LIGHTHOUSE LAB

CYBERSECURITY

NETWORK ADMINISTRATION PROJECT

DANIEL D. OLUWAYALE

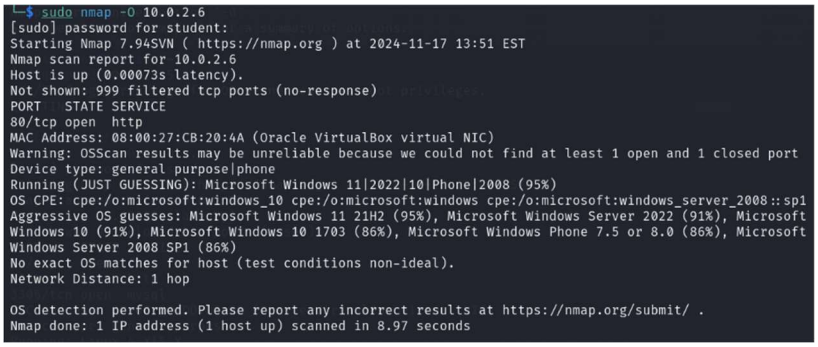
Table of Content

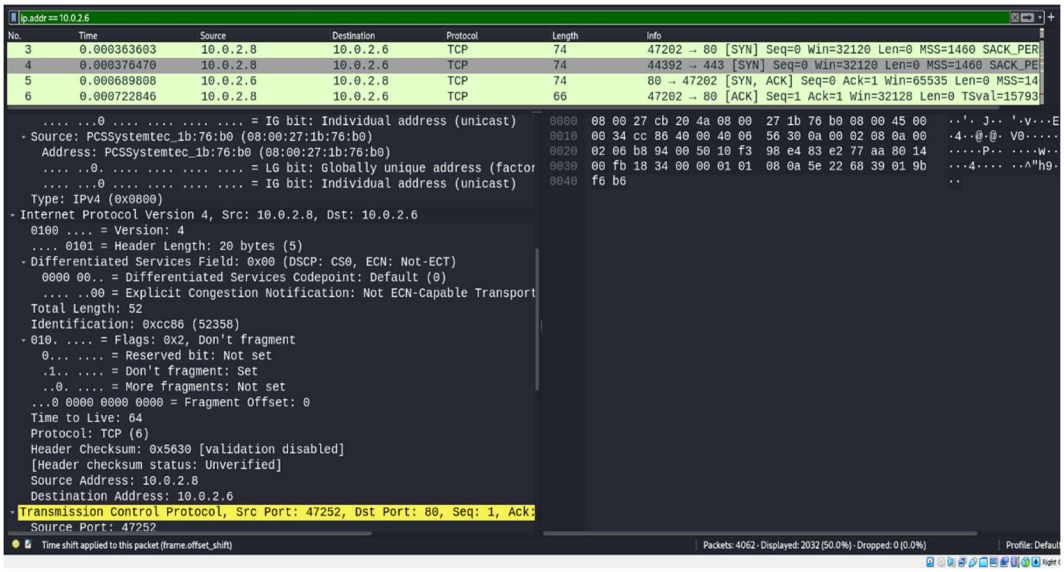
Introduction

As the digital landscape evolves, securing virtualized environments has become a critical concern for organizations and individuals alike. Virtual machines (VMs) provide an efficient means of isolating workloads and testing various configurations, but they also introduce unique security challenges that require careful consideration. This report presents an analysis of the details of two virtual machines: one running Windows 11 and the other running a Linux-based operating system and captured network packets from the source device which the Kali OpenVAS VM.

