COMPREHENSIVE CYBERSECURITY HOMELAB: DETECTION, MONITORING, AND PENETRATION TESTING IN A CONTROLLED ENVIRONMENT

This is a Cybersecurity Homelab which provides a hands-on environment for learning and applying security concepts in a controlled setting. It enables the setup of tools for detection, such as Intrusion Detection Systems (IDS), and monitoring with SIEM solutions to analyze network traffic and logs. Penetration testing can be conducted safely to identify vulnerabilities and practice ethical hacking techniques. This lab setup mimics real-world enterprise environments, offering invaluable experience in securing and defending IT infrastructures.

Tools and Their Descriptions

1. **Kali Linux (Attacker)**
   A penetration testing and ethical hacking operating system equipped with tools to simulate attacks and test security defenses. It enables users to explore vulnerabilities and assess the effectiveness of their configurations.
2. **pfSense (Firewall)**
   An open-source firewall and router software designed to provide secure network segmentation. It is highly customizable and helps control and monitor network traffic.
3. **SecurityOnion (IDS)**
   A robust intrusion detection system (IDS) and log analysis platform used for network security monitoring. It provides tools to analyze network traffic and detect potential threats.
4. **Splunk/Wazuh (SIEM)**
   A powerful security information and event management (SIEM) tool for log collection, analysis, and visualization. It enables real-time monitoring and advanced threat detection.
5. **VMWare/VirtualBox (Hypervisor)**
   Virtualization platforms used to create and manage virtual machines, making it easy to build a scalable, isolated environment for experimentation and learning.

6. **Windows Active Directory (Domain Controller)**
   A centralized system for managing users, devices, and permissions in a network. It provides authentication, authorization, and directory services.
7. **Vulnerable Machines (Ubuntu, Windows, Metasploitable 2, DVWA, Vul**

CONTROLLED AND CENTRALIZED ENTERPRISE ENVIRONMENT

Active Directory and Windows 10 Client in an Enterprise Environment

Active Directory (AD) on a Windows Server acts as a centralized directory service, managing authentication, permissions, and policies for all connected systems. By integrating a Windows 10 client with the AD, users can log in with centralized credentials, enabling consistent access control and resource management. This setup replicates an enterprise environment, allowing users to simulate real-world scenarios such as group policy management, user provisioning, and secure communication between devices.

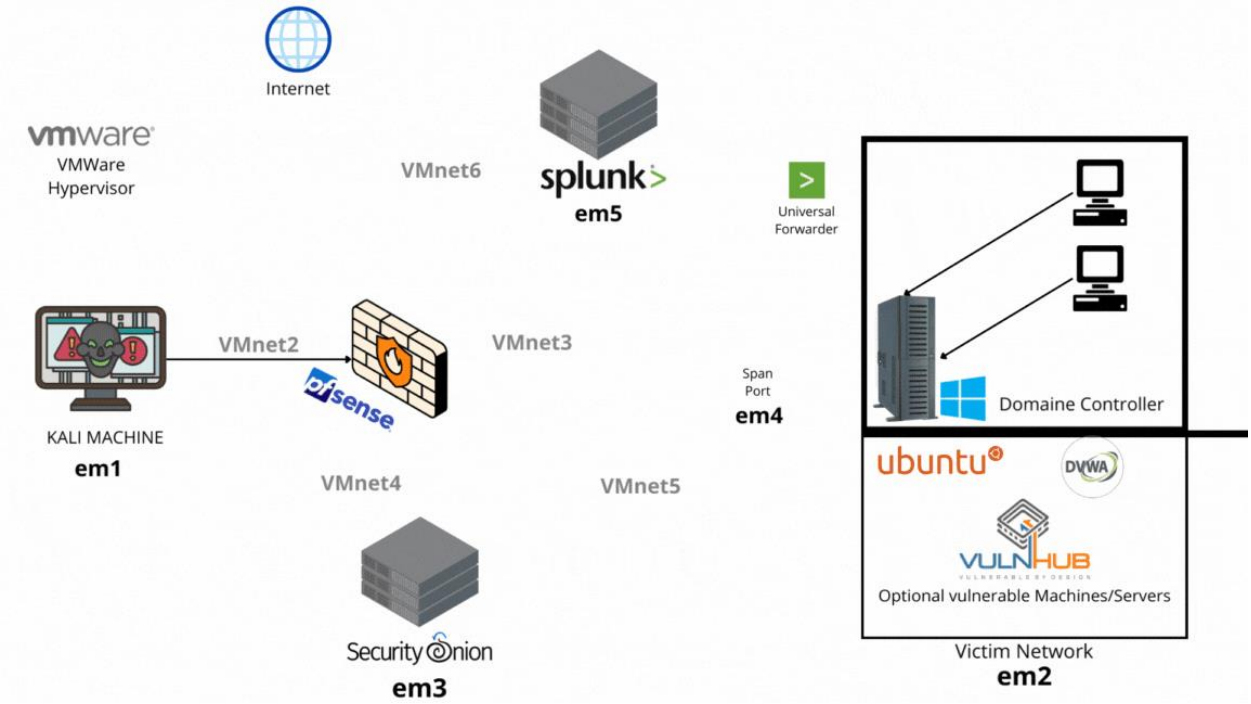
PURPOSE

Integrating Active Directory (AD) with a Windows 10 client in a security homelab is essential for replicating enterprise-level environments, where AD is a critical component. Here's why this setup enhances security and is crucial for a homelab:

1. Centralized Authentication and Authorization:
   Active Directory provides a centralized platform for managing user accounts, passwords, and access rights. This enables administrators to simulate enterprise practices, such as enforcing password policies, multi-factor authentication, and user role management, which are critical for securing IT systems.
2. Realistic Attack Surface:
   AD is a frequent target in real-world cyberattacks due to its central role in organizations. Simulating an environment with an AD domain controller and a Windows 10 client allows for practical exploration of vulnerabilities (e.g., privilege escalation, pass-the-hash attacks) and strengthens skills in detecting and defending against such threats.
3. Policy Enforcement and Monitoring:
   The integration supports Group Policy Objects (GPOs) for managing security

configurations across the client machine. Users can experiment with enforcing security baselines, monitoring user activity, and testing incident response workflows in a safe environment.

