Chapter 1 Lab A: Researching Network Attacks and Security Audit Tools

Objectives

Part 1: Researching Network Attacks

- Research network attacks that have occurred.
- Select a network attack and develop a report for presentation to the class.

Part 2: Researching Security Audit Tools

- Research network security audit tools.
- Select a tool and develop a report for presentation to the class.

Background/Scenario

Network attacks have resulted in the loss of sensitive data and significant network downtime. When a network or the resources in it are inaccessible, worker productivity can suffer, and business income may be lost.

Attackers have developed many tools over the years to attack and compromise the networks of organizations. These attacks take many forms, but in most cases, they seek to obtain sensitive information, destroy resources, or deny legitimate users access to resources.

To understand how to defend a network against attacks, an administrator must first identify network vulnerabilities. Specialized security audit software developed by equipment and software manufacturers can be used to help identify potential weaknesses. In addition, the same tools used by attackers can be used to test the ability of a network to mitigate an attack. After the vulnerabilities are known, steps can be taken to help mitigate the network attacks.

This lab provides a structured research project that is divided into two parts: Researching Network Attacks and Researching Security Audit Tools. You can elect to perform Part 1, Part 2, or both. Let your instructor know what you plan to do so to ensure that a variety of network attacks and vulnerability tools are reported on by the members of the class.

In Part 1, you research various network attacks that have actually occurred. You select one of these and describe how the attack was perpetrated and how extensive the network outage or damage was. You also investigate how the attack could have been mitigated or what mitigation techniques might have been implemented to prevent future attacks. You prepare a report based on a predefined form included in the lab.

In Part 2, you research network security audit tools and investigate one that can be used to identify host or network device vulnerabilities. You create a one-page summary of the tool based on a predefined form included in the lab. You prepare a short (5–10 minute) presentation to present to the class.

You may work in teams of two with one person reporting on the network attack and the other reporting on the security audit tools. Each team member delivers a short overview (5–10 minutes) of their findings. You can use live demonstrations or PowerPoint to summarize your findings.

Required Resources

- Computer with Internet access for research.
- Presentation computer with PowerPoint or other presentation software installed.
- Video projector and screen for demonstrations and presentations.

Part 1. Researching Network Attacks

In Part 1 of this lab, you research various network attacks that have actually occurred and select one on which to report. Fill in the form below based on your findings.

Step 1: Research various network attacks.

List some of the attacks you identified in your search.

_____
_____
_____

Step 2: Fill in the following form for the network attack selected.

Name of attack:	
Type of attack:	
Dates of attacks:	
Computers / Organizations affected:	
How it works and what it did:	

Mitigation options:
References and info links:
Presentation support graphics (include PowerPoint filename or web links):

Part 2. Researching Security Audit Tools

In Part 2 of this lab, you research network security audit tools and attacker tools and investigate one that can be used to identify host or network device vulnerabilities. Fill in the report below based on your findings.

Step 1: Research various security audit and network attack tools.

List some of the tools that you identified in your search.

_____
_____
_____

Step 2: Fill in the following form for the security audit or network attack tool selected.

Name of tool:	
Developer:	
Type of tool (character-based or GUI):	
Used on (network device or computer host):	
Cost:	
Description of key features and capabilities of product or tool:	

References and info links:
Presentation support graphics:

Step 3: Reflection

a. What is the prevalence of network attacks and what is their impact on an organization's operation? What are some key steps organizations can take to help protect their networks and resources?

_____
_____
_____
_____
_____

b. Have you actually worked for an organization or know of one where the network was compromised? If so, what was the impact to the organization and what did they do about it?

_____
_____
_____

c. What steps can you take to protect your own PC or laptop computer?

_____
_____
_____