**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. **X (Twitter) DDoS Attack (2025)** – A massive DDoS attack targeted X (formerly Twitter), causing widespread outages and disruptions for users globally. The attack was claimed by the pro-Palestinian group Dark Storm Team, which allegedly used Ukrainian IP addresses.
2. **SolarWinds Supply Chain Attack (2020)** – Attackers inserted a backdoor into SolarWinds' Orion software, impacting thousands of organizations.
3. **Colonial Pipeline Ransomware Attack (2021)** – A ransomware attack disrupted fuel supply on the East Coast of the U.S.
4. **Log4j Vulnerability Exploit (2021)** – A critical flaw in Log4j allowed remote code execution across various systems.
5. **Twitter Bitcoin Scam (2020)** – Hackers gained access to high-profile Twitter accounts and promoted a Bitcoin scam.
6. **Uber Data Breach (2022)** – Social engineering led to unauthorized access to Uber’s internal systems.
7. **T-Mobile Data Breach (2023)** – Attackers exploited API vulnerabilities to steal customer data.
8. **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.
9. **Microsoft Exchange Server Hack (2021)** – State-sponsored hackers exploited vulnerabilities in Microsoft Exchange servers.
10. **MOVEit File Transfer Hack (2023)** – A zero-day vulnerability in MOVEit file transfer software was exploited to steal data.
11. **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.
12. **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.
13. **23andMe data breach (2022) -** An unauthorized party gained access to the personal data of some of the genetic testing company's users.
14. **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**

**Microsoft exchange server hack (2021)**

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

A few vulnerabilities that allowed for unauthenticated http requests to be made to servers along with servers allowing for code to be ran with systems permissions and open access to write files to any location on the servers.

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

Hanifum a Chinese state sponsored hacking group.

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

Massive data breach which led to stolen data from around 250,000 servers.

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

An outside cybersecurity company volexity monitored servers and discovered the breach. Another cybersecurity company ESET also reported discovering multiple threat actors activity present on servers.

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

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

A vulnerability was discovered which allowed attackers to make unauthenticated http requests to exchange servers allowing then to access mailboxes and other sensitive information using server-side request forgery.

Another vulnerability was found in the Unified messaging service which allowed attackers to run code with system permissions after authenticating using the vulnerability above

Another vulnerability was that once authenticated systems allowed attackers to write files to any location on the exchange servers.

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

The attacks could have been prevented by implementing policies that only allow authenticated http requests to the exchange server. Use of an endpoint detection and response tool which would use AI and machine learning to detect threats and run scripts to automatically remediate the issue. Another preventative measure would be to ensure that systems are designed using the principles of least privilege which would give users the bare minimum permissions for the tasks they need to perform. Another measure would be multi factor authentication or conditional access polices which would require at least 2 forms of authentication before access is given. Conditional access would help as you could choose whether to allow authentication based on information in the authentication request.

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.

Regular patching and scanning of servers would be a good measure to prevent future attacks. Network monitoring could be used to monitor http requests and block access if anything suspicious is flagged by the monitoring agent.

An Endpoint Detection and remediation tool like crowd strike falcon could help to ensure that endpoints are constantly monitored and