Cybersecurity Home Lab Project

Niña Jorene L. Montecer

November 2024

Project Description

This project aims to establish a foundational cybersecurity home lab with network setup and tool utilization using virtual machines with Linux operating systems allowing for simple experimentation with network security concepts, vulnerability assessment, and penetration testing.

Project Objectives

1. Setup a Virtual Environment
    a. Configure VMware Workstation to host Ubuntu and Kali Linux virtual machines
2. Install Essential Tools
    a. Install Nmap and Wireshark as part of the network security experimentation
3. Simulate Network Attacks and Defenses
4. Analyze Network traffic using Wireshark

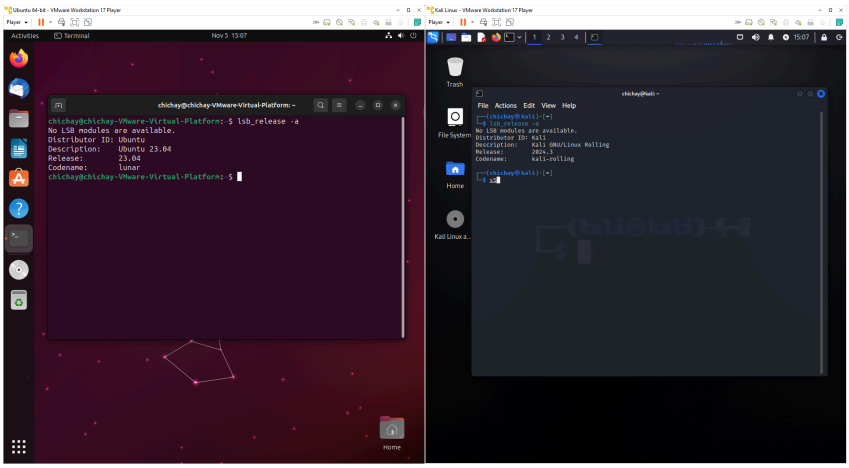
Project Methodology

1. Hardware and Software Requirements
    a. A personal computer or laptop
    b. VirtualBox or VMware Workstation Player
    c. Ubuntu and Kali Linux ISO images

2. Virtual Machine Setup
    a. Operating System

        Ubuntu 64-bit (Ubuntu)

        Debian 10.x 64-bit (Kali Linux)



b. Resource Allocation

Memory: 2GB

Processors: 2

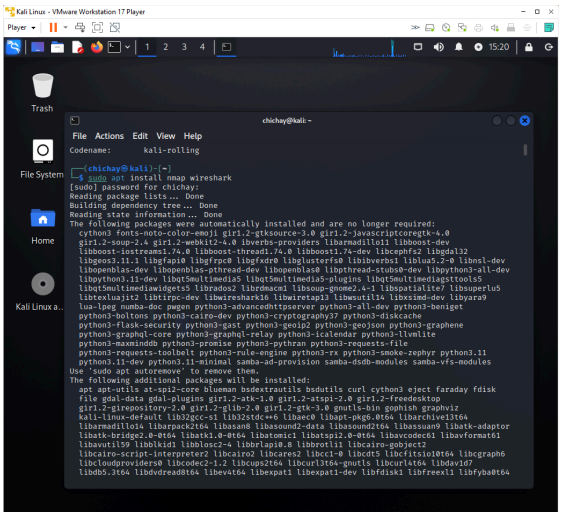
Hard Disk: 20GB

Network Adapter: NAT

3. Network Configuration
    a. NAT (Network Address Translation) network

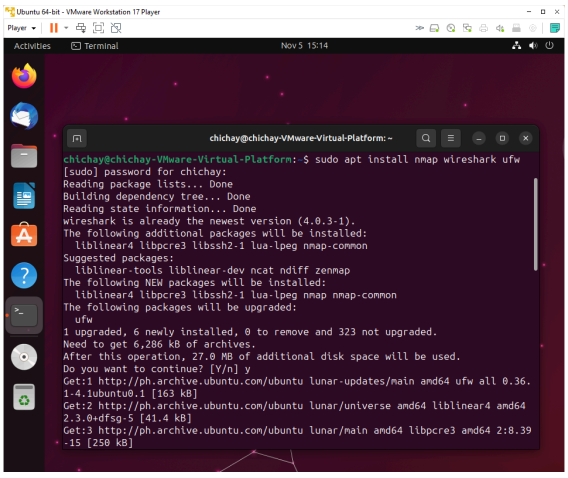
4. Tools Installation
    a. Kali Linux: Nmap, Wireshark

