

LIGHTHOUSE LAB
CYBERSECURITY
NETWORK ADMINISTRATION PROJECT
DANIEL D. OLUWAYALE

Table of Content

- Introduction section
- Network Devices Information
- Information Collection Methodology
- References and Citation

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.

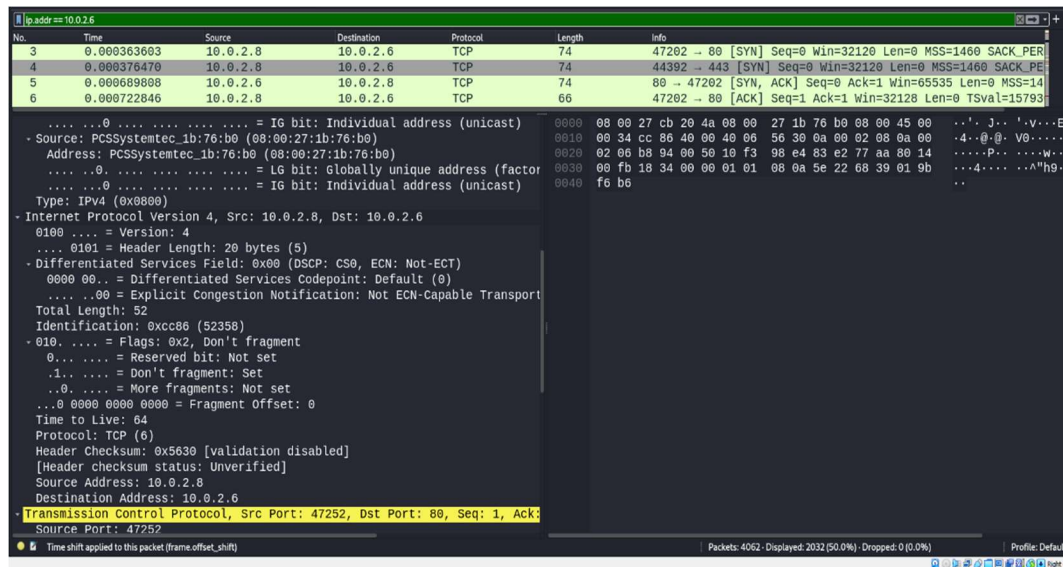
Network Device Information

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

```
L$ sudo nmap -O 10.0.2.6
[sudo] password for student:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-17 13:51 EST
Nmap scan report for 10.0.2.6
Host is up (0.00073s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 08:00:27:CB:20:4A (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|phone
Running (JUST GUESSING): Microsoft Windows 11|2022|10|Phone|2008 (95%)
OS CPE: cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_server_2008::sp1
Aggressive OS guesses: Microsoft Windows 11 21H2 (95%), Microsoft Windows Server 2022 (91%), Microsoft
Windows 10 (91%), Microsoft Windows 10 1703 (86%), Microsoft Windows Phone 7.5 or 8.0 (86%), Microsoft
Windows Server 2008 SP1 (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.97 seconds
```

