**Lab Tutorial: Cyberattack Case Study and Mitigation Strategies**

**Lab Duration:** 1 Hour  
**Objective:** Analyze a recent cyberattack, determine its root cause, and propose mitigation strategies.

**Lab Overview:**

In this lab, students will conduct a case study on a recent cyberattack. Each student can choose a cyberattack from the list provided. The goal is to understand how the attack occurred, what vulnerabilities were exploited, and how similar attacks can be prevented.

You are required to formally record your details in this document instead of solely getting information from the web server. This document should be present in your weekly code folder.

**Lab Instructions:**

**Step 1: Choose an Attack**

Each student should select one of the following cyberattacks:

1. **SolarWinds Supply Chain Attack (2020)** – Attackers inserted a backdoor into SolarWinds' Orion software, impacting thousands of organizations.
2. **Colonial Pipeline Ransomware Attack (2021)** – A ransomware attack disrupted fuel supply on the East Coast of the U.S.
3. **Log4j Vulnerability Exploit (2021)** – A critical flaw in Log4j allowed remote code execution across various systems.
4. **Twitter Bitcoin Scam (2020)** – Hackers gained access to high-profile Twitter accounts and promoted a Bitcoin scam.
5. **Uber Data Breach (2022)** – Social engineering led to unauthorized access to Uber’s internal systems.
6. **T-Mobile Data Breach (2023)** – Attackers exploited API vulnerabilities to steal customer data.
7. **CrowdStrike IT Outages (2024) –** In March 2024, following a stress test, CrowdStrike released Rapid Response Content for Channel File 291. Subsequent updates in April 2024 led to IT outages for some customers, prompting investigations and clarifications from the company.
8. **Microsoft Exchange Server Hack (2021)** – State-sponsored hackers exploited vulnerabilities in Microsoft Exchange servers.
9. **MOVEit File Transfer Hack (2023)** – A zero-day vulnerability in MOVEit file transfer software was exploited to steal data.
10. **WannaCry Ransomware Attack (2017)** – A global ransomware attack exploited a vulnerability in Microsoft Windows, impacting thousands of organizations worldwide, including the NHS in the UK.
11. **Zoom Security Issues (2020)** – During the rise of remote work, cybercriminals exploited flaws in Zoom’s video conferencing software, leading to "Zoombombing" incidents and concerns over encryption.
12. **23andMe data breach (2022) -** An unauthorized party gained access to the personal data of some of the genetic testing company's users.
13. **Kaseya VSA Ransomware Attack (2021)** – Attackers targeted the Kaseya VSA platform, which is used by managed service providers, infecting their clients with ransomware. This attack impacted hundreds of businesses and organizations globally.

**Step 2: Research the Attack**

1. **How did the attack happen?** Identify the vulnerabilities or weaknesses exploited.

Log4j is a logging library for java applications. Log4j allows dynamic lookups in the log messages using a feature known as JNDI. This allows attackers to craft a message with a link to malicious domain and use as an input. Then JNDI will connect to the malicious domain Which the attacker can use to load malicious payloads.

1. **Who were the attackers?** (If known) Identify whether it was a nation-state, criminal group, or individual hackers.

There were many criminal groups and hacktivist that used this vulnerability.

1. **What was the impact?** Discuss the financial, operational, and reputational damage.

Many companies such as Apple, Amazon, Tesla, RedHat were affected. There were financial implications as the companies had to patch the systems and deal with downtime or ransomware and viruses. Damage was also reputational because consumers will lose their sense of security. The companies also had to change their operations in order to deal with similar situation in the future.

1. **How was it discovered?** Explain how organizations or security researchers identified the attack.

The **Log4j vulnerability** was first discovered by a security researcher working at **Alibaba Cloud's security team**. The discovery was part of their ongoing security efforts to identify and mitigate vulnerabilities in software used by cloud services and applications.

**Step 3: Determine the Cause and Mitigation**

1. **Why did the attack succeed?** Identify security gaps, misconfigurations, or lack of updates.

The attack succeeded due to being able to do dynamic lookups without any checks in place. This was a secure programming issue.

1. **How could it have been prevented?** Suggest security best practices and solutions.

Following secure coding guidelines and testing could have prevented the issue. Any kind of input or access to external sources must be checked.

1. **What mitigation strategies should be in place to prevent future attacks?** Discuss security controls like network monitoring, incident response plans, and user awareness training.

Any kind of external lookup or user input must be checked before running it.

**Step 4:** Work with at least one of your peer and share your findings to them

**Lab Logbook Requirement:** Record the following in your lab logbook:

1. The attack type you have chosen

**Log4j Vulnerability Exploit (2021)** – A critical flaw in Log4j allowed remote code execution across various systems.

1. Any one key website or research paper link that you found was useful.

<https://builtin.com/articles/log4j-vulerability-explained>

**Optional Exercise:** You can analyze more than one type of attack.