Lab – Researching Network Security Threats (Instructor Version)

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

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.

____

____

Reading Room, Webcasts, Newsletters, Blogs, Top 25 Programming Errors, Top 20 Critical Controls, Security Policy Project

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 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.

____

____

____

____

____

____

Answers will vary. Critical Control 5: Malware Defenses. Employ automated tools to continuously monitor workstations, servers, and mobile devices. Employ anti-malware software and signature auto-update features. Configure network computers to not auto-run content from removable media.

Step 3: Locate the Newsletters menu.

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

____

____

____

____

____

____

SANS NewsBites - A high level summary of the most important news articles that deal with computer security. The newsletter is published twice a week and includes links for more information.

@RISK: The Consensus Security Alert - A weekly summary of new network attacks and vulnerabilities. The newsletters is also provides insights on how recent attacks worked.

Ouch! – A security awareness document that provides end users with information about how they can help ensure the safety of their network.

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.

____

____

____

Answers will vary. Win.Trojan.Quarian, Win.Trojan.Changeup, Andr.Trojan.SMSsend-1, Java.Exploit.Agent-14, Trojan.ADH.

Step 2: Identify sites providing recent security threat information.

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

____

____

____

Answers will vary but could include 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.

____

____

____

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

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:	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 eEye Code Red advisory Code Red II analysis

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

Reflection

1. What steps can you take to protect your own 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 and bios, configuring screensavers to timeout and requiring a password, protecting important files by making them read-only, encrypting confidential files and backup files for safe keeping.

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

   Answers will vary but could include the use of firewalls, intrusion detection and prevention, hardening of network devices, endpoint protection, network vulnerability tools, user education, and security policy development.