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.

Webcast, Blogs, 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.

Data Protection (Bảo vệ dữ liệu). Xem xét tất cả các nguồn có thể rò rỉ dữ liệu. Giám sát tất cả các nguồn thông tin nhạy cảm tiềm ẩn. Coi bảo mật là một khoản đầu tư, không phải là một gánh nặng. Sử dụng mã hóa bất cứ nơi nào có thể.

### Locate the Newsletters menu.

#### Question:

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

NewsBites: Là một loạt các cảnh báo và đề xuất về an ninh mạng từ các tập và số khác nhau. Các chủ đề được đề cập bao gồm vá các lỗ hổng trong tường lửa FortiGate, bảo mật cho CI/CD, đáp ứng các yêu cầu lưu giữ dữ liệu, bảo mật chuỗi cung ứng, ngừng hoạt động DDoS trong Azure và người dùng MOVEit bị xâm phạm.   
@RISK: Bao gồm một số tập và số phát hành của "Cảnh báo lỗ hổng bảo mật đồng thuận". Những cảnh báo này có thể tập trung vào các lỗ hổng và rủi ro bảo mật khác nhau đã được xác định trong khoảng thời gian được đề cập.   
OUCH!: Bao gồm các bài viết khác nhau về các chủ đề khác nhau liên quan đến an ninh mạng và an toàn trực tuyến. Các bài viết này nhằm mục đích giáo dục người đọc về các mối đe dọa tiềm ẩn, đồng thời cung cấp thông tin chi tiết và khuyến nghị về cách bảo vệ các tài khoản của bản thân.

## 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.

Log4j vulnerability (CVE-2021-44228, PrintNightmare vulnerability (CVE-2021-34527), ProxyShell vulnerability (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207)

### Identify sites providing recent security threat information.

#### Questions:

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

nvd.nist.gov, mitre.org,

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

NVD: CVE-2023-1619. Mitre: Trojan.Karagany.

## 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:** | Rootkit |
| **Type of attack:** | Trojan |
| **Dates of attacks:** | 1999, được phát hiện vào 2003 |
| **Computers / Organizations affected:** | Hầu như những máy tính cá nhân đều có thể bị ảnh hưởng |
| **How it works and what it did:** | |
| Rootkit là trojan cho phép hacker truy cập máy tính từ xa để cài đặt phần mềm gián điệp, đánh cắp dữ liệu và kiểm soát máy tính, đồng nghĩa là Rootkit sẽ hoàn toàn kiểm soát hệ thống. Rootkit sẽ che giấu một số đối tượng hoặc hoạt động ngầm trong hệ thống máy tính. Tuy nhiên do nó hoạt động ngầm nên các phần mềm diệt virus khó có thể phát hiện ra. Rootkit sẽ hoạt động ngầm trong cả tầng user và tầng kernel của hệ điều hành. | |
| **Mitigation options:** | |
| Đồng bộ dữ liệu liên tục, backup hệ điều hành, nâng cấp hệ điều hành và tường lửa, liên tục quét các phần mềm đáng nghi trong hệ thống, theo dõi hoạt động của chúng trong Task manager. | |
| **References and info links:** | |
| <https://en.wikipedia.org/wiki/Rootkit#:~:text=The%20first%20malicious%20rootkit%20for,programmable%20logic%20controllers%20(PLC)>.  https://www.malwarebytes.com/blog/news/2020/01/how-to-prevent-a-rootkit-attack | |

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

# Reflection Questions

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

Đối với máy tính cá nhân: Luôn đảm bảo thiết bị phải được cập nhật phần mềm bảo mật mới nhất. Đồng thời thay đổi các mật khẩu tài khoản định kỳ, mã hóa và đồng bộ các tài liệu, dữ liệu một cách an toàn.

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

Đối với máy tính của các tổ chức: Đảm bảo phần mềm được cập nhật liên tục, sử dụng mật khẩu mạnh và yêu cầu đổi mật khẩu thường xuyên, backup dữ liệu và lưu ở ổ nhớ không bị ảnh hưởng, theo dõi trạng thái tường lửa liên tục.

End of Document