This configuration provides a hands-on platform for understanding enterprise security challenges, configuring defenses, and practicing detection and response techniques effectively



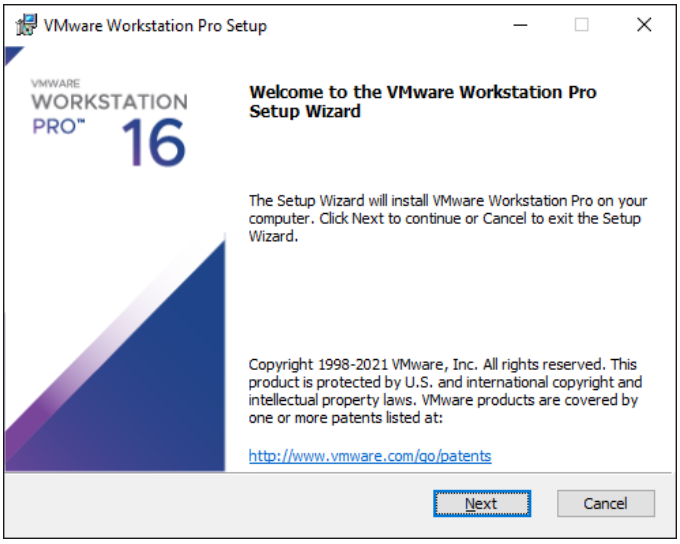
DOWNLOADS AND INSTALLATION PROCEDURES

1. VMWare and Kali Linux Installation

This project will demonstrate how to properly install both **VMWare Workstation** and **Kali Linux. VMWare** allows the users to set up virtual machines on a single physical machine and have its own operating system. **Kali Linux** is an operating system based on Debian Linux that is mainly designed for tasks such as forensics and penetration testing.

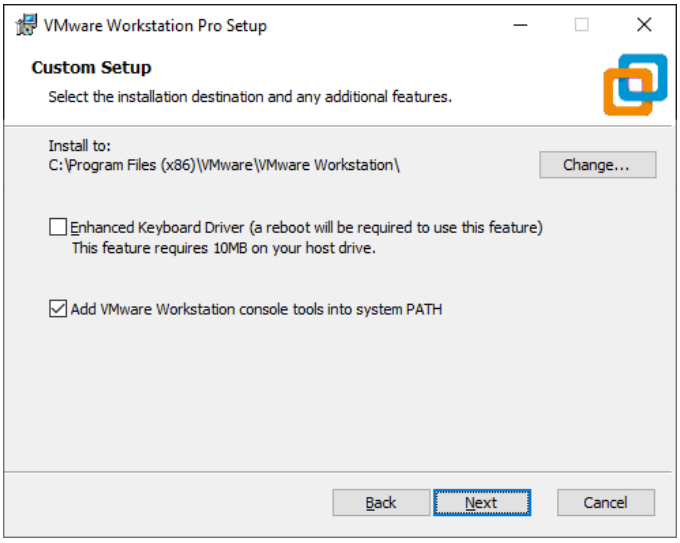
VMWare Installation

You can go to https://www.vmware.com/products/workstation-player.html and download **VMWare** from there. Locate the installation file and run the program



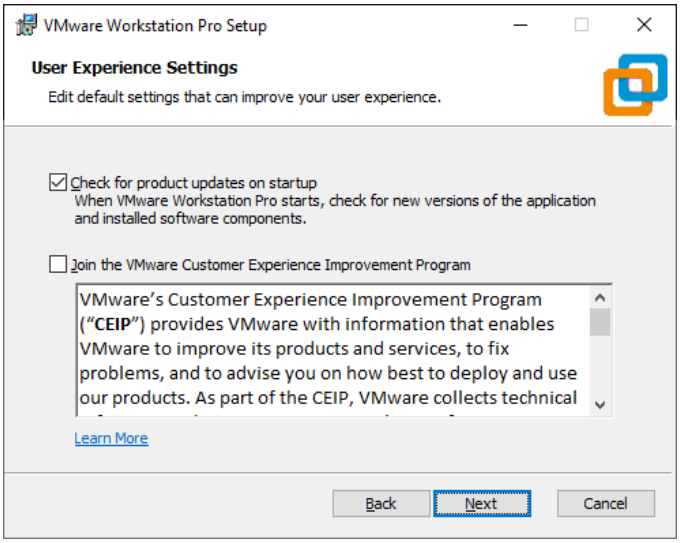
github-small

You can choose to have the enhanced keyboard options, which enables users to have better handeling with international keyboards. I opted not to install the driver



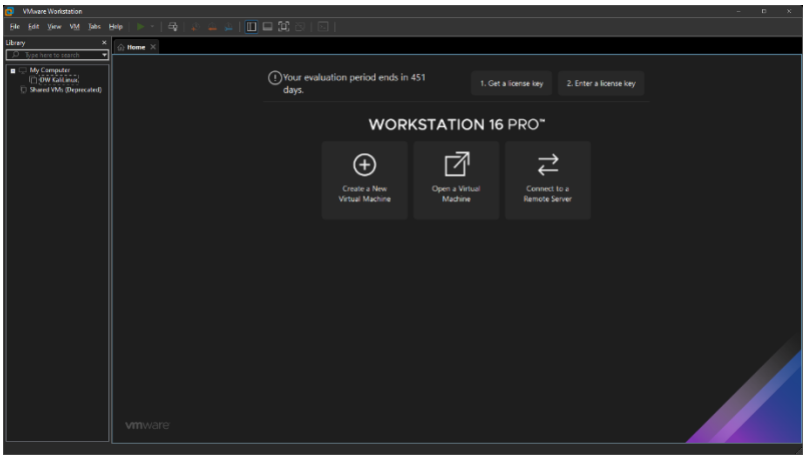
github-small

The next step asks if you want to have update checks on startup. I opted to keep it checked to have opportunities to improve my experience of **VMWare** with updates.



