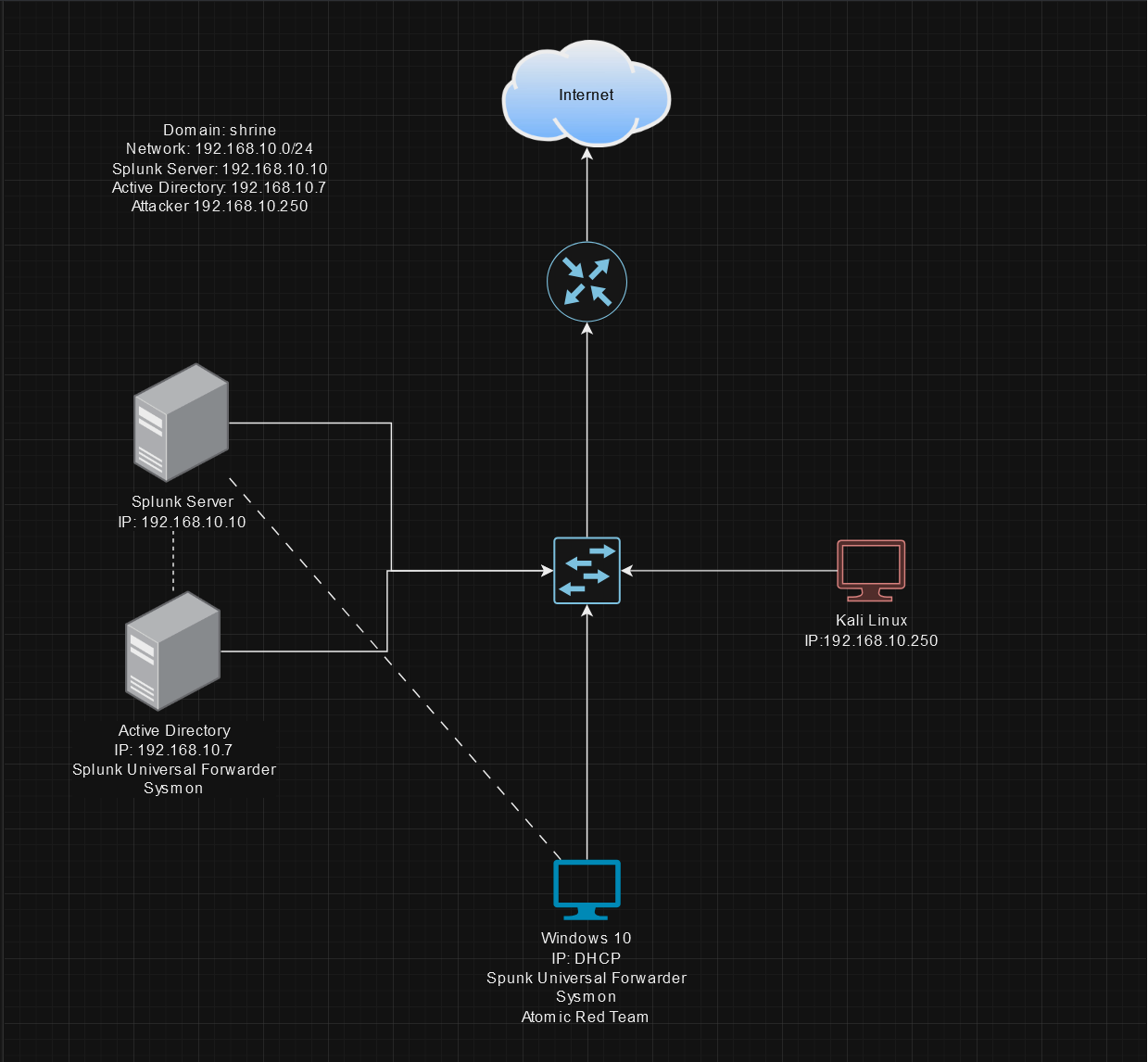
**Active Directory Homelab Project**

For this active directory homelab project, I will be building and simulating a business network with different components including:

* Installing Windows 10 image
* Setting up Oracle VM Virtual Box
* Configuring and working with Active Directory
* Setting up and connecting Linux Desktop and Windows 10 pro (enterprise) VM images to AD
* Configuring a System Information Event Management System (SIEM) with Splunk and logging events
* Possibly more

For this project, I began with creating a network topology of the environment I want. This was essential in my project in order to gain a better understanding of how I want data to flow and what I am trying to do.

**Network Topology**



**Typology Breakdown**

**Installing Kali Image**

I will be installing the pre-built virtual machine for VirtualBox to simulate an attacker.

* <https://www.kali.org/get-kali/#kali-virtual-machines>

**Setting up Virtual Box**

Virtual box is free to use, I will be configuring the lab within here.

* <https://www.virtualbox.org/wiki/Downloads>

**Installing Windows Server 2022**

I will be installing the iso image for windows server 2022 to base my AD environment.

* <https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2022>

**Configuring and working with Active Directory**

My devices will be centrally managed by AD. To do this, I will be setting up an AD environment. I will be using MyDFIR’s five part video tutorial and walk through setting up an AD environment.

* <https://www.youtube.com/watch?v=5OessbOgyEo>

**Connecting Desktops**

**Setting up and connecting Linux Desktop and Windows 10 enterprise VM images to AD**

**Linux Desktop**

I want to connect a Linux distribution to AD. The distribution will be Ubuntu Linux 18.04.4 TLS.

* <https://ubuntu.com/download/desktop>

**Windows 10 Pro (Enterprise)**

I will also be connecting a Windows 10 enterprise VM to simulate an employee workstation. Download link is available on the official Microsoft website.

* <https://developer.microsoft.com/en-us/windows/downloads/virtual-machines/>

**Configuring a vulnerability scanner (Nessus) and simulating vulnerability scans**

Vulnerability scanners offer a means of identifying and actively managing known vulnerabilities. Tenable Nessus is a popular vulnerability scanner used in all kinds of corporate networks. Nessus Essentials (previously known as Nessus Home) is a free vulnerability scanner you can use to scan up to 16 IPs. Since this homelab will be relatively small, I will be using Nessus Essentials as my vulnerability scanner.

* <https://www.tenable.com/products/nessus/nessus-essentials>

**Configuring a System Information Event Management System (SIEM) with Splunk and logging events**

System Information Event Management Systems (SIEMs) are used to correlate and congregate logged events and alerts into meaningful and actionable data so an organization can prioritize critical alerts. Splunk is a well-known SIEM solution within the industry. Splunk provides a free, lightweight version for at-home users to try out. I will be using this as my SIEM.

* <https://www.splunk.com/en_us/download/splunk-enterprise.html>

**Let the Project Begin**

This Active Directory Project will be a meaningful and positive experience with it being such a common technology in the field. It is a great opportunity to apply what I have learned through self-study. This document is meant to outline the process of building a lab.

**Sources**

Download Kali Linux: <https://www.kali.org/get-kali/#kali-virtual-machines>

Download Windows 10: <https://www.microsoft.com/en-us/software-download/windows10>

Download Windows 2022 Server: <https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2022>

Download Virtual Box: <https://www.virtualbox.org/wiki/Downloads>

Download Ubuntu Desktop: <https://ubuntu.com/download/desktop>

Nessus Essentials: <https://www.tenable.com/products/nessus/nessus-essentials>

Download Splunk Enterprise 8.0.2.1: <https://www.tenable.com/products/nessus/nessus-essentials>

Homelab Idea first inspired by MyDFIR: <https://www.youtube.com/watch?v=5OessbOgyEo>

Sources subject to change as I go throughout the project.