Lab - Researching Network Attacks and Security Audit Tools/Attack 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 Network Security Audit Tools and Attack Tools

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

Background / Scenario

Attackers have developed many tools over the years to attack and compromise networks. These attacks take many forms, but in most cases, they seek to obtain sensitive information, destroy resources, or deny legitimate users access to resources. When network resources are inaccessible, worker productivity can suffer, and business income may be lost.

To understand how to defend a network against attacks, an administrator must identify network vulnerabilities. Specialized security audit software, developed by equipment and software manufacturers, can be used to help identify potential weaknesses. These same tools used by individuals to attack networks can also be used by network professionals to test the ability of a network to mitigate an attack. After the vulnerabilities are discovered, steps can be taken to help protect the network.

This lab provides a structured research project that is divided into two parts: Researching Network Attacks and Researching Security Audit Tools. Inform your instructor about which network attack(s) and network security audit tool(s) you have chosen to research. This will ensure that a variety of network attacks and vulnerability tools are reported on by the members of the class.

In Part 1, research network attacks that have actually occurred. Select one of these attacks and describe how the attack was perpetrated and the extent of the network outage or damage. Next, investigate how the attack could have been mitigated, or what mitigation techniques might have been implemented to prevent future attacks. Finally, prepare a report based on the form included in this lab.

In Part 2, research network security audit tools and attack tools. Investigate one that can be used to identify host or network device vulnerabilities. Create a one-page summary of the tool based on the form included within this lab. Prepare a short (5–10 minute) presentation to give to the class.

You may work in teams of two, with one person reporting on the network attack and the other reporting on the tools. All team members deliver a short overview 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 will research real network attacks 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 Network Security Audit Tools and Attack Tools

In Part 2 of this lab, research network security audit tools and attack tools. 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 network security audit tools and attack tools.

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

Step 2: Fill in the following form for the network security audit tool/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:

Reflection

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

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

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