TASK - 3

Wi-Fi Security Assessment Report

1. Introduction This report presents the findings of a security assessment conducted on a home Wi-Fi network. The objective was to identify vulnerabilities, such as weak passwords, open ports, and unauthorized devices, and to recommend measures for improving network security.

2. Objectives

- Evaluate the security of the home Wi-Fi network.
- Identify weak passwords, open ports, and unauthorized devices.
- Assess Wi-Fi encryption and security configurations.
- Provide actionable recommendations to enhance security.

3. Tools Used

- **Wireshark**: Network protocol analyzer used to monitor and analyze traffic.
- **Aircrack-ng**: Toolset for assessing Wi-Fi encryption security.
- **Nmap**: Network scanning tool used to identify open ports and connected devices.

4. Methodology

- **Network Scanning**: Used Nmap to detect open ports and connected devices.
- **Traffic Analysis**: Used Wireshark to monitor network packets for any suspicious activity.
- **Wi-Fi Encryption Testing**: Used Aircrack-ng to check the strength of Wi-Fi encryption.
- **Password Strength Assessment**: Tested for weak or default passwords.

5. Results & Analysis

- **Password Strength**: The network was found to be using **[medium]** passwords.
- **Wi-Fi Encryption**: The network was secured using **[WPA2/WPA3/]**, which is **[secure]**.
- **Open Ports**: **[80,85]** open ports were detected, posing a **[medium/high]** security risk.

- **Unauthorized Devices**: **[2]** unknown devices were detected on the network.
- **Traffic Anomalies**: No suspicious activity was found **[or]** anomalous traffic patterns were identified, indicating a potential security risk.

6. Recommendations

- Use a strong, complex Wi-Fi password with at least 12 characters.
- Upgrade to WPA3 encryption if available.
- Close unnecessary open ports and restrict access where possible.
- Regularly check for unauthorized devices and remove them.
- Enable MAC address filtering for better access control.
- Disable WPS (Wi-Fi Protected Setup) to prevent brute-force attacks.
- Keep router firmware updated to patch security vulnerabilities.

7. Conclusion The security assessment revealed that there were vulnerable in the home Wi-Fi network. By implementing the recommended security measures, the network's resilience against potential attacks can be significantly improved.