Command: `sudo apt install nmap wireshark`



b. Ubuntu: Nmap, Wireshark, UFW Firewall

Command: `sudo apt install nmap wireshark ufw`



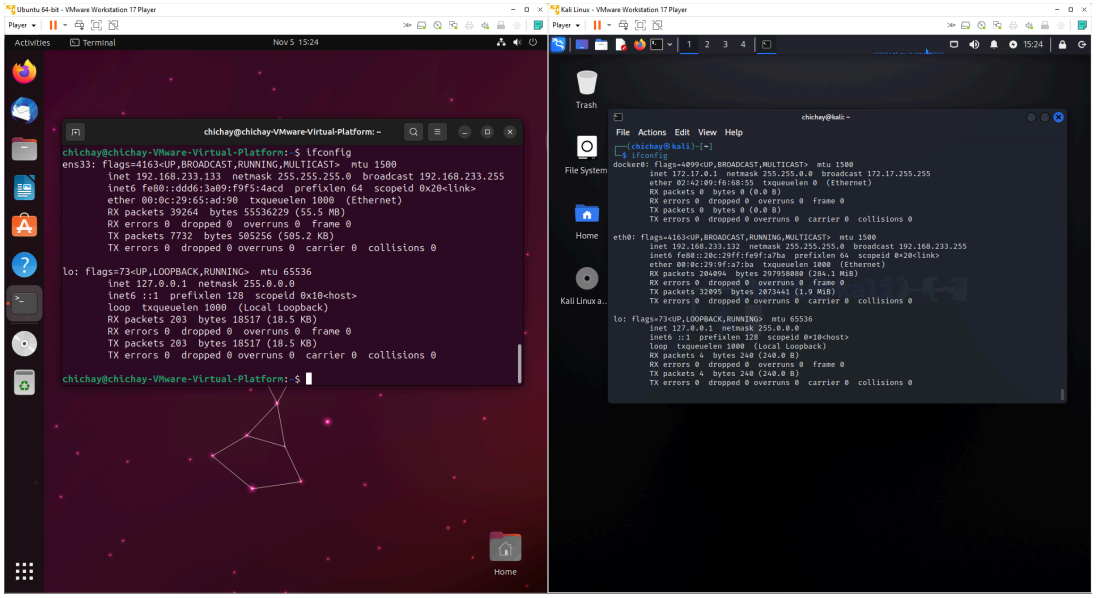
***Nmap**: discover devices and vulnerabilities on a network*

***Wireshark**: see and analyze network data*

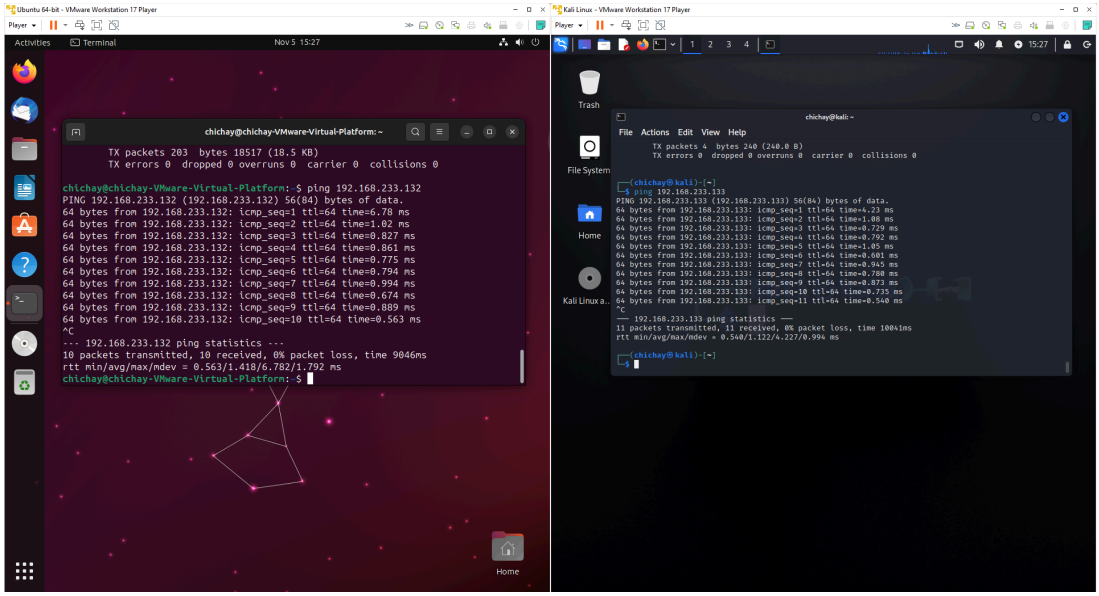
***UFW (Uncomplicated Firewall)**: manage network access and improve security on system*

