|  |
| --- |
|  |
| Wi-Fi Network Scanning & Vulnerability Check Report |
| Task 3 |

|  |
| --- |
| Jeffery Tetteyfio  4-23-2025 |

Contents

[**1.** **Introduction** 2](#_Toc196367615)

[**2. Tools Used** 2](#_Toc196367616)

[**3. Testing Procedure** 2](#_Toc196367617)

[**4. Findings** 4](#_Toc196367618)

[**5. Recommendations** 4](#_Toc196367619)

[**6. Conclusion** 4](#_Toc196367620)

[**7.Screenshots** 5](#_Toc196367621)

## **Introduction**

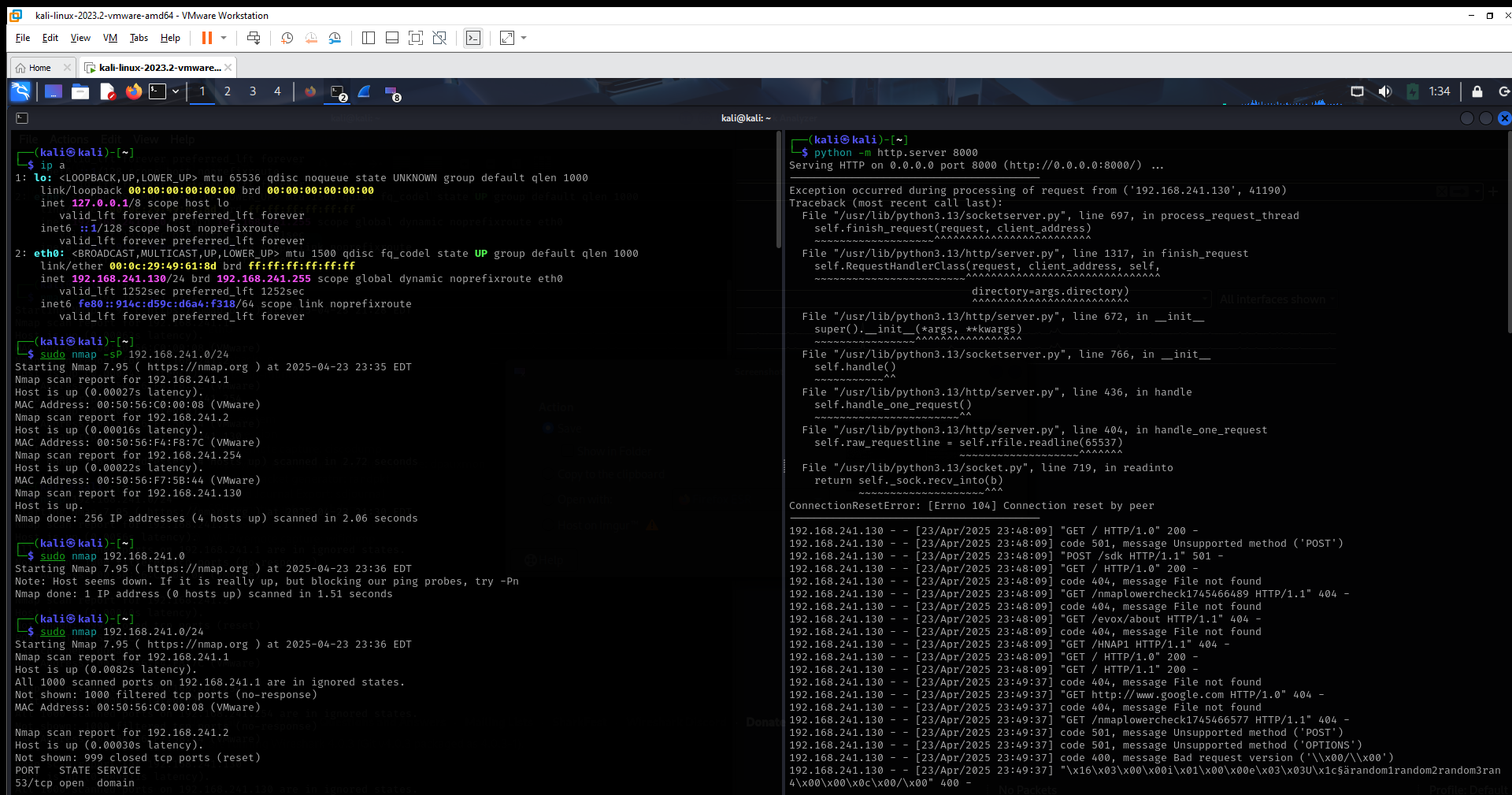
The purpose of this assessment was to evaluate the security of the local Wi-Fi network by identifying potential vulnerabilities. Nmap was utilized to gather information about connected devices and their services.

## **Tools Used**

| **Tool** | **Purpose** |
| --- | --- |
| Nmap | For network scanning and service version detection |
| Kali Linux | The operating system used to run the tools |
| Python HTTP Server – to simulate a web service | To simulate a web service |

## **3. Testing Procedure**

**Identifying Network Interfaces and Local IP**

* Ran **ip a** in the terminal to find my local IP address and active network interface (eth0).
* My local IP was 192.168.241.130, and the router was 192.168.241.2

**Scanning the Network with Nmap**

* To detect all devices on the network:

**nmap -sn 192.168.241.0/24**

* This identified all active devices along with their MAC addresses.

**Checking for Open Ports and Services**

* To check open ports and services running on a specific host:

**sudo nmap -sV 192.168.241.2**

* Result: Port 53/tcp was open for DNS service.

**Detecting Operating Systems and Versions**

* Used aggressive OS detection to identify system versions:

**sudo nmap -O 192.168.241.2**

* Gathered details on the type of devices and OS in the network.

**Setting up a Python HTTP Server**

* Created a temporary server to simulate a web service:

**python3 -m http.server 8000**

* Attempted to connect and capture logs from other devices scanning or accessing the service.

## **4. Findings**

* Devices discovered using their MAC addresses and IPs.
* Router had common ports open (DNS - port 53).
* Most devices were fingerprinted successfully, showing their OS and vendor info.
* The Python HTTP server received connection attempts, confirming its visibility on the network.

## **5. Recommendations**

* Change router default credentials.
* Close unused ports through router configuration.
* Enable MAC filtering to allow only known devices.
* Routinely scan network for unknown devices and monitor traffic.

## **6. Conclusion**

This task provided practical experience in identifying devices, scanning for open ports, analyzing operating systems, and simulating network services. It improved my skills in using Nmap, understanding how networks are structured, and reinforced the importance of securing Wi-Fi environments.

## **7. Screenshots**