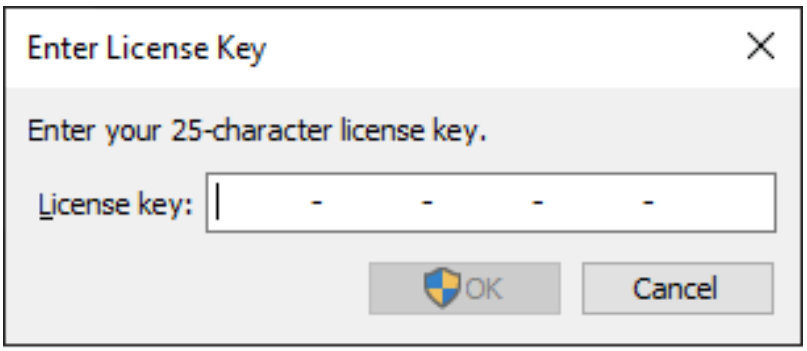
github-small

After the setup it should look like this:



github-small

Go to the Help option and choose the Licensce Key option. You can choose to do the 30 day trial or input the key if you bought the product. If you don't input the key, you will not be able to utilize all of **VMWare's** functionalities.



github-small

Kali Linux Installation

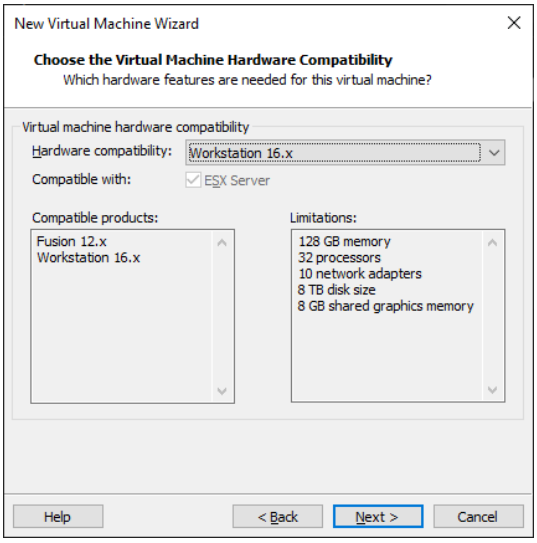
Go to https://www.kali.org/get-kali/ and scroll down until you find the Kali Linux Changelog. Depending on what type of system you have, you may want the 64x or 32x version of **Kali Linux**

github-small

Go to **VMWare** and create a new virtual machine with the option of custom installation checked

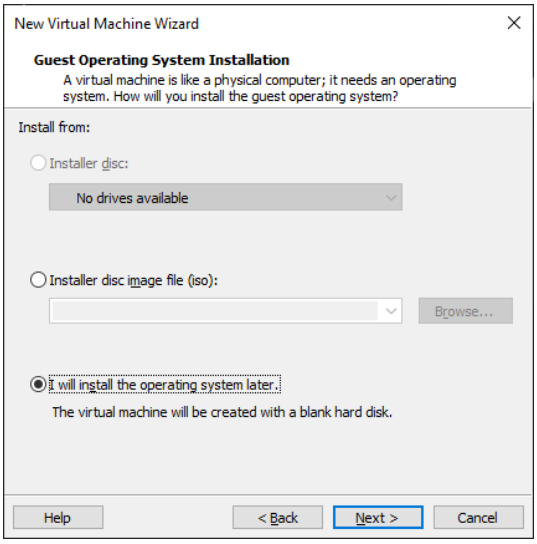
github-small

Choose the hardware compatability. In this case, I chose Workstation 16.x as it is the most recent edition.



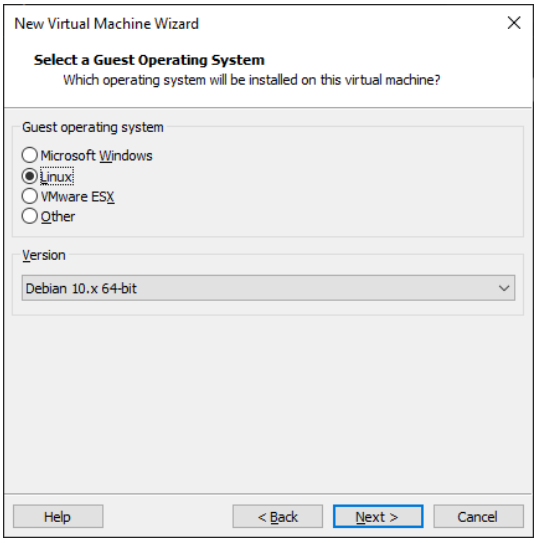
github-small

Choose to install the Operating System later.



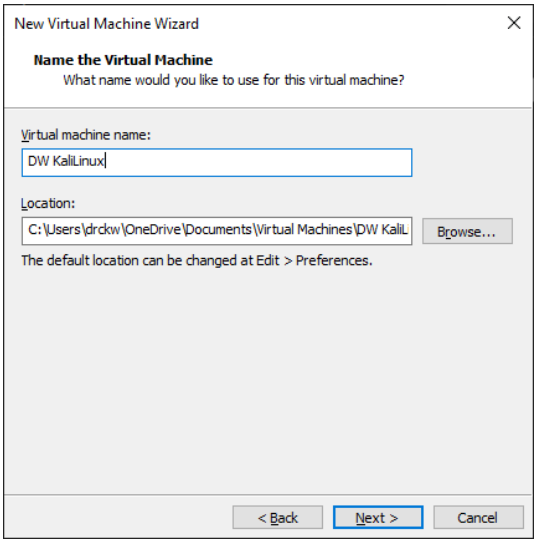
github-small

When choosing the guest operating system, make sure to choose Linux. For the version, make sure to choose Debian or Ubuntu as it is what Kali Linux is based off of.