5. Simulating Attacks and Defenses
    a. Determine IP address of both virtual machines and ping both machines to test connectivity and is reachable over the network

Command: `ifconfig`



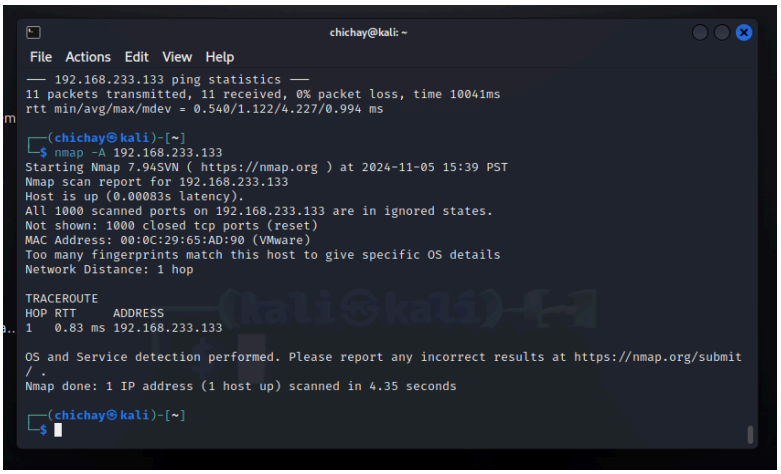
Command: `ping [target IP]`



b. Use Nmap to scan the Ubuntu VM for open ports and services (Simulated Attack)

Command: `nmap -A 192.168.233.133`

This command performs an aggressive scan on the target address providing detailed information on open ports and services.



c. Configure UFW on the Ubuntu VM to implement basic firewall rules and protect against attacks (Simulated Defense)

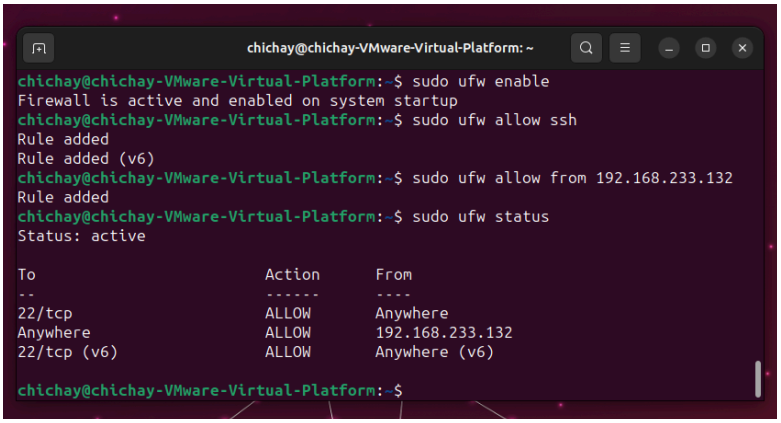
Commands:

`sudo ufw enable` activates firewall

`sudo ufw allow ssh` allow connections on port 22

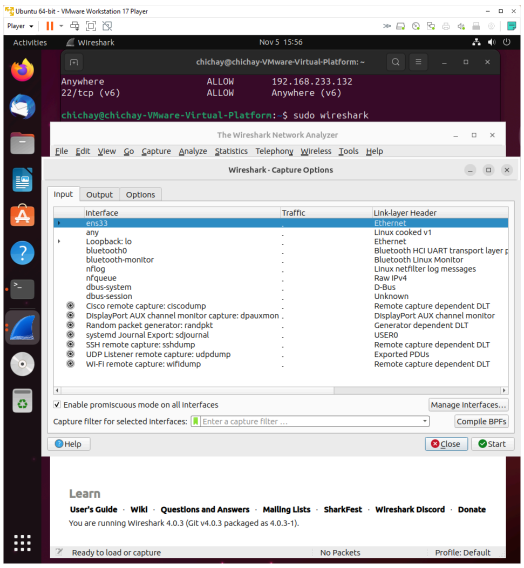
`sudo ufw allow from [specific IP]` allow specific traffic or grant access to trusted source

