MODULE 6 - TASK 7 & 8 REPORT

# Task 7: Scan Network Devices using Nmap and Zenmap

This task involved using Nmap (CLI) and Zenmap (GUI) to scan all devices connected to the local network.

The `nmap -sn 10.0.2.15/24` command was used to perform a ping scan across the local subnet. This identified live hosts on the network, along with their IP and MAC addresses.

Zenmap was also used with the 'Intense Scan' profile to scan the same subnet. This provided more detailed information such as open ports, services running, and device operating systems.

Sample commands used:

nmap -sn 10.0.2.15/24

nmap -T4 -A -v 192.168.0.0/24

Screenshots were taken showing the terminal output of Nmap and the results window of Zenmap.

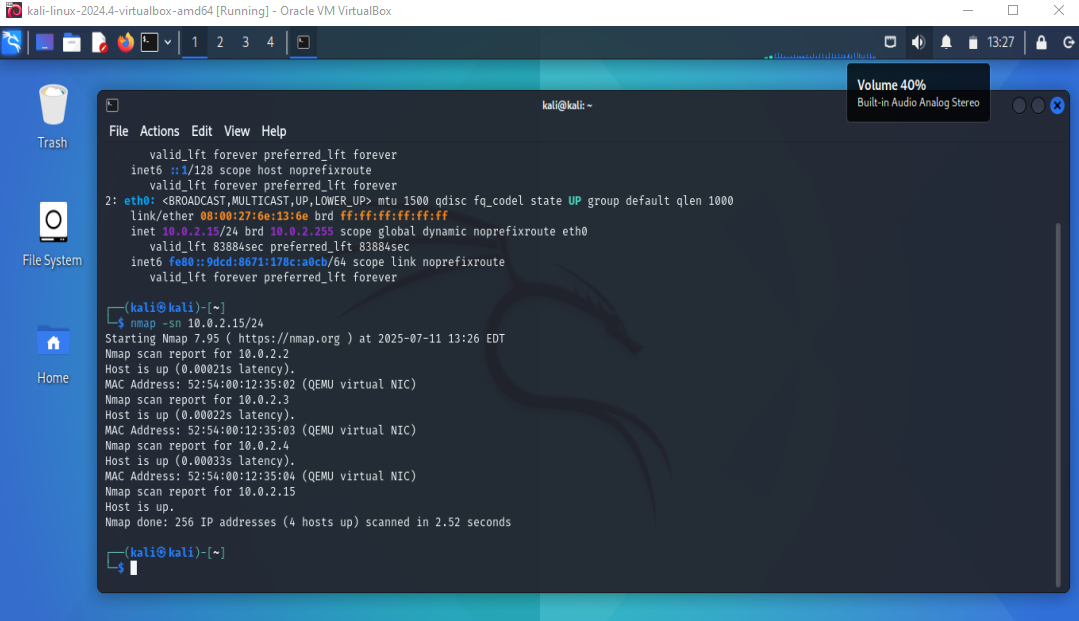


Fig 1: Terminal output of Nmap

# 

Fig 2: Terminal output of Zenmap

# Task 8: Wireshark Basics and HTTP Packet Filtering

In this task, Wireshark was used to capture network traffic. The goal was to filter HTTP packets and understand basic packet structure.

An HTTP-based website (e.g., http://neverssl.com) was visited during the capture to generate visible HTTP traffic, which could then be filtered using the Wireshark filtering feature.

Filters applied during this task included:

1. http

2. tcp.port == 80

3. ip.addr == 192.168.0.1

Screenshots were captured for each of the filters above, displaying packet-level details including source and destination IPs, ports, and HTTP headers.

