Lab - Research Network Security Threats

Link clip guide : <https://drive.google.com/file/d/1oauWTdOhhFC16eA2mwoWaGU4qJh-6XGr/view?usp=drivesdk>

# 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, Whitepaper, Posters and Cheat Sheets

### 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.

Control 11: Data Recovery

* Establish and Maintain a Data Recovery Process
* Perform Automated Backups
* Protect Recovery Data
* Establish and Maintain an Isolated Instance of Recovery Data
* Test Data Recover

### Locate the Newsletters menu.

#### Question:

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

* NewsBites: An annotated, semiweekly executive summary of the most recent and important and important cyber security news deadlines.
* @RISK: A reliable weekly summary of newly discovered attack vectors, vulnerabilities with active new exploits, insightful explanations of how recent attacks worked, and other valuable data.
* OUCH!: The world's leading, monthly security awareness newsletter designed for the common computer user, translated in over 20 languages and free for the community.

## 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.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

### Identify sites providing recent security threat information.

#### Questions:

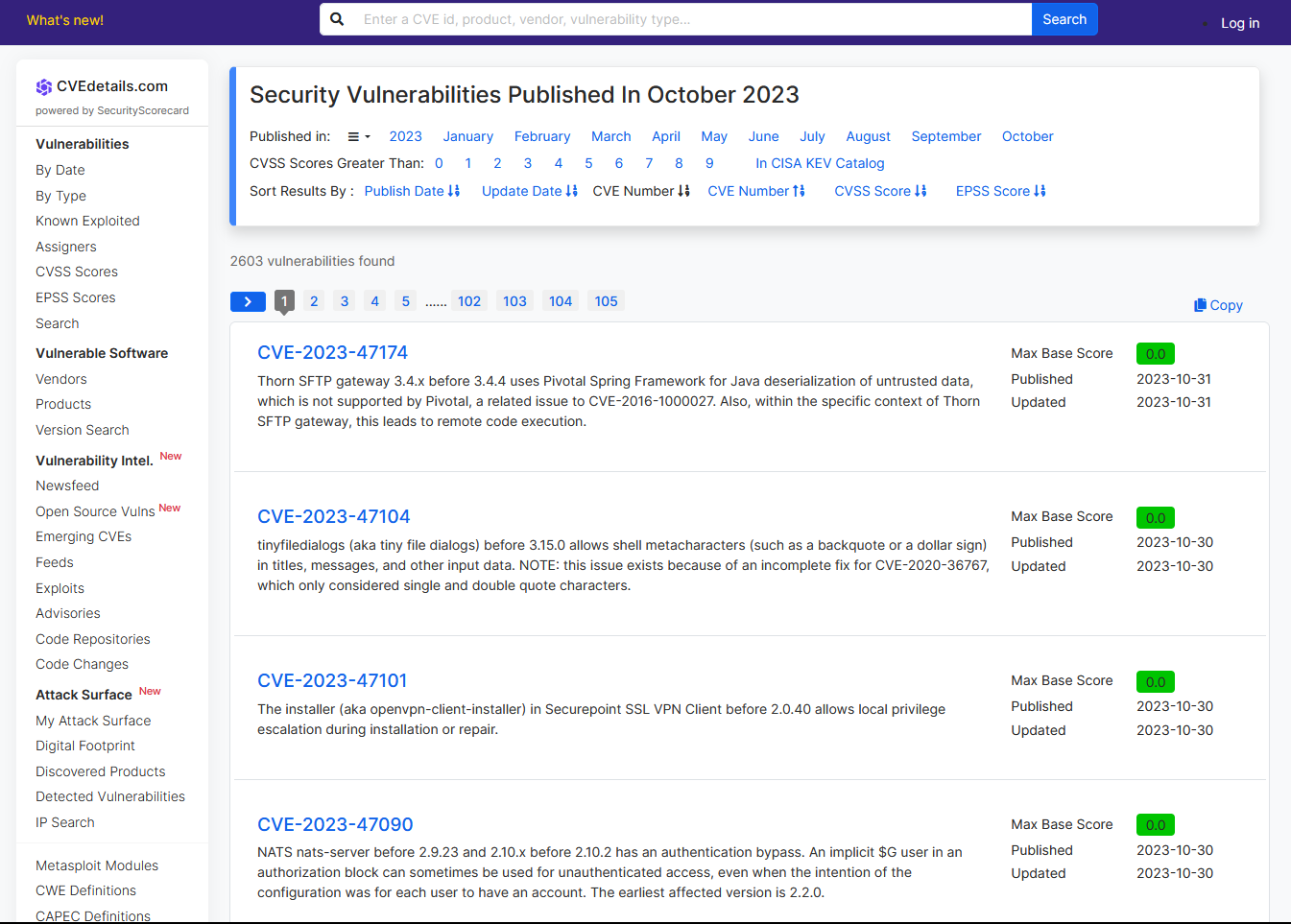
Besides the SANS site, identify some other websites that provide recent security threat information.