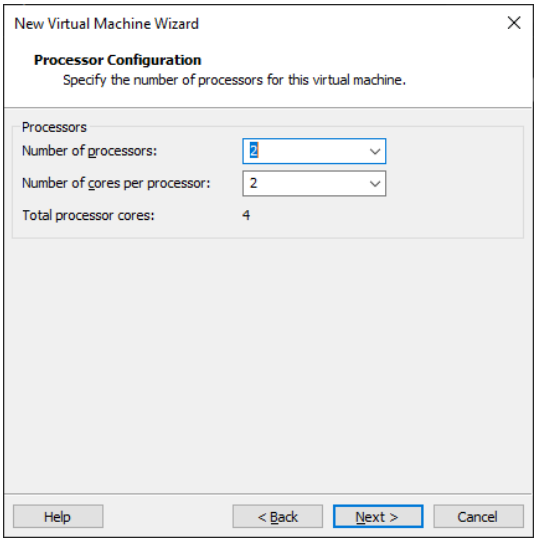
github-small

Name your virtual machine. In this example, I named my VM **DWKaliLinux**



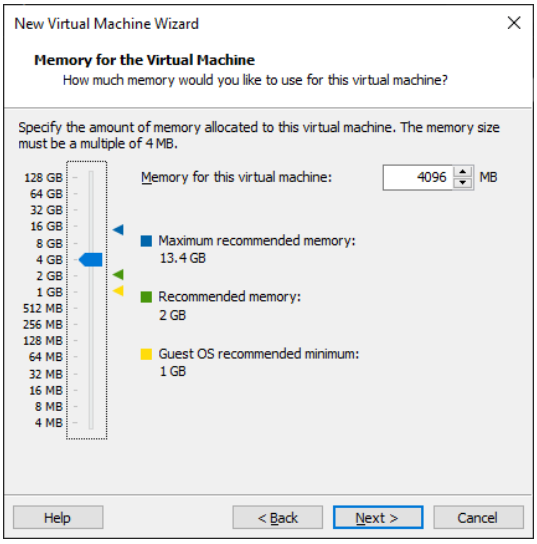
github-small

Input the number of processors and cores you want to give to your virtual machine. The amount you can give depends on the specifications of your computer. In this case, I gave my virtual machine 2 processors and 2 cores.



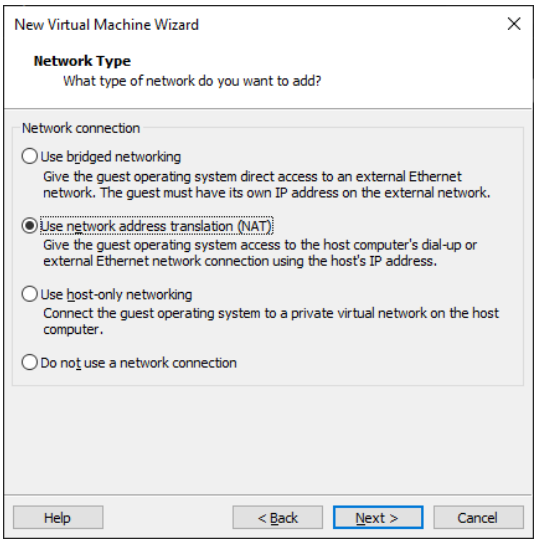
github-small

Input how much virtual memory or VRAM you want to give your virtual machine. This determines how fast your VM will run. The more VRAM you can provide, the better the speed



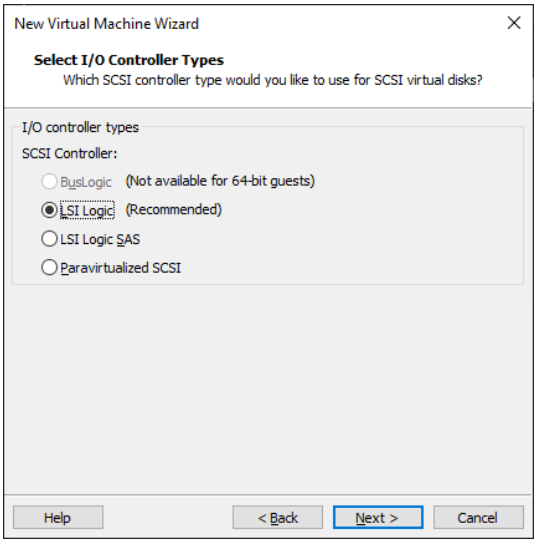
github-small

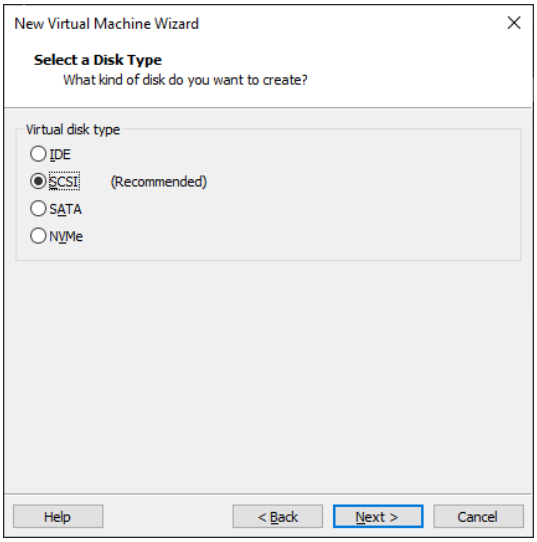
Choose NAT if you want to utilize the internet on your VM.



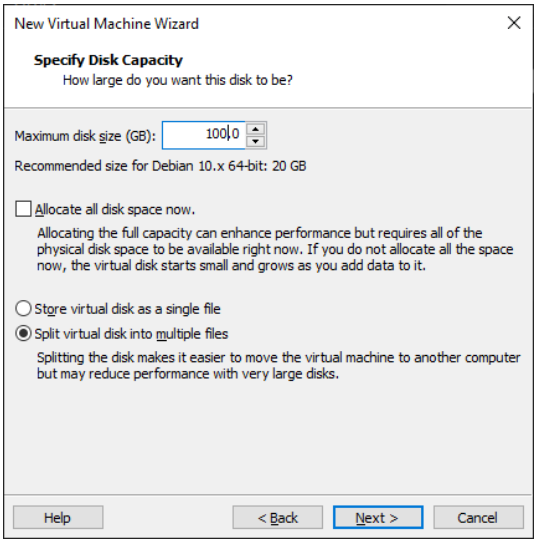
github-small

For disk and I/O controller settings, I used the reccommended settings



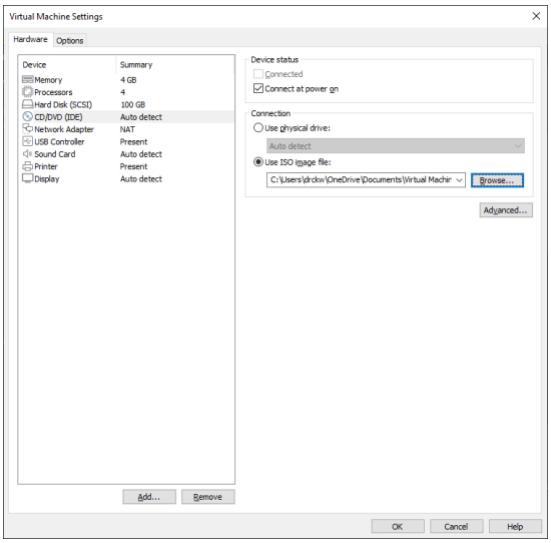


Input how much disk capacity you want for the VM. For the demonstration, I used 100 Gb of disk capacity. 20 is the reccommended



