Module 11

Wi-Fi Network Security Assessment

Assignment : Wi-Fi Network Security Assessment and Hardening

Project Description:

In this project, students will conduct a comprehensive security assessment of a Wi-Fi network, identify vulnerabilities, and implement security measures to harden the network. The project will provide practical experience in understanding and securing wireless networks.

Project Components:

Select a Target Wi-Fi Network:

Choose a Wi-Fi network for assessment and hardening. It can be a home network, a small business network, or a network within a controlled lab environment.

Wireless Network Assessment:

Conduct an initial assessment of the selected Wi-Fi network to understand its configuration, encryption methods, and potential security risks.
Identify the types of devices connected to the network.

Wireless Network Attack Vectors:

Review and discuss different attack vectors that can be used against wireless networks, including eavesdropping, deauthentication attacks, and rogue APs.

WPA2 Pen Testing:

Utilize tools like FERN to perform penetration testing on the target Wi-Fi network secured with WPA2 encryption.
Document and analyze the results of the penetration test.

Hands-On Wi-Fi Auditing:

Demonstrate how to use whoisonmywifi to gather information about nearby Wi-Fi networks and connected devices and detecting unauthorized devices.

Security Tools and Countermeasures:

Introduce students to wireless network security tools and countermeasures, such as intrusion detection systems, wireless intrusion prevention systems, and VPNs.
Explain how these tools can enhance Wi-Fi security.

Wi-Fi Hardening Plan:

Have students create a comprehensive Wi-Fi network hardening plan based on their findings from the assessment.
Include recommendations for improving encryption, access control, and network segmentation.

Implement Security Measures:

Implement the security measures outlined in the Wi-Fi hardening plan within the target network.
Configure stronger encryption, change default passwords, and implement access controls.

Documentation:

Maintain documentation of the Wi-Fi network assessment, hardening plan, and the changes made to the network.

Reporting:

Create a detailed report summarizing the Wi-Fi network assessment process, vulnerabilities discovered, and the implementation of security measures.
Provide a risk assessment and priority ranking for vulnerabilities.

Presentation:

The students must present their findings, Wi-Fi hardening plan, and recommendations to the class.

Discuss the significance of Wi-Fi security in safeguarding data and privacy.

Project Benefits:

- Provides hands-on experience in assessing and securing Wi-Fi networks.
- Reinforces knowledge of wireless network concepts and encryption.
- Encourages responsible network hardening practices to protect against wireless attacks.
- Emphasizes the importance of securing Wi-Fi networks in both home and business environments.

This project allows students to apply their knowledge of Wi-Fi network security in a practical context, helping them gain valuable skills in assessing and hardening wireless networks against potential threats and attacks.