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.

Reading Room, Webcasts, Newsletters, Blogs, Top 25 Software Errors, 20 Critical Controls, Security Policies

### 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.

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.

### Locate the Newsletters menu.

#### Question:

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

SANS NewsBites is a semiweekly high-level executive summary of the most important news articles that have been published on computer security during the last week. Each news item is very briefly summarized and includes a reference on the web for detailed information, if possible.

@RISK provides a reliable weekly summary of (1) newly discovered attack vectors, (2) vulnerabilities with active new exploits, (3) insightful explanations of how recent attacks worked, and other valuable data

OUCH! is the world’s leading, free security awareness newsletter designed for the common computer user. Published every month and in multiple languages, each edition is carefully researched and developed by the SANS Securing The Human team, SANS instructor subject matter experts, and team members of the community. Each issue focuses on and explains a specific topic and actionable steps people can take to protect themselves, their family and their organization.

## 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.

- VMware Tools contains an authentication bypass vulnerability in the vgauth module.

- **VMware Aria Operations for Networks (formerly vRealize Network Insight) contains a command injection vulnerability that allows a malicious actor with network access to perform an attack resulting in remote code execution.**

**-  Microsoft Win32k contains an unspecified vulnerability that allows for privilege escalation.**

### Identify sites providing recent security threat information.

#### Questions:

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

1. Wombat Security Technologies: Wombat Security Technologies specializes in security awareness and training solutions. Their blog covers recent events, employee-specific threats (such as phishing), and actionable information to enhance security awareness.
2. Kaspersky Labs' Threatpost: Threatpost, a publication by Kaspersky Labs, provides daily articles, podcasts, and videos covering all aspects of security. They focus on new threats, attacks, and vulnerabilities, making it a valuable resource to stay updated on potential risks.

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

1. Wombat Security Technologies:

-The EvilProxy Phishing Toolkit:  EvilProxy is a phishing toolkit that can steal user credentials and [multifactor authentication (MFA)](https://www.proofpoint.com/us/threat-reference/multifactor-authentication) tokens. It works by sitting between the target and a legitimate webpage.

-TOAD attack: A TOAD attack is a relatively new form of [phishing attack](https://www.proofpoint.com/us/threat-reference/phishing) that combines voice and email phishing techniques. Attackers aim to trick users into disclosing sensitive information over the phone, such as login credentials or financial data, by impersonating a trusted authority figure. They will get on a call with the victim, claiming to be a representative from a reputable company or organization. Then, they will follow up with an email that contains a phishing link or attachment.

1. Kaspersky Labs' Threatpost:
2. **-Watering Hole Attacks Push ScanBox Keylogger:** **Researchers uncover a watering hole attack likely carried out by APT TA423, which attempts to plant the ScanBox JavaScript-based reconnaissance tool.**
3. **-Malicious Npm Packages Tapped Again to Target Discord Users:** **Recent LofyLife campaign steals tokens and infects client files to monitor various user actions, such as log-ins, password changes and payment methods.**

## 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:** | **WannaCry ransomware** |
| **Type of attack:** | **CryptoWorm** |
| **Dates of attacks:** | **July 2001May2017** |
| **Computers / Organizations affected:** | **Estimated 200,000 computers in 150 countries** |
| **How it works and what it did:** | |
| **From Wikipedia:**  **WannaCry is a ransomware cryptoworm, which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoincryptocurrency. The worm is also known as WannaCrypt, Wana Decrypt0r 2.0, WanaCrypt0r 2.0, and Wanna Decryptor. It is considered a network worm because it also includes a “transport” mechanism to automatically spread itself. This transport code scans for vulnerable systems, then uses the EternalBlue exploit to gain access, and the DoublePulsar tool to install and execute a copy of itself. WannaCry versions 0, 1, and 2 were created using Microsoft Visual C++ 6.0.**  **EternalBlue is an exploit of Windows’ Server Message Block (SMB) protocol released by The Shadow Brokers. Much of the attention and comment around the event was occasioned by the fact that the U.S. National Security Agency (NSA) (from whom the exploit was likely stolen) had already discovered the vulnerability, but used it to create an exploit for its own offensive work, rather than report it to Microsoft. Microsoft eventually discovered the vulnerability, and on Tuesday, 14 March 2017, they issued security bulletin MS17-010, which detailed the flaw and announced that patches had been released for all Windows versions that were currently supported at that time, these being Windows Vista, Windows 7, Windows 8.1, Windows 10, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2016.**  **When executed, the WannaCry malware first checks the “kill switch” domain name; if it is not found, then the ransomware encrypts the computer’s data, then attempts to exploit the SMB vulnerability to spread out to random computers on the Internet, and “laterally” to computers on the same network. As with other modern ransomware, the payload displays a message informing the user that files have been encrypted, and demands a payment of around US$300 in bitcoin within three days, or US$600 within seven days. Three hardcoded bitcoin addresses, or “wallets”, are used to receive the payments of victims. As with all such wallets, their transactions and balances are publicly accessible even though the cryptocurrency wallet owners remain unknown.** | |
| **Mitigation options:** | |
| **Apply patches issued by Microsoft for the Windows operating system** | |
| **References and info links:** | |
| **Wikipedia CSO Online** | |

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

# Reflection Questions

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

It includes the use of firewalls, intrusion detection and prevention, hardening of network devices, endpoint protection, network vulnerability tools, user education, and security policy development.

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

It include the use of firewalls, intrusion detection and prevention, hardening of network devices, endpoint protection, network vulnerability tools, user education, and security policy development.

End of Document