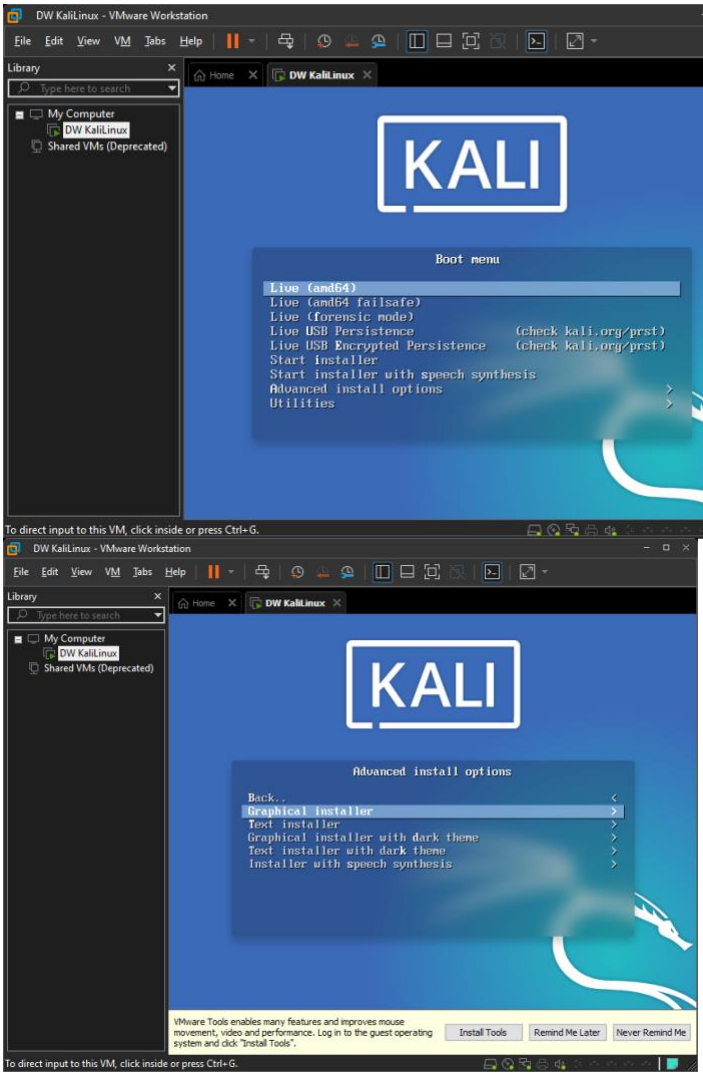
github-small

Go to the CD/DVD settings and set the ISO image path to the **Kali Linux** ISO.

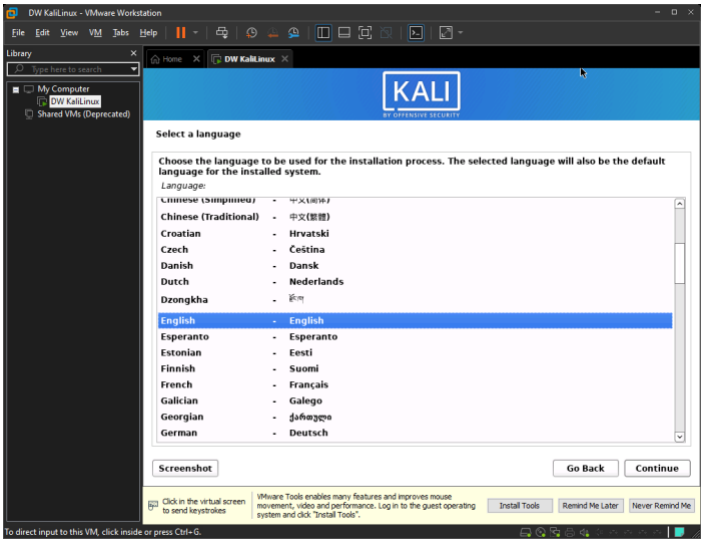


github-small

Power up Kali Linux and choose advanced installer, and then graphical installer

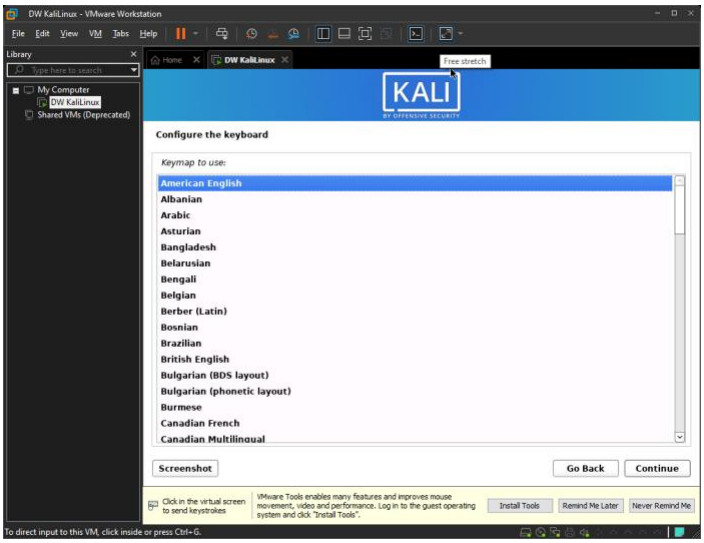


Once the installer loads up, choose the language you want and location



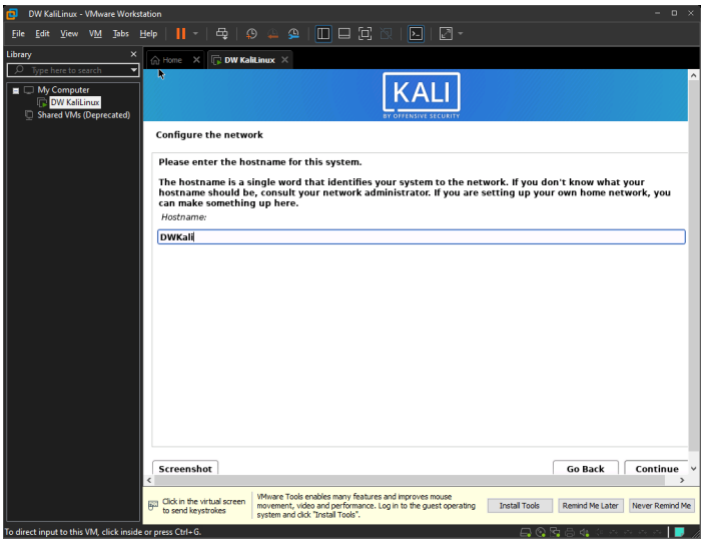
github-small

Choose the keyboard configuration you want. I chose American English



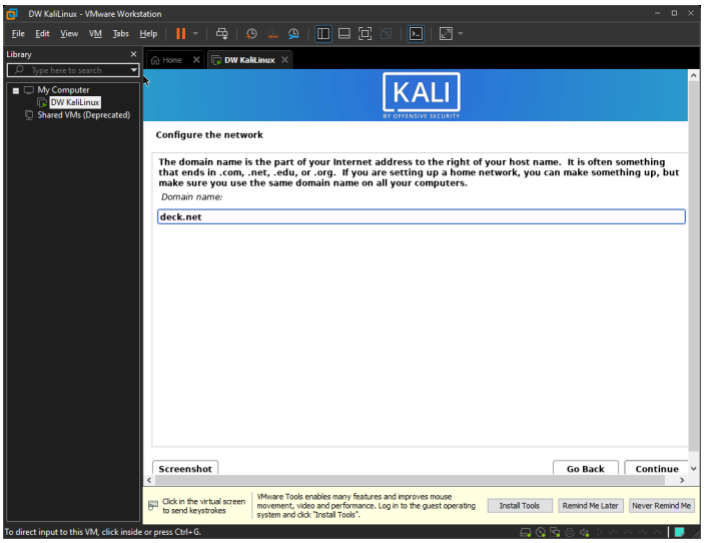
github-small

Enter a hostname for the system. For my hostname, it is **DWKali.**



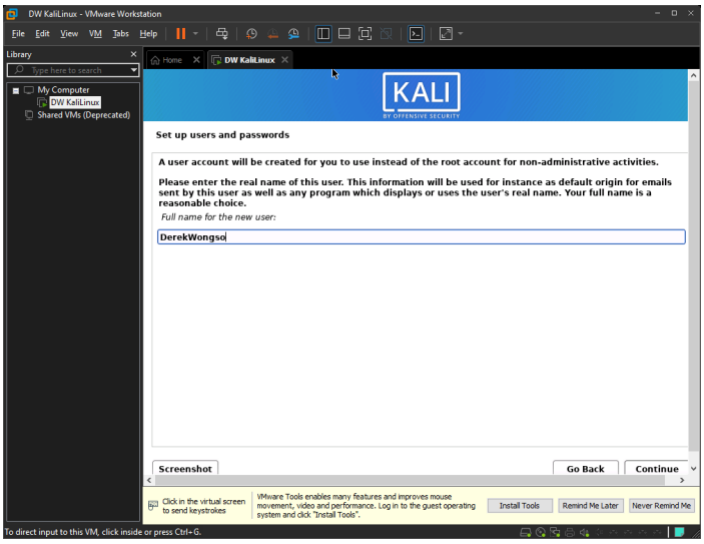
github-small

Create a domain name for part of your internet address



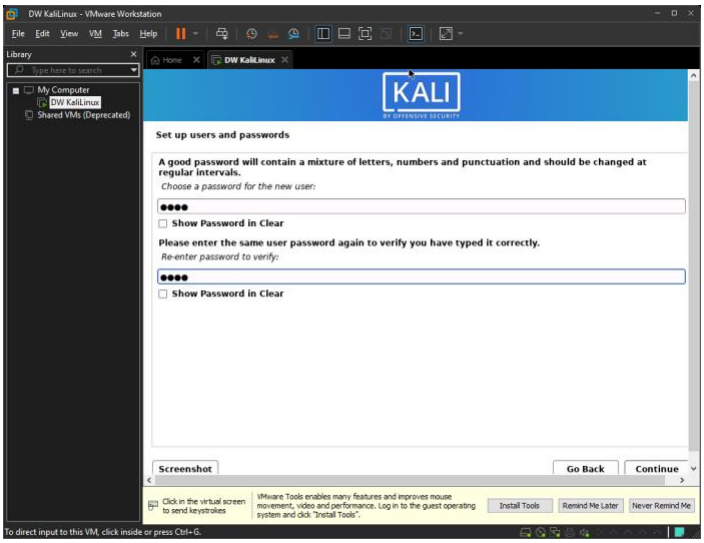
github-small

Create your username



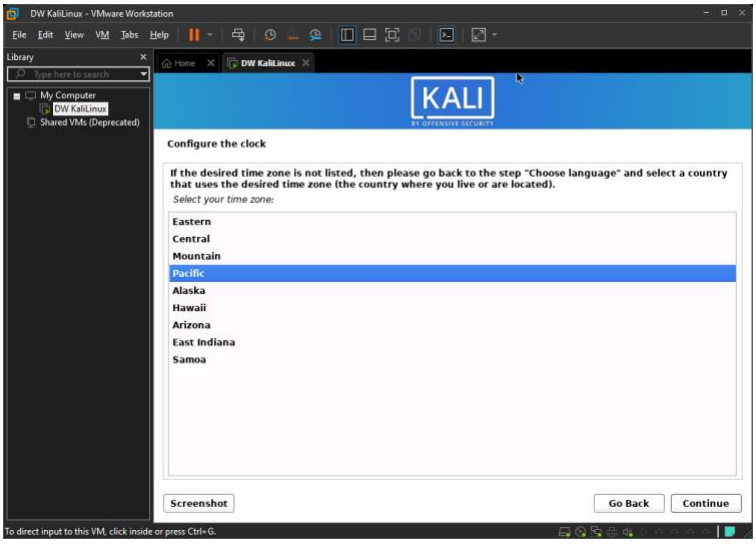
github-small

Create your login password



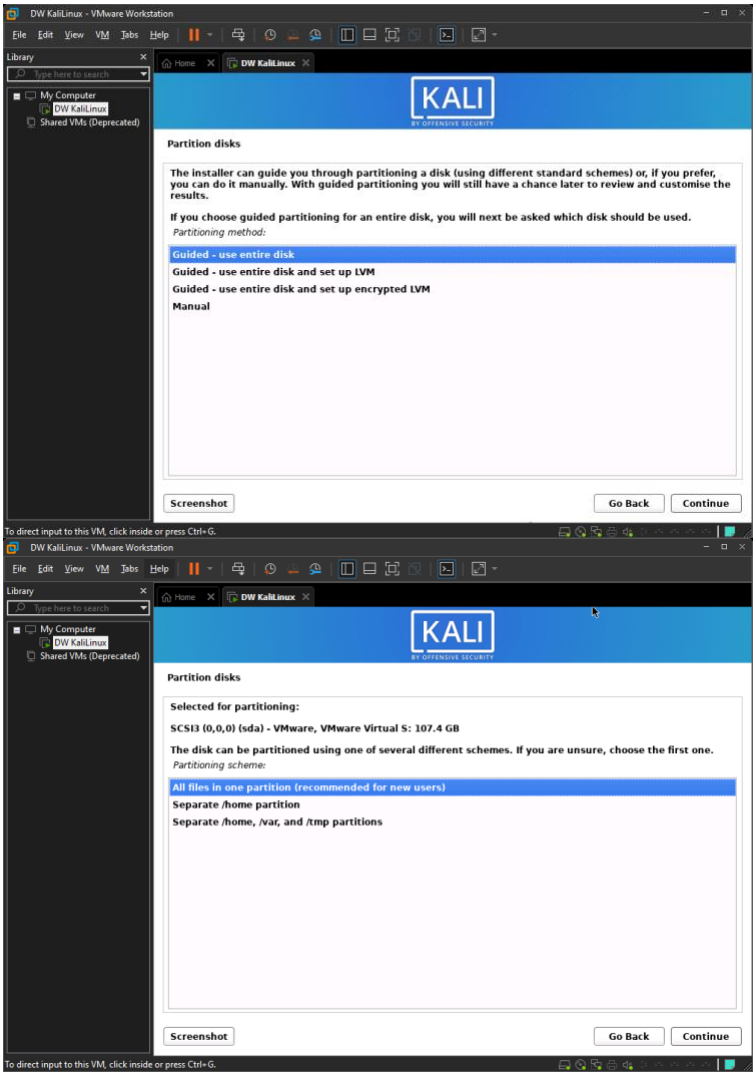
github-small

Set up your time zone

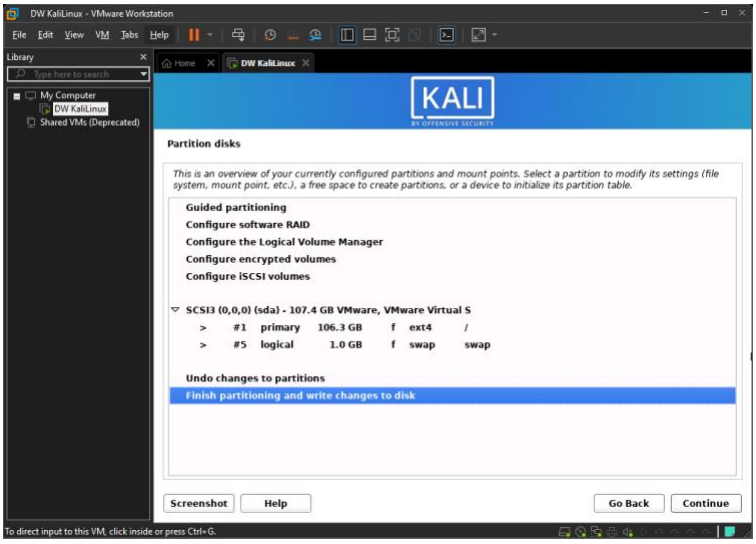


github-small

Use the entire disk to partition and put all the files in one partition as reccommended

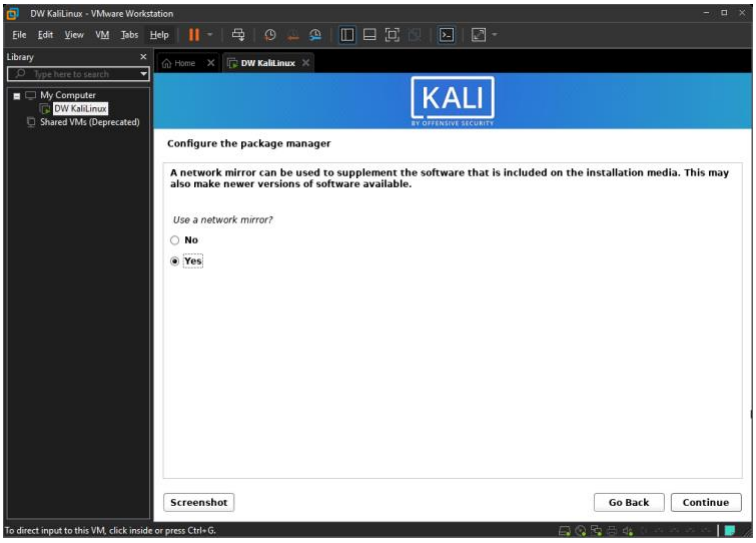


Now, write the changes to disk



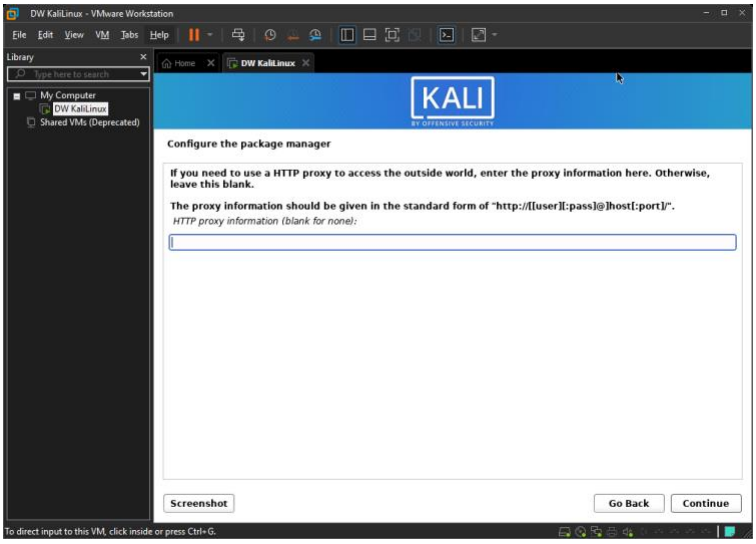
github-small

For the next step, I chose to have netowrk mirrors as it can help supplement the software that is included with the installation media



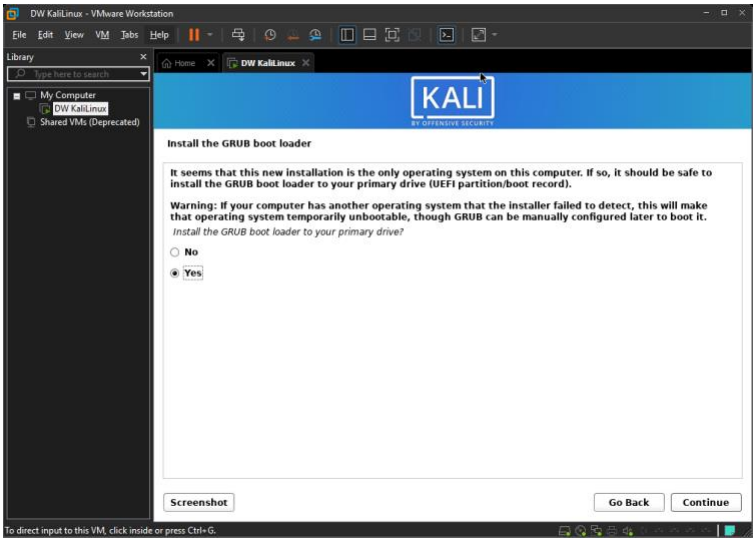
github-small

If you are using a proxy, you may want to put the http proxy information. Otherwise you can leave it blank and move on



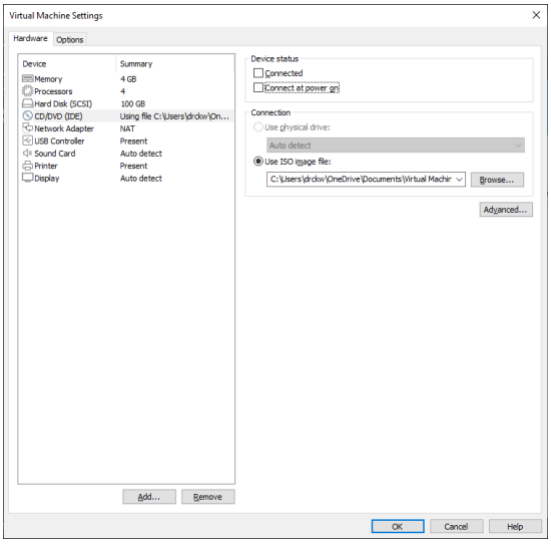
github-small

The important part of this step is to make sure you check yes to have the grub boot loader enabled. If you do not, then **Kali Linux** will not load. Make sure to input dev/sda.



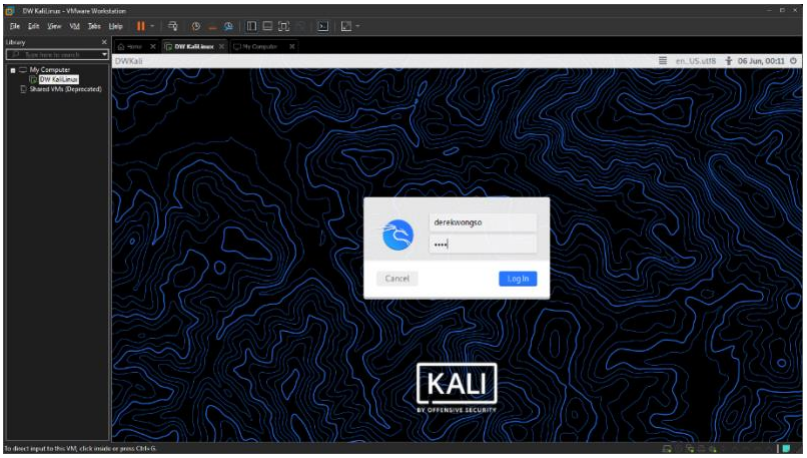
github-small

Before rebooting the VM, go to the **VMWare** settings for **Kali Linux**. On the CD/DVD settings, make sure the “Connected at power” box is unchecked. If not, then the installation process will begin once again after booting up the VM. Finish the installation process and then reboot.



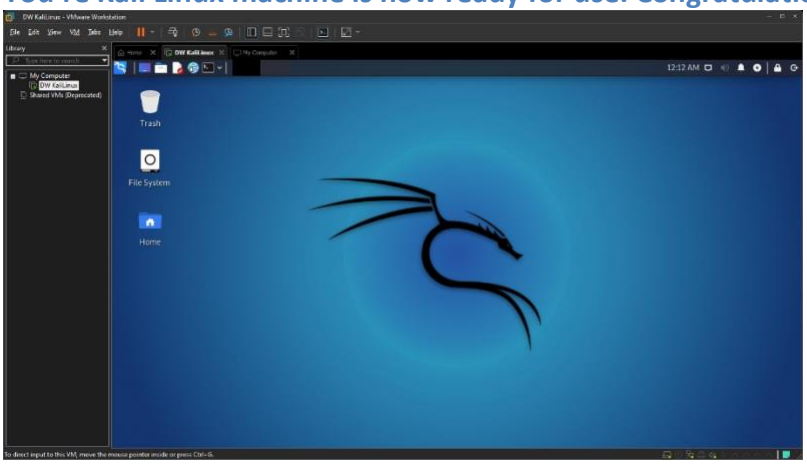
github-small

Once the VM is rebooted, you should be prompted with a login screen. Input the username and password you created within the installer



github-small

You’re Kali Linux machine is now ready for use. Congratulations!



github-small