Wireless Attacks and Countermeasures

Estimated Time: 25 minutes
Number of Team Members: Students will work in teams of two.

Objective

In this lab, students will gain an understanding of the primary attack methods used to bypass conventional security measures on WLANs. Additionally, students will learn the countermeasures that can be implemented for security on a WLAN.

Scenario

Network security is the process by which digital information assets are protected. The goals of security are to maintain integrity, protect confidentiality, and assure availability.

This lab will focus on understanding wireless security concepts.

Preparation

The students will require access to the Internet for online research.

Tools and Resources

Each student team needs one PC with Internet access.

Step 1 Network security goals

Answer the following questions:

1. List the three primary goals of network security covered in FWL Module 8.

_____

_____

_____

2. Which of the goals refers to the assurance that data is not altered or destroyed?

_____

3. Which of the goals refers to the protection of data from unauthorized disclosure?

_____

4. Which of the goals refers to the continuous operation of the computing system?

_____

Step 2 Network security weaknesses

Answer the following questions:

a. List the three primary network security weaknesses covered in FWL Module 8.

_____

_____

_____

b. Which of the weaknesses refers to a lack of a written security policy?

_____

c. Which of the weaknesses refers to unsecured default settings?

_____

d. Which of the weaknesses refers to weak initialization vector, poor encryption and authentication schemes, and firewall holes?

_____

Step 3 Network security threats

Answer the following questions:

a. List the four basic network security threats covered in FWL Module 8.

_____

_____

_____

_____

Step 4 Attack methods

Answer the following questions:

a. List the three primary attack methods covered in FWL Module 8.

_____

_____

_____

b. Which of the attacks is occurring when the attacker now controls one system and can either deface the public Web presence or continue hacking for more interesting information?

_____

c. How is this attack performed? What tools are available?

_____

_____

_____

d. Which of the attacks is occurring when the attack results in obtaining address ranges, hosts, and services? In this case, the known servers and the firewall may or may not be detected.

e. How is this attack performed? What tools are available?

f. Which of the attacks is occurring when the attacker has disabled valid users from accessing the target network causing lost revenue, lost communications, and damaged software and hardware?

g. How is this attack performed? What tools are available?

Step 5 The security wheel

Answer the following questions:

a. List the four processes involved in building a secure network.

b. Which of the processes involve collecting and analyzing information from the monitoring and testing phases to make security improvements?

c. Which of the processes involve monitoring the network for violations and attacks against the corporate security policy?

d. Which of the processes involve testing the effectiveness of the security safeguards in place?

e. Which of the processes involve implementing security devices, which include firewalls, identification authentication systems, and virtual private networks?

f. What is at the center of the Wireless Security Wheel?

_____

Step 6 WLAN security technologies

Answer the following questions:

a. List the two first-generation security technologies covered in FWL Module 8.

_____

_____

b. Name the one that serves to logically segment the users and APs that form part of a wireless subsystem.

_____

c. Name the other that replaces the original data payload with the output of the encryption algorithm.

_____

d. What are the two types of authentication methods defined in IEEE 802.11?

_____

_____

e. What are the three elements of the association process?

_____

_____

_____

