Lab – Researching Network Security Threats

Objectives

Part 1: Explore the SANS Website

- Navigate to the SANS website and identify resources.

Part 2: Identify Recent Network Security Threats

- Identify several recent network security threats using the SANS site.
- Identify sites beyond SANS that provide network security threat information.

Part 3: Detail a Specific Network Security Threat

- Select and detail a specific recent network threat.
- Present information to the class.

Background / Scenario

To defend a network against attacks, an administrator must identify external threats that pose a danger to the network. Security websites can be used to identify emerging threats and provide mitigation options for defending a network.

One of the most popular and trusted sites for defending against computer and network security threats is SysAdmin, Audit, Network, Security (SANS). The SANS site provides multiple resources, including a list of the top 20 Critical Security Controls for Effective Cyber Defense and the weekly @Risk: The Consensus Security Alert newsletter. This newsletter details new network attacks and vulnerabilities.

In this lab, you will navigate to and explore the SANS site, use the SANS site to identify recent network security threats, research other websites that identify threats, and research and present the details about a specific network attack.

Required Resources

- Device with Internet access
- Presentation computer with PowerPoint or other presentation software installed

Part 1: Exploring the SANS Website

In Part 1, navigate to the SANS website and explore the available resources.

Step 1: Locate SANS resources.

Using a web browser, navigate to www.SANS.org. From the home page, highlight the **Resources** menu.

List three available resources.

Step 2: Locate the Top 20 Critical Controls.

The **Twenty Critical Security Controls for Effective Cyber Defense** listed on the SANS website are the culmination of a public-private partnership involving the Department of Defense (DoD), National Security Association, Center for Internet Security (CIS), and the SANS Institute. The list was developed to prioritize the

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

cyber security controls and spending for DoD. It has become the centerpiece for effective security programs for the United States government. From the **Resources** menu, select **Top 20 Critical Controls**.

Select one of the 20 Critical Controls and list three of the implementation suggestions for this control.

Step 3: Locate the Newsletters menu.

Highlight the **Resources** menu, select **Newsletters**. Briefly describe each of the three newsletters available.

Part 2: Identify Recent Network Security Threats

In Part 2, you will research recent network security threats using the SANs site and identify other sites containing security threat information.

Step 1: Locate the @Risk: Consensus Security Alert Newsletter Archive.

From the **Newsletters** page, select **Archive** for the @RISK: The Consensus Security Alert. Scroll down to **Archives Volumes** and select a recent weekly newsletter. Review the **Notable Recent Security Issues and Most Popular Malware Files** sections.

List some recent attacks. Browse multiple recent newsletters, if necessary.

Step 2: Identify sites providing recent security threat information.

Besides the SANS site, identify some other websites that provide recent security threat information.

List some of the recent security threats detailed on these websites.

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Part 3: Detail a Specific Network Security Attack

In Part 3, you will research a specific network attack that has occurred and create a presentation based on your findings. Complete the form below based on your findings.

Step 1: Complete the following form for the selected network attack.

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:	

Step 2: Follow the instructor's guidelines to complete the presentation.

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Reflection

1. What steps can you take to protect your own computer?

2. What are some important steps that organizations can take to protect their resources?

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.