Lab 1.4.5 Identifying Network Vulnerabilities

Objectives

- Use the SANS site to quickly identify Internet security threats.
- Explain how threats are organized.
- List several recent security vulnerabilities.
- Use the SANS links to access other security-related information.

640-802 CCNA Exam Objectives

This lab contains skills that relate to the following CCNA exam objectives:

- Describe security recommended practices including initial steps to secure network devices.
- Describe today's increasing network security threats and explain the need to implement a comprehensive security policy to mitigate the threats.
- Explain general methods to mitigate common security threats to network devices, hosts, and applications.
- Describe the functions of common security appliances and applications.

Expected Results and Success Criteria

Before starting this lab, read through the tasks that you are expected to perform. What do you expect the result of performing these tasks will be?

____

____

____

How is an understanding of Network Vulnerabilities useful in network administration?

____

____

____

How will a network administrator maintain network security?

____

____

____

Background / Preparation

One of the most popular and trusted sites related to defending against computer and network security threats is SANS. SANS stands for SysAdmin, Audit, Network, Security. SANS contains several components, each a major contributor to information security. For additional information about SANS, go to http://www.sans.org/ and select items from the **Resources** menu.

How can a corporate security administrator quickly identify security threats? SANS and the FBI have compiled their list of the **SANS Top-20 Internet Security Attack Targets** at http://www.sans.org/top20/. The list is regularly updated with information under the following categories:

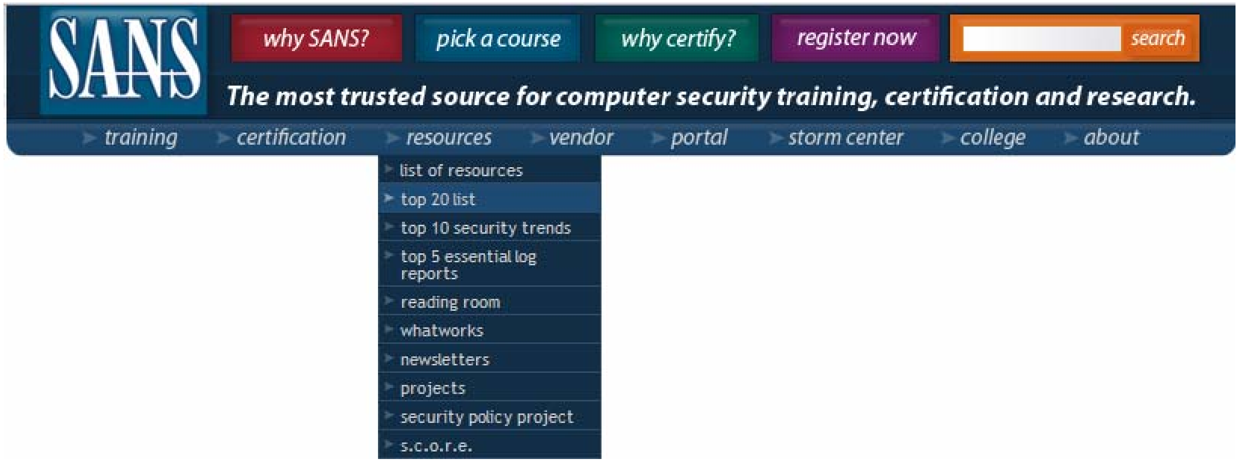
- Operating Systems – Windows, Unix/Linux, MAC
- Cross-Platform Applications – Includes web, database, Peer-to-Peer, instant messaging, media players, DNS servers, backup software, and management servers
- Network Devices – Network infrastructure devices (routers, switches, etc.), VoIP devices
- Security Policy and Personnel – Security policies, human behavior, personnel issues
- Special Section – Prevention strategies and additional security issues

In this lab, you will be introduced to computer security issues and vulnerabilities. The SANS website will be used as a tool for threat vulnerability identification, understanding, and defense.

Estimated completion time is one hour.

Step 1: Open the SANS Top 20 List

Using a web browser, go to http://www.sans.org/. On the **resources** menu, choose **top 20 list.**



The **SANS Top-20 Internet Security Attack Targets** list is organized by category. An identifying letter indicates the category type, and numbers separate category topics. Router and switch topics fall under the **Network Devices** category, **N**. There are two major hyperlink topics:

N1. VoIP Servers and Phones

N2. Network and Other Devices Common Configuration Weaknesses

Step 2: Review common configuration weaknesses

a. Click hyperlink **N2. Network and Other Devices Common Configuration Weaknesses**.

b. List the four headings in this topic.

____

____

____

____

Step 3: Review common default configuration issues

Review the contents of **N2.2 Common Default Configuration Issues**. As an example, **N.2.2.2** (in January 2007) contains information about threats associated with default accounts and values. A Google search on “wireless router passwords” returns links to multiple sites that publish a list of wireless router default administrator account names and passwords. Failure to change the default password on these devices can lead to compromised security and vulnerability to attackers.

Step 4: Note the CVE references

The last line under several topics cites references to CVE or Common Vulnerability Exposure. The CVE name is linked to the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD), sponsored by the United States Department of Homeland Security (DHS) National Cyber Security Division and US-CERT, which contains information about the vulnerability.

Step 5: Investigate a topic and associated CVE hyperlink

The remainder of this lab walks you through a vulnerability investigation and solution.

Choose a topic to investigate, and click on an associated CVE hyperlink. The link should open a new web browser connected to http://nvd.nist.gov/ and the vulnerability summary page for the CVE.

NOTE: Because the CVE list changes, the current list may not contain the same vulnerabilities as those in January 2007.

Step 6: Record vulnerability information

Complete the information about the vulnerability.

Original release date: ______________________________

Last revised: ______________________________________

Source: ____

Overview: ____

____

____

____

Step 7: Record the vulnerability impact

Under **Impact**, there are several values. The Common Vulnerability Scoring System (CVSS) severity is displayed and contains a value between 1 and 10.

Complete the information about the vulnerability impact.

CVSS Severity: ____

Access Complexity: ____

Authentication: ____

Impact Type: ____

Step 8: Record the solution

The **References to Advisories, Solutions, and Tools** section contains links with information about the vulnerability and possible solutions.

Using the hyperlinks, write a brief description of the solution found on those pages.

____

____

____

____

____

____

____

____

Step 9: Reflection

The number of vulnerabilities to computers, networks, and data, continues to increase. Many national governments have dedicated significant resources to coordinating and disseminating information about security vulnerability and possible solutions. It remains the responsibility of the end user to implement the solution. Think of ways that users can help strengthen security. Write down some user habits that create security risks.

____

____

____

____

____

____

____

____

____

____

Challenge

Try to identify an organization that will meet with the class to explain how vulnerabilities are tracked and solutions applied. Finding an organization willing to do this may be difficult, for security reasons, but will benefit students, who will learn how vulnerability mitigation is accomplished in the world. It will also give representatives of the organization an opportunity to meet the class and conduct informal intern interviews.