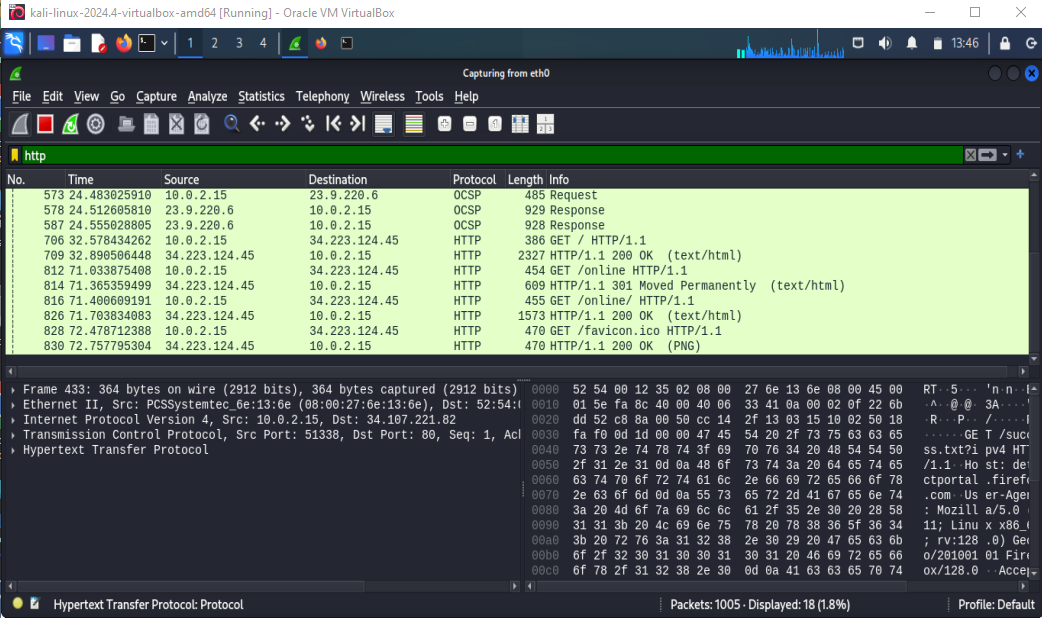


Fig 3: Screenshot of Applied http filter

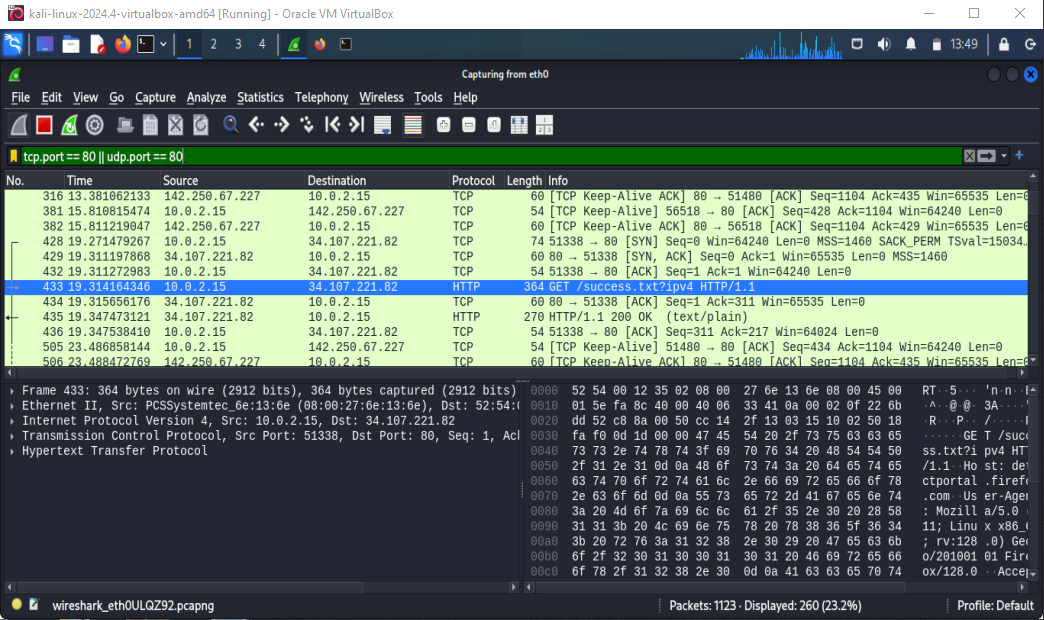


Fig 4: Screenshot of Applied tcp.port == 80 filter

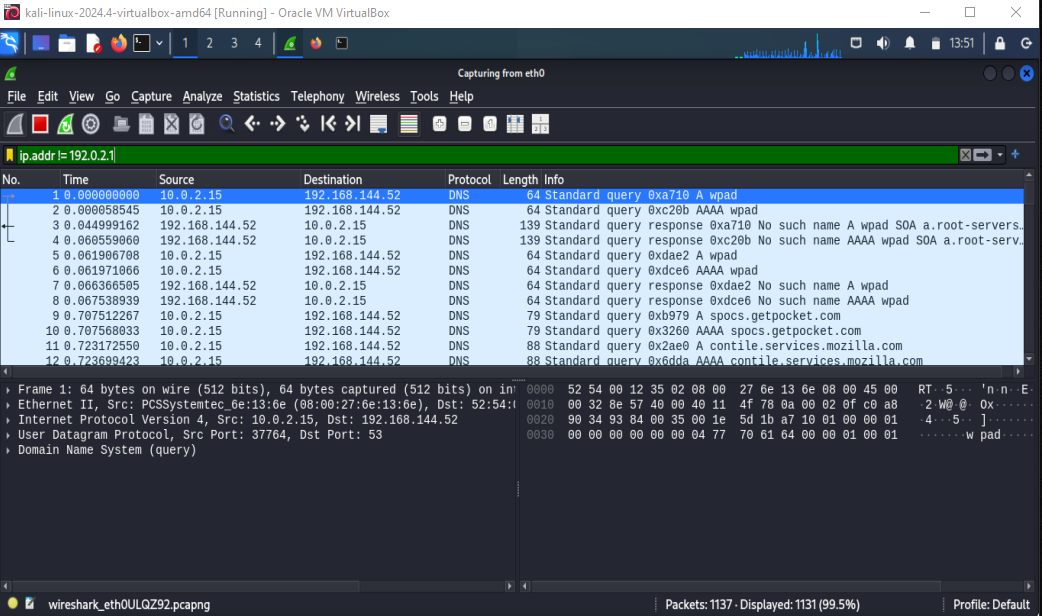


Fig 5: Screenshot of Applied ip.addr == 192.168.0.1 Filter