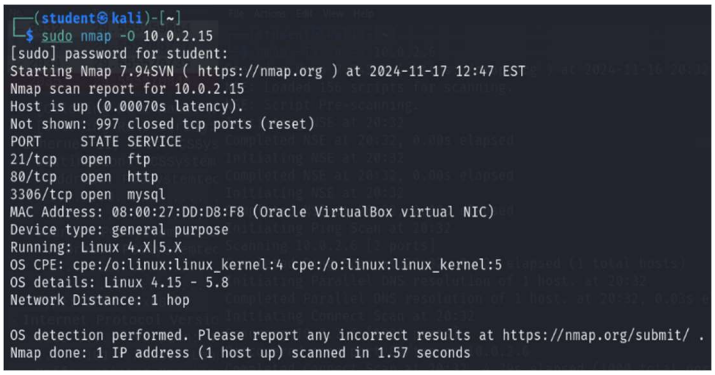
Network Device Information

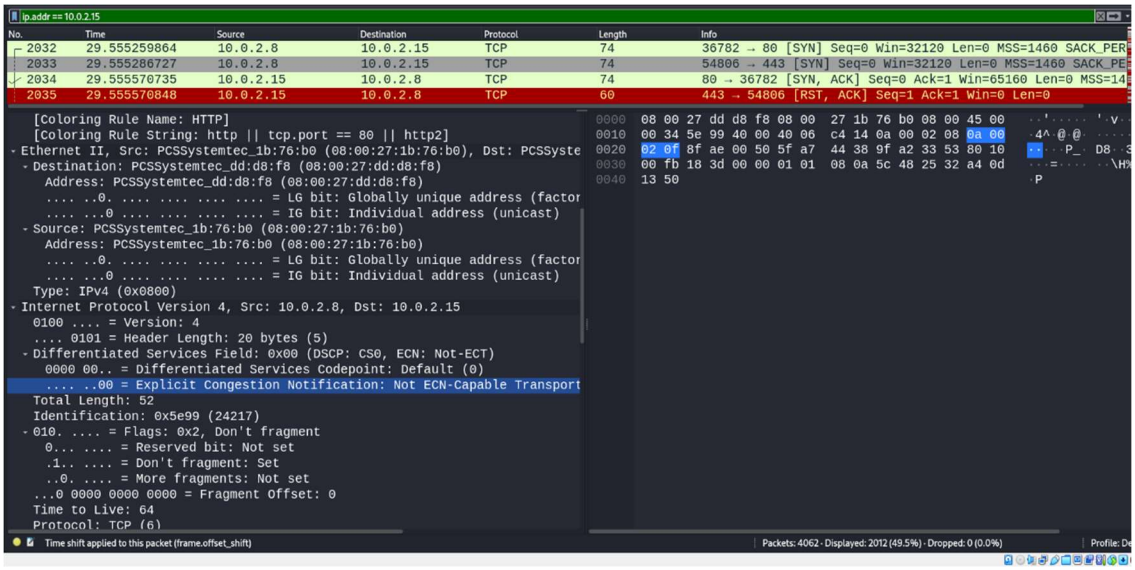
1. Windows11 Machine
    - Machine Designation – Windows11
    - Device Host Name - windows11-deskt:2321
    - IP address – 10.0.2.6. This was found in the IPV4 header
    - MAC address – 08-00-27-CB-20-4A. This was found in the ethernet header
    - Operating System & version – Windows11 (flag -O with the Nmap command)
    - Open ports with associated services – 80/tcp; Service – http (Nmap command). This was found in the TCP header
    - ARP Ping Scan elapsed time – 8.97s





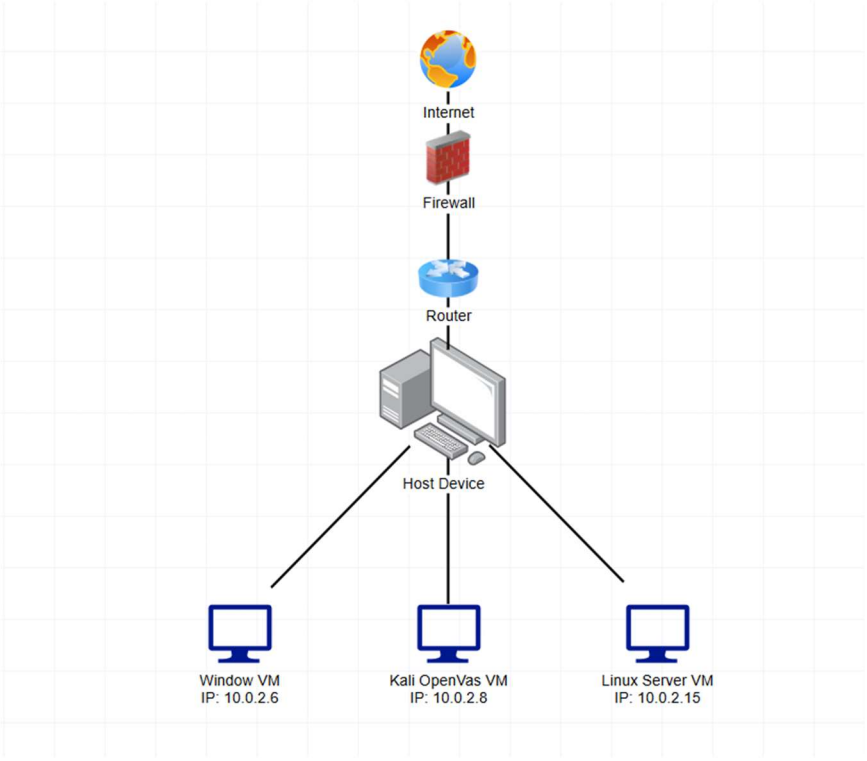
2. Linux Virtual Machine
   - Machine Designation – Linux Server
   - Device Host Name - Linux server
   - IP address – 10.0.2.15. This was found in the IPV4 header
   - MAC address – 08:00:27:dd:d8:f8. This was found in the ethernet header
   - Operating System & version – Linux 4.15 – 5.8 (flag -O with the Nmap command)
   - Open ports with associated services (Nmap command). These were found the TCP header
     - 21/tcp; Service – ftp
     - 80/tcp; Service – http
     - 3306/tcp; Service - MySQL
   - ARP Ping Scan elapsed time – 1.57s





3. **Information Collection Methodology**

   To get the details and information of the devices, I had the three VMs (Windows 11, Linux Server and Kali OpenVAS) running and opened the Wireshark on the Kali VM to capture network traffic. I ran the intense Nmap command on the Kali VM for each of the other VMs which produced an outcome each which includes the details of the devices. Above are the screenshots to confirm the procedure.



Reference

Gordon, F. (n.d.). *Nmap examples*. Nmap.org. Retrieved November 20, 2024, from https://nmap.org/book/man-examples.html

Wireshark Foundation. (n.d.). *Wireshark*. Wireshark.org. Retrieved November 20, 2024, from https://www.wireshark.org/

diagrams.net. (n.d.). *diagrams.net*. diagrams.net. Retrieved November 20, 2024, from https://app.diagrams.net/