<https://www.cvedetails.com/>

<https://thehackernews.com/>

<https://www.securityweek.com/>

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



A screenshot of a computer

Description automatically generated

A screenshot of a computer screen

Description automatically generated

## 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:** | NotPetya/Petya/ExPetr Ransomware Attack (2017) |
| **Type of attack:** | Ransomware |
| **Dates of attacks:** | June 27, 2017 |
| **Computers / Organizations affected:** | The attack impacted organizations and systems worldwide, with a significant focus on Ukraine. It affected government systems, banks, utilities, shipping companies (e.g., Maersk), and multinational corporations (e.g., Merck, FedEx). |
| **How it works and what it did:** | |
| * The NotPetya attack leveraged the EternalBlue vulnerability in Microsoft Windows to rapidly spread across networks. * It initially appeared as a ransomware attack, but its true intent was destructive. It encrypted the Master Boot Record (MBR) of infected computers, making them inoperable. * NotPetya also included a data-wiping component, making data recovery nearly impossible. * The malware demanded a ransom in Bitcoin, but the email address for ransom correspondence was quickly disabled, rendering payment ineffective. | |
| **Mitigation options:** | |
| * Regularly apply security patches and updates to protect against known vulnerabilities. * Maintain up-to-date and robust cybersecurity measures, including intrusion detection systems and strong access controls. * Implement data backup and recovery strategies to ensure data can be restored in case of an attack. * Develop an incident response plan to quickly respond to and recover from cyber incidents. | |
| **References and info links:** | |
| 1. [NotPetya Ransomware Cyber Attack (Wikipedia)](https://en.wikipedia.org/wiki/Petya_(malware)) 2. [The Petya Ransomware (NotPetya) - What We Know and How to Prevent It (Trend Micro)](https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/the-petya-ransomware-notpetya-epidemic-what-we-know-so-far) 3. [Petya ransomware attack: What it is, and why this is happening again (CNN)](https://www.cnn.com/2017/06/28/europe/generic-ransomware-petya-attack/index.html) | |

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

# Reflection Questions

* 1. What steps can you take to protect your own computer?
* Use strong, unique passwords and enable two-factor authentication (2FA) for accounts.
* Keep your operating system and software updated.
* Install reputable antivirus and anti-malware software.
* Use a firewall and secure your Wi-Fi network.
* Regularly back up your important data.
* Be cautious of phishing emails and suspicious downloads.
* Use a standard user account for daily activities.
* Encrypt sensitive data and use a secure web browser.
* Monitor your accounts for suspicious activity.
* Educate yourself about cybersecurity threats and best practices.
  1. What are some important steps that organizations can take to protect their resources?
* Implement strong access controls.
* Keep systems and software updated.
* Use network segmentation.
* Provide security awareness training.
* Deploy endpoint security measures.
* Utilize firewalls and intrusion detection.
* Encrypt sensitive data.
* Have an incident response plan.
* Maintain regular backups.
* Manage vendor risks.
* Enforce security policies and procedures.
* Continuously monitor for threats.
* Follow secure development practices.
* Plan for business continuity.