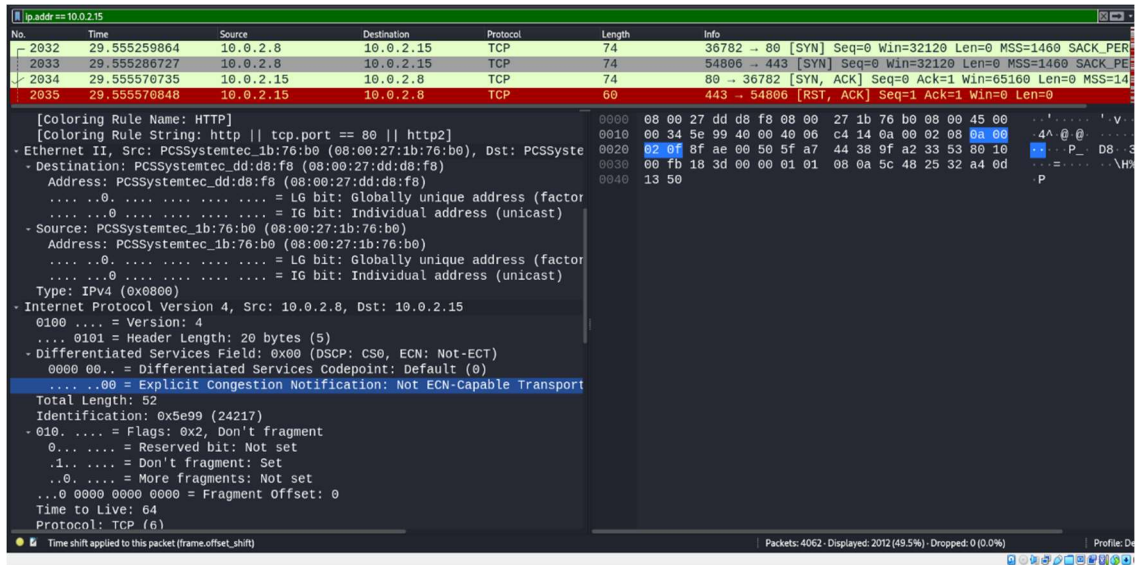


2. Linux Virtual Machine

- 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

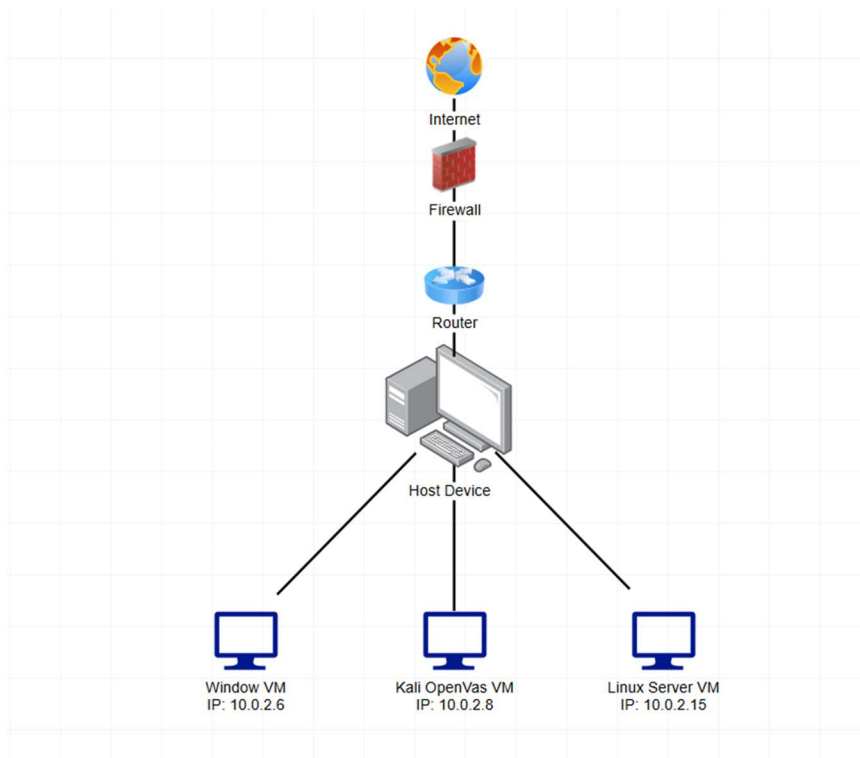
```
(student@kali)-[~]
$ sudo nmap -O 10.0.2.15
[sudo] password for student:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-17 12:47 EST
Nmap scan report for 10.0.2.15
Host is up (0.00070s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
3306/tcp  open  mysql
MAC Address: 08:00:27:DD:D8:F8 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 1.57 seconds
```



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/>