Lab - Research Network Security Threats Objectives

Part 1: Explore the SANS Website

Part 2: Identify Recent Network Security Threats

Part 3: Detail a Specific Network Security Threat

# 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

# Instructions

## Exploring the SANS Website

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

### Locate SANS resources.

Search the internet for SANS. From the SANS home page, click on FREE **Resources**.

#### Question:

List three available resources.

Webcasts, Blog, White papers

### Locate the link to the CIS Critical Security Controls.

The **CIS Critical Security Controls** linked 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 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 **Critical Security Controls**, or similar. The CIS Critical Security Controls document is hosted at the Center for Internet Security (CIS) web site and requires free registration to access. There is a link on the CIS Security Controls page at SANS to download the 2014 SANS Critical Security Controls Poster, which provides a brief description of each control.

#### Question:

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

CIS Control 2: Inventory and Control of Software Assets. This tool provides an opportunity for an organization to identify, monitor and automate software management processes. It is important to identify and document all software resources, as well as remove unnecessary, outdated or vulnerable components from them. It is also necessary to compile a list of authorized software to prevent the installation and use of unauthorized programs. To ensure the control and effective management of software applications, it is recommended to perform sequential scanning and updating.

Type your answers here.

### Locate the Newsletters menu.

#### Question:

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

• SANS NewsBites is a weekly review of the most significant news articles about cybersecurity that have been published recently. News about events and incidents are provided with comments from recognized experts of the SIMS community, which provide important context.

• @RISK provides a weekly overview of recently discovered attack vectors, vulnerabilities with active new exploits, as well as detailed explanations of how recent attacks occurred and other valuable information.

• OUCH! is the world's leading free security newsletter designed for a wide audience. It is published monthly in several languages and each issue is thoroughly researched and developed by the SANS Security Awareness team, instructors and community members.

Type your answers here.

## 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.

### 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.

#### Question:

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

* CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
* CWE-434: Unrestricted Upload of File with Dangerous Type
* CWE-193: Off-by-one Error

### Identify sites providing recent security threat information.

#### Questions:

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

www.mcafee.com/us/mcafee-labs.aspx, www.symantec.com, news.cnet.com/security/, www.sophos.com/en-us/threat-center/, us.norton.com/security\_response/.

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

Trojan.Ransomlock, Inostealer.Vskim, Trojan,Fareit, Backdoor.Sorosk, Android.Boxer, W32.Changeup!gen35

Type your answers here.

## 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.

### Complete the following form for the selected network attack.

|  |  |
| --- | --- |
| **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:** | |
| Code Red exploited buffer overflow vulnerabilities in unregistered Microsoft Internet information servers. He launched a Trojan code during a denial-of-service attack on fixed IP addresses. The worm spread itself by exploiting a common type of vulnerability known as buffer overflow. He used a long string repeating the "N" character to overflow the buffer, which then allowed the worm to execute arbitrary code and infect the computer. | |
| **Mitigation options:** | |
| To prevent the IIS vulnerability from being exploited, organizations needed to apply Microsoft's IIS fix. | |
| **References and info links:** | |
| CERT Advisory CA-2001-19  eEye Code Red advisory  Code Red II analysis | |

### Follow the instructor’s guidelines to complete the presentation.

# Reflection Questions

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

Keeping the operating system and applications up to date with patches and service packs, using a personal firewall, configuring passwords to access the system and bios, setting screensavers to timeout and requiring password entry, protecting important files by granting them read-only access, encrypting confidential files and backup files for safe storage.

Type your answers here.

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

Use of firewall, intrusion detection and prevention, hardening of network devices, endpoint protection, network vulnerability tools, user education, and security policy development.