CCNA Security

Lab - Researching Network Attacks and Security Audit Tools/Attack Tools (Instructor Version)

Instructor Note: Red font color or Gray highlights indicate text that appears in the instructor copy only.

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

Instructor Note: If desired, you can provide students with a list of recent network attacks and network security audit tools/attack tools from which to choose. You might want to ask the students to email you their desired research project by a specific time, or you will assign them a topic. In the email, the student should provide some background information (description, links, etc.) to ensure that no other students are presenting on the same topics.

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.

____

____

____

____

Possible examples include: Code Red, Flame, Nimba, Back Orifice, Blaster, MyDoom, SQL Slammer, SMURF, Tribe flood network (TFN), Stacheldraht, Sobig, Netsky, Witty, Stuxnet and Storm.

The Code Red attack is used as an example here.

Instructor Note: An extensive list of viruses and worms listed by the year they were discovered can be found at http://en.wikipedia.org/wiki/Timeline_of_computer_viruses_and_worms

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

Name of attack:	Code Red
Type of attack:	Worm
Dates of attacks:	July 2001
Computers / Organizations affected:	Infected an estimated 359,000 computers in one day.
How it works and what it did:	
Instructor Note: Most of the following is from Wikipedia. Code Red exploited buffer-overflow vulnerabilities in unpatched Microsoft Internet Information Servers. It launched Trojan code in a denial-of-service attack against fixed IP addresses. The worm spread itself using a common type of vulnerability known as a buffer overflow. It used a long string repeating the character 'N' to overflow a buffer, which then allowed the worm to execute arbitrary code and infect the machine. The payload of the worm included the following: • Defacing the affected website with the message: HELLO! Welcome to http://www.worm.com! Hacked By Chinese! • It tried to spread itself by looking for more IIS servers on the Internet. • It waited 20–27 days after it was installed to launch DoS attacks on several fixed IP addresses. The IP address of the White House web server was among them.	

• When scanning for vulnerable machines, the worm did not check whether the server running on a remote machine was running a vulnerable version of IIS or whether it was running IIS at all.
Mitigation options:
To prevent the exploitation of the IIS vulnerability, organizations needed to apply the IIS patch from Microsoft.
References and info links:
CERT Advisory CA-2001-19 CAIDA Analysis of Code-Red Code Red II analysis
Presentation support graphics (include PowerPoint filename or web links):
Wikipedia Animation on "The Spread of the Code-Red Worm (CRv2)". CAIDA Analysis.

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.

____

____

____

____

____

____

____

Possible examples include: Microsoft Baseline Security Analyzer (MBSA), NMAP, Cisco IOS AutoSecure.. Sourceforge Network Security Analysis Tool (NSAT), Solarwinds Engineering Toolset.

Attacker tools may also be investigated, including L0phtcrack, Cain and Abel, John the Ripper, Netcat, THC Hydra, Chkrootkit, DSniff, Nessus, AirSnort, AirCrack, WEPCrack.

Cisco IOS AutoSecure is used as an example here.

Instructor Note: Additional sources of information include the following:

http://www.yolinux.com/TUTORIALS/LinuxSecurityTools.html

Top Network Security Tools:

http://sectools.org/

Password Crackers:

http://sectools.org/tag/pass-audit/

http://resources.infosecinstitute.com/10-popular-password-cracking-tools/

Sniffers:

http://sectools.org/sniffers.html

Vulnerability Scanner:

http://sectools.org/vuln-scanners.html

Web Scanners:

http://sectools.org/web-scanners.html

Wireless:

http://sectools.org/wireless.html

Exploitation:

http://sectools.org/sploits.html

Packet Crafters:

http://sectools.org/tag/packet-crafters

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

Name of tool:	Cisco AutoSecure
Developer:	Cisco Systems
Type of tool (character-based or GUI):	Character-based
Used on (network device or computer host):	Cisco router or switch
Cost:	Included as part of IOS
Description of key features and capabilities of product or tool:	
AutoSecure feature allows a user to perform the following functions: • Disable common IP services that can be exploited for network attacks • Enable IP services and features that can aid in the defense of a network when under attack. • Automates the configuration of security features on a router or switch and disables certain features that are enabled by default and could be exploited as security holes.	
References and info links:	
http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/autosec.html	

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?

____

____

____

____

____

____

Answers will vary. Massive network attacks like Code Red, which can affect large portions of the Internet, are less common because of mitigation strategies that have been implemented. However, smaller targeted attacks, especially those intended to acquire personal information, are more common than ever. Networking devices and hosts have many vulnerabilities that can be exploited.

Vulnerability analysis tools can help identify security holes so that network administrators can take steps to correct the problem before an attack occurs. Other steps that can be taken include the use of firewalls, intrusion detection and prevention, hardening of network devices, endpoint protection, AAA, user education and security policy development.

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?

____

____

____

____

____

____

Answers will vary, and the results can be interesting.

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

____

____

____

____

____

____

Answers will vary but could include keeping the operating system and applications up to date with patches and service packs, using a personal firewall, configuring passwords to access the system, configuring screensavers to timeout and requiring a password, protecting important files by making them read-only, encrypting confidential files and backup files for safekeeping.