Activity 1.4.5: Identifying Top Security Vulnerabilities

Learning Objectives

Upon completion of this activity, you will be able to:

- 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.

Background

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 the SANS site, 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 top 20 Internet Security Attack Targets at http://www.sans.org/top20/. The list is regularly updated with information formatted by:

- Operating Systems—Windows, Unix/Linux, MAC
- Applications—Cross-platform, including 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
- Human Elements—Security policies, human behavior, personnel issues
- Special Section—Security issues not related to any of the above categories

Scenario

This lab will introduce students to computer security issues vulnerabilities. The SANS web site will be used as a tool for threat vulnerability identification, understanding, and defense.

This lab must be completed outside of the Cisco lab from a computer with Internet access.

Estimated completion time is one hour.

Task 1: Locate the SANS Resources.

Step 1: Open the SANS Top 20 List.

Using a web browser, go to URL http://www.sans.org. On the **resources** menu, choose **top 20 list**, shown in Figure 1.

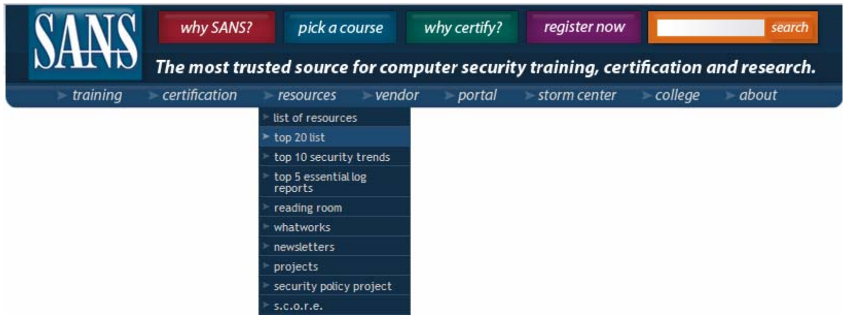

Figure 1. SANS Menu

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. These topics change annually due in part to rapid changes in technology. For the purpose of this activity, navigate to http://www.sans.org/top20/2006/?portal=8cd2978e94c0c1ae18da87e90a085409.

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: Click hyperlink N2. Network and Other Devices Common Configuration Weaknesses to jump to this topic.

Task 2: Review the SANS Resources.

Step 1: Review the contents of N2.2 Common Default Configuration Issues.

For 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 compromise and vulnerability by attackers.

Step 2: Note the CVE references.

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

Task 3: Collect Data.

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

Step 1: Choose a topic to investigate, and click on an example CVE hyperlink.

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

The link should open a new web browser connected to http://nvd.nist.gov/ and the vulnerability summary page for the CVE.

Step 2: Fill in information about the vulnerability:

Original release date: ____________________________

Last revised: ___________________________________

Source: _______________________________________

Overview:

____

____

____

____

____

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

Step 3: Fill in information about the vulnerability impact:

CVSS Severity: ________________________

Range: _______________________________

Authentication: _________________________

Impact Type: __________________________

The next heading contains links with information about the vulnerability and possible solutions.

Step 4: Using the hyperlinks, write a brief description of the solution as found on those pages.

____

____

____

____

____

____

____

____

Task 4: Reflection

The number of vulnerabilities to computers, networks, and data continues to increase. The governments have dedicated significant resources to coordinating and disseminating information about the 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. Think about user habits that create security risks.

Task 5: Challenge

Try to identify an organization that will meet with us to explain how vulnerabilities are tracked and solutions applied. Finding an organization willing to do this may be difficult, for security reasons, but will benefits 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.