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.

Security Policy Templates, CIS Controls v8 and Annual SANS Security Awareness Report.

Type your answers here.

### 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.

Malware Defenses:

The suggestion is to monitor serves, workstations and mobile devices through automation. Implement anti-malwares, configure network computers to disable automatic execution of 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 summarizes the most important computer security news articles from the past week;  
@RISK summarizes newly discovered attack vectors, vulnerabilities and explanations of recent attack methods;  
OUCH! Is free and widely recognized security awareness newsletter, developed by the SANS Securing The Human team, SANS instructors and community members, and goes over instructing readers to protect themselves.

## 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.

CVE-2023-2145 **- Campcodes Online Thesis Archiving System 1.0 is vulnerable to remote SQL injection via manipulation of the id argument in projects\_per\_curriculum.php (VDB-226266);**

CVE-2023-29336 - Win32k Elevation of Privilege Vulnerability;

CVE-2023-29778 - GL.iNET MT3000 4.1.0 Release 2 is vulnerable to OS Command Injection via /usr/lib/oui-httpd/rpc/logread.

CVE-2023-25717 - Ruckus Wireless Admin through 10.4 allows remote code execution via unauthenticated HTTP GET Request.

CVE-2023-1389 - TP-Link Archer AX21 firmware versions prior to 1.1.4 Build 20230219 have a command injection vulnerability in the country form of the /cgi-bin/luci;stok=/locale endpoint, allowing an attacker to run commands as root.

### Identify sites providing recent security threat information.

#### Questions:

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

https://www.securityweek.com/category/malware-cyber-threats/

https://cyware.com/cyber-security-news-articles

https://www.cisa.gov/topics/cyber-threats-and-advisories

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

Android apps with spyware installed 421 million times from Google Play;

Retailer Database Error Leaks Over One Million Customer Records;

Many Vulnerabilities Found in PrinterLogic Enterprise Software;

[CAPTCHA-Breaking Services with Human Solvers Helping Cybercriminals Defeat Security](https://thehackernews.com/2023/05/captcha-breaking-services-with-human.html).

## 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:** | Dorchester school IT system held to ransom in cyber attack |
| **Type of attack:** | Ransomware |
| **Dates of attacks:** | May 21, 2023 |
| **Computers / Organizations affected:** | Thomas Hardye School from Dorchester, England |
| **How it works and what it did:** | |
| The Thomas Hardye School in Dorchester was targeted by a ransomware attack on the 21st of May. As a result of the attack, all functions dependent on the school server, such as canteen payments, records and emails, became unavailable and parents of the more than two thousand students have been asked to communicate with the school by telephone. Following the cyber-attack, the attackers send a ransom demanding the school to make a payment through the dark web in order to reestablish the proper functioning of the school server. However, the school staff said they would not be paying the ransom and were working with the National Cyber Security Centre and police to resolve the issue. Details about how the attackers gained access to the school server were not given. | |
| **Mitigation options:** | |
| Have an incident response plan;  Have an update backup of system and files;  Don’t pay the ransom;  Isolate affected endpoints;  Report the attack to authorities;  Remove any malware from the system. | |
| **References and info links:** | |
| https://www.bbc.com/news/uk-england-dorset-65685607 | |

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

# Reflection Questions

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

Use firewall, keep firewall, other software and operating system always updated, encrypt important information and always having a backup of your system and files in a separate drive.

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

Use firewall, network vulnerability tools, develop a security policy development and hardening of network devices, and informing and educating their users to ensure they are aware make use of security practices.