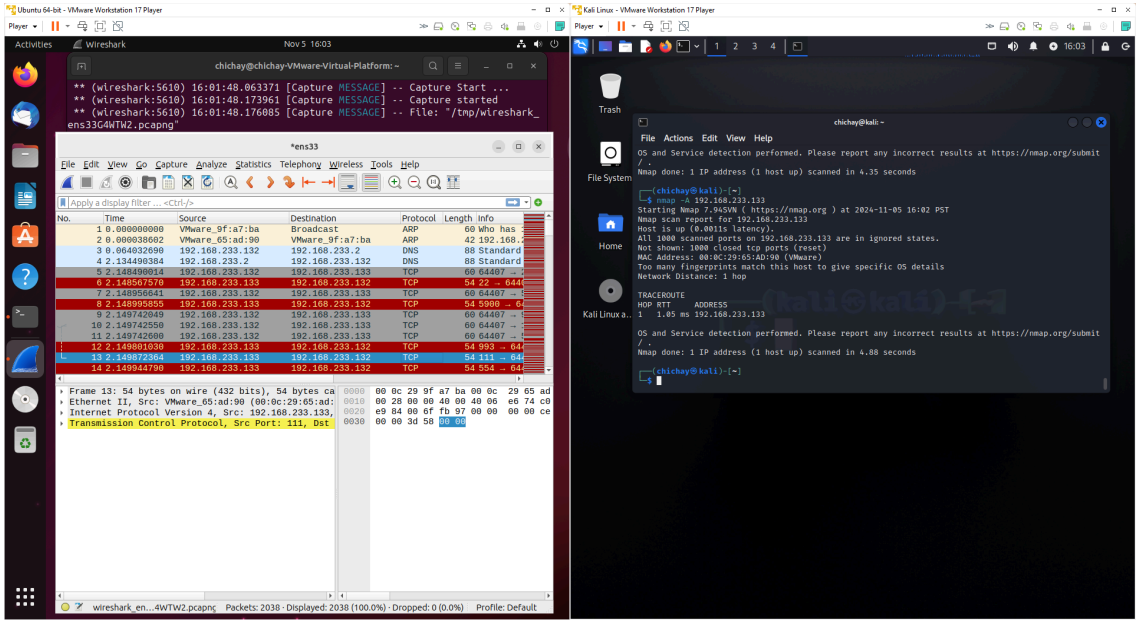
`sudo ufw status` display current status and other rules



6. Network Traffic Analysis

   a. Use Wireshark to capture network traffic coming into the Ubuntu VM in the Ethernet. Simulate the Nmap attack again to record on Wireshark

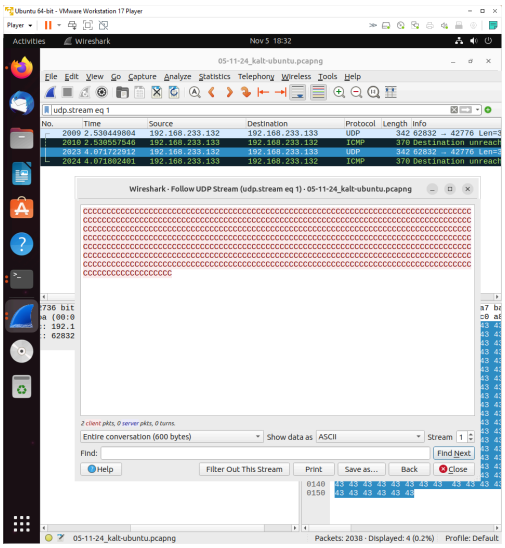




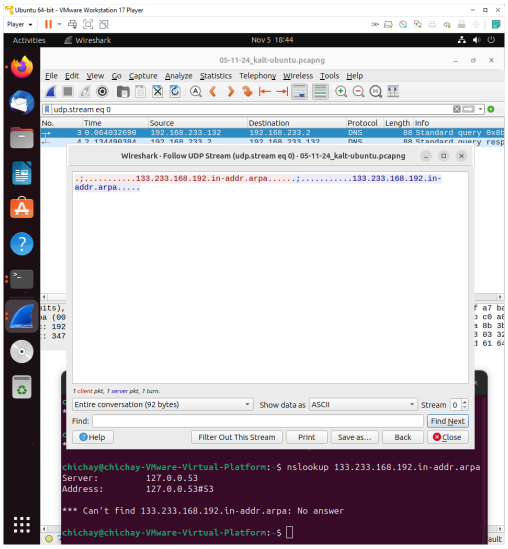
   b. Analyze the captured packets to identify attack patterns, vulnerabilities, and successful defense mechanisms.

