Home Lab

In this **HOME LAB** set up i am trying to cover various domains of cyber security so we get to learn many things in our home lab. To set up home lab you need to have a system of at least **8gb RAM** and **512 SSD minimum and GPU if you have**

NOTE: In this Documentation I am using links for reference to save time and better reference I am not using my own Screenshot

Let's deep down into the lab

Lab Requirements

here is the links and details things to download for lab

Cisco packet tracer

Cisco packet tracer will help us to build our networking skills.

The wikipedia says "Packet Tracer is a cross-platform visual simulation tool designed by Cisco Systems that allows users to create network topologies and imitate modern computer networks.The software allows users to simulate the configuration of Cisco routers and switches using a simulated command line interface.Packet Tracer makes use of a drag and drop user interface, allowing users to add and remove simulated network devices as they see fit"

Now we know what is Cisco Packet tracer lets learn how to download it

1. Download Packet Tracer

- Go to Cisco's Networking Academy website: You need to create a Cisco Networking Academy account (if you don't already have one).

  - Visit: Cisco Networking Academy https://www.netacad.com/

  - Sign up for an account or log in if you already have one.

- Download Packet Tracer: After logging in, go to the "Resources" section and look for "Packet Tracer." Select the version for your operating system (Windows, macOS, or Linux).

- Or you can use this link also**: https://www.computernetworkingnotes.com/ccna-study-guide/download-packet-tracer-for-windows-and-linux.html**

2. Install on Windows

- Run the Installer: Once downloaded, double-click the installer file (it will have a `.exe` extension).

- Follow the Installation Steps:

  - Accept the terms and conditions.

  - Choose the installation directory (you can leave the default settings).

  - Click "Install" to begin.

- Complete the Installation: Once the installation is complete, you can launch Packet Tracer from the Start menu.

3.Launch Cisco Packet Tracer

- Once the installation is complete, launch the Packet Tracer application.

You may need to log in using your Cisco Networking Academy credentials.

For Linux and MacOS

Note: For Linux and Mac Os

Linux**: https://www.geeksforgeeks.org/how-to-install-cisco-packet-tracer-on-ubuntu-22-04-lts/**

MacOS: **https://learningnetwork.cisco.com/s/feed/0D53i00000Kt6e0CAB**

Windows Server

Windows Server is the platform for building an infrastructure of connected applications, networks, and web services, from the workgroup to the data center.

Windows Server bridges on-premises environments with Azure, adding additional layers of security while helping you modernize your applications and infrastructure

Windows Server is a robust server operating system developed by Microsoft, designed to manage enterprise-level tasks such as hosting websites, running applications, and handling IT infrastructure.

It includes features like Active Directory for centralized identity management, Hyper-V for virtualization, and PowerShell for automation, making it a cornerstone in enterprise environments for file storage, email hosting, and database management.

Windows Server

1. Start the VM and boot from the ISO.

2. Follow the installation steps:

- Select language, edition, and enter a product key if prompted.

- Partition the virtual disk and proceed with installation.

3. After installation, configure basic settings like administrator password and updates.

Download link: **https://software-static.download.prss.microsoft.com/sg/download/888969d5-f34g-4e03-ac9d-1f9786c66749/SERVER_EVAL_x64FRE_en-us.iso**

Windows

Windows is a widely used family of client operating systems, including popular versions like Windows 10 and Windows 11.

Known for its intuitive interface and broad software compatibility, it is ideal for personal and professional tasks, offering features such as the Start Menu, the Microsoft Store,

and built-in security tools like Windows Defender. I am using windows 7, windows 10 and windows 11 for lab

1. Start the VM and boot from the ISO.

2. Follow the setup wizard:

- Choose language, version, and activation options.

- Partition the virtual disk and install.

3. Complete initial setup, including setting a username and password.

Windows 11: **https://software-static.download.prss.microsoft.com/dbazure/888969d5-f34g-4e03-ac9d-1f9786c66749/26100.1742.240906-0331.ge_release_svc_refresh_CLIENT_LTSC_EVAL_x64FRE_en-us.iso**

Windows 10: **https://www.microsoft.com/en-us/evalcenter/download-windows-10-enterprise**

To download more windows system

https://tb.rg-adguard.net/public.php

https://files.rg-adguard.net/category

Vulnerable Machine

A vulnerable machine refers to a computer system intentionally configured with weaknesses or flaws, allowing cybersecurity practitioners to:

1. Identify Vulnerabilities: Practice finding security issues such as unpatched software, misconfigurations, or outdated protocols.

2. Exploit Weaknesses: Learn and practice exploiting these vulnerabilities to understand attack techniques.

3. Test Security Tools: Use tools like Metasploit, Nmap, Burp Suite, etc., to perform assessments.

4. Develop Skills: Improve their ethical hacking, penetration testing, and defensive cybersecurity capabilities.

Here i am only using metasploitable 2 matrix is just alternative if you want

Vulnerable machines from **https://www.vulnhub.com/** to test

This will be our target each time when we want to perform pretesting

https://www.vulnhub.com/entry/metasploitable-2,29/

https://www.vulnhub.com/entry/matrix-breakout-2-morpheus,757/

Wazuh

Wazuh is a free and open source platform used for threat prevention, detection, and response. It is capable of protecting workloads across on-premises, virtualized, containerized, and cloud-based environments.

Wazuh solution consists of an endpoint security agent, deployed to the monitored systems, and a management server, which collects and analyzes data gathered by the agents.

Besides, Wazuh has been fully integrated with the Elastic Stack, providing a search engine and data visualization tool that allows users to navigate through their security alerts.

This we will use for collecting logs and other things

More Information about Wazuh

https://github.com/wazuh/wazuh

Guidance to install Wazuh

Documentation: **https://documentation.wazuh.com/current/installation-guide/index.html**

Kali Linux

Kali Linux, on the other hand, is a specialized Debian-based Linux distribution designed for penetration testing, ethical hacking, and cybersecurity research.

It is preloaded with an extensive array of security tools, including Metasploit, Nmap, and Wireshark,

providing a streamlined and customizable environment for cybersecurity professionals to conduct vulnerability assessments and security audits.

Kali Linux Installation

Start the VM and boot from the ISO.

- Follow the setup wizard:
  - Choose language, version, and activation options.
  - Partition the virtual disk and install.
- Complete initial setup, including setting a username and password.

Kali Linux : **https://www.kali.org/get-kali/#kali-platforms**

Pfsense as a firewall

pfSense is an open-source firewall and router software distribution based on FreeBSD. It's designed to be a powerful, flexible, and cost-effective solution for network security and management. pfSense can be installed on standard PC hardware, dedicated network appliances, or as a virtual machine

Go to the following link:

[pfSense CE Download] (**https://atxfiles.netgate.com/mirror/downloads/)**

Download link: **https://atxfiles.netgate.com/mirror/downloads/**

You can refer to following link for setup

https**://blog.davidvarghese.net/posts/building-home-lab-part-2/**

Network Topology For Home lab

To design network topology i am using cisco packet tracer

>> Open Cisco Packet tracer —→ login using your account

>> Devices we will have in our lab

- Pfsense (Firewall we will create Vlan using it)

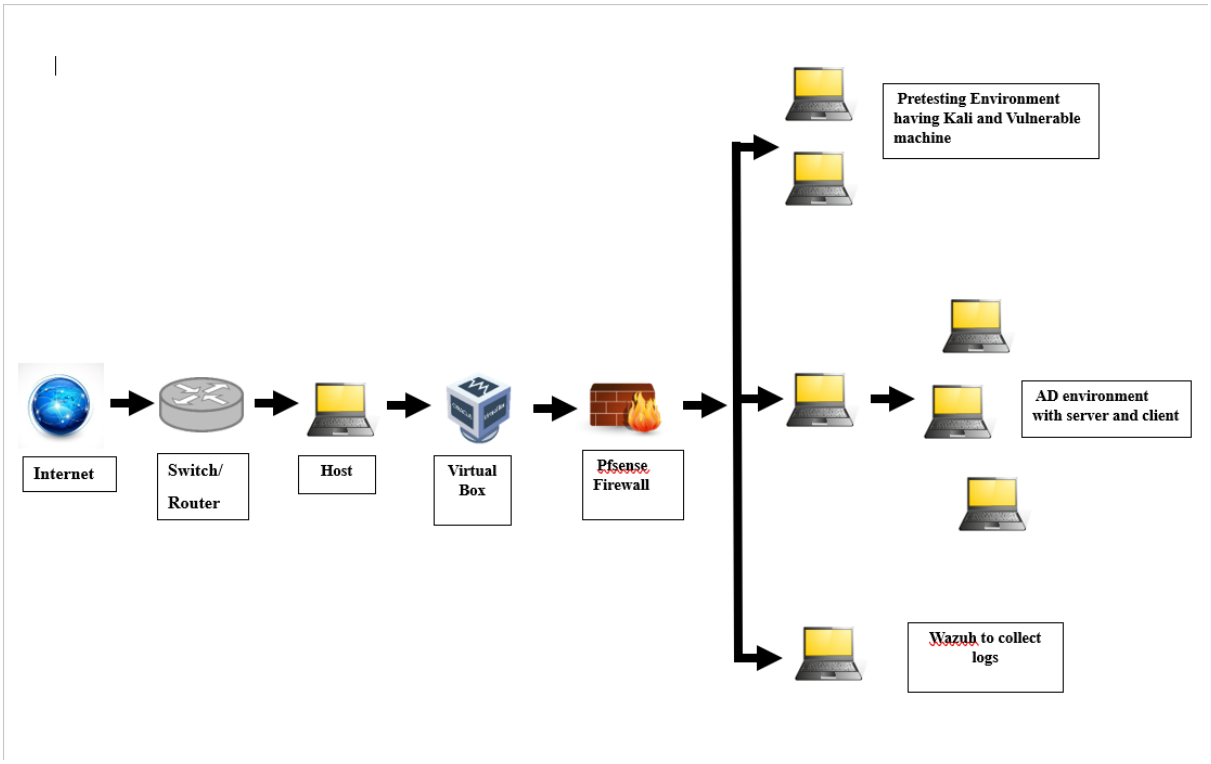
- Wazuh Server (TO monitoring the logs)

- Kali linux + Vulnerable machine (For testing)

- AD Server + AD Client (Active Directory)

>> Your Pfsense will give up an Ip address and design the ip according to the ip address given and Keep some Ip address to other Host and subnet Net

Network Topology



I am not adding Ip address in the diagram please use that you are selecting for your system

Here on words i am referring links and notes. I am not adding my personal steps because the errors and system specifications are different is based on system to system

To install Virtual box refer this (egnor the topology present here i am making different)

https://blog.davidvarghese.net/posts/building-home-lab-part-1/

To install pfsense and configuration

https://blog.davidvarghese.net/posts/building-home-lab-part-2/

use this once you installed all systems and installed in virtual box

https://blog.davidvarghese.net/posts/building-home-lab-part-4/

To kali linux

https://blog.davidvarghese.net/posts/building-home-lab-part-3/

For Active Directory

Here is my personal notes you can refer

here I am using windows 7, 10 and 11. Each has different privilege as a common company have

Windows 7 least privilege (such as employees in company)

Windows 10 mid privilege (such as team leader)

Windows 11 highest privilege (such as manager or boss)

Active Directory: https://repeated-mind-6c6.notion.site/Active-Directory-1aa4764998228001a681c71b2a7b1b7b?pvs=74

Here is the links

https://blog.davidvarghese.net/posts/building-home-lab-part-6/

https://blog.davidvarghese.net/posts/building-home-lab-part-7/

For metaspoitable

https://blog.davidvarghese.net/posts/building-home-lab-part-5/

For wazuh

https://www.notion.so/Wazuh-11247649982280ed9dc8e343796111d9?pvs=21

Download link

https://github.com/wazuh/wazuh-documentation/issues/309

or refer the links given here

https://www.linkedin.com/pulse/home-lab16-setting-up-wazuh-using-docker-home-lab-rajneesh-gupta-99qif/

https://medium.com/@halimaholaolohun/wazuh-homelab-setup-6a53d3b96524

Thank you so much!

— — — — — — — — — — — — !Happy Haccking!— — — — — — — — — — — — —