Wireshark Captured Packets Analysis

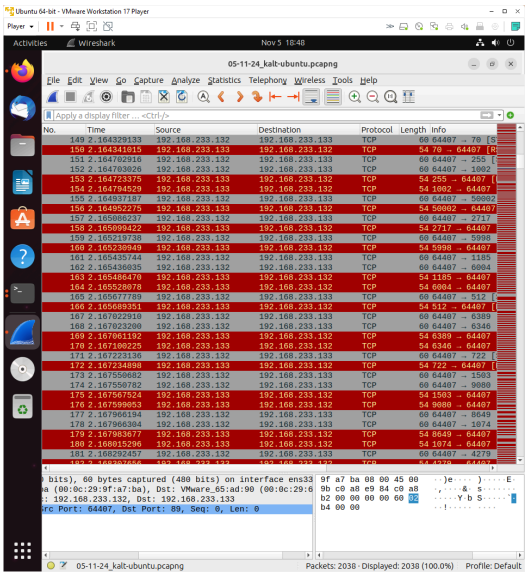
1. UDP Stream
    - During the analysis of a captured UDP stream, a significant amount of repetitive character data was identified. The sequence consists of a long repetition of the letter “C”.



2. DNS Stream
    - The following string was observed in the DNS traffic. The repetitive structure suggests a DNS query attempting to resolve the IP address back to a host name. Since the IP address is reversed, a reverse DNS lookup was performed using nslookup. However, it resulted in a “No answer”.

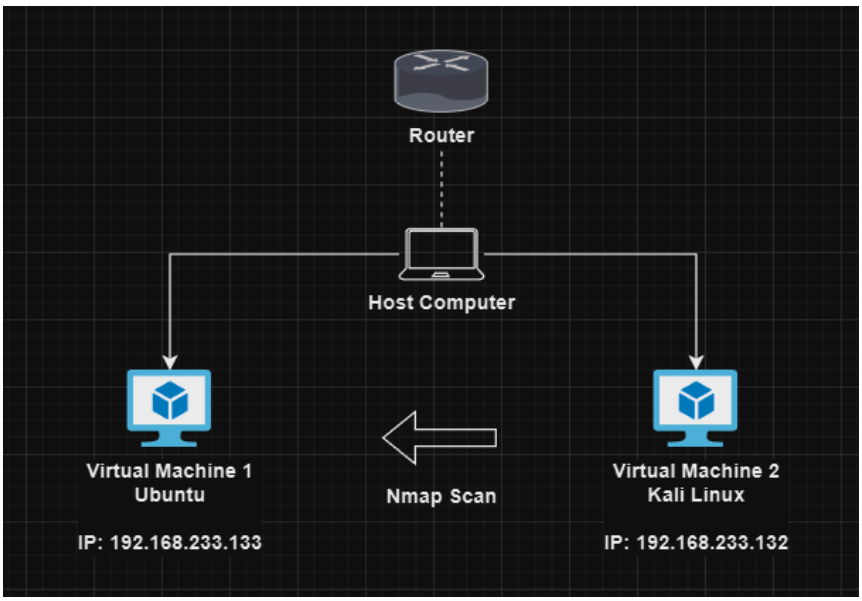


3. TCP Stream
    - Most of the packets captured by wireshark were TCP protocols. As per checking the stream, it does not contain any noteworthy contents.



4. Other protocols captured were ARP (Address Resolution Protocol), which facilitates local network communications through MAC addresses and ICMP (Internet Control Message Protocol), which aids in diagnosing network issues and errors with regards to packets.

Network Diagram



The diagram shows a home lab environment consisting of a router, a host computer, and two virtual machines.

Main Components:

Router

- The central device that connects all other components in the network.
- It facilitates communication between the host computer and the virtual machines.

Host Computer

- The physical computer where the virtual machines are running.
- It acts as the bridge between the physical network and the virtualized environment.

Virtual Machine 1 (Ubuntu)

- A virtual machine running the Ubuntu operating system.
- It serves as the target for network scans and potential attacks.

Virtual Machine 2 (Kali Linux)

- A virtual machine running the Kali Linux operating system.
- It is used to perform network scans, vulnerability assessments, and penetration testing on the Ubuntu VM.

Network Connections:

- The host computer is connected to the router via a wireless connection, as indicated by the dotted line.
- The virtual machines are isolated from the physical network and communicate with the external world through the host computer's network connection, using Network Address Translation (NAT).
- The router assigns IP addresses to all devices in the network, including the virtual machines.

Project Outcomes

1. A functional home lab environment for cybersecurity practice.
2. Basic hands-on experience with network scanning, vulnerability assessment, and penetration testing.
3. Understanding of basic network defense mechanisms and firewall configuration.
4. Ability to analyze network traffic and identify potential threats.

Recommendations for Improvements

- Expand the lab by adding more virtual machines to simulate complex network topologies.
- Provide more In-depth analysis of project outcomes.
- Explore advanced penetration testing techniques and exploit development.
- Explore more security tools already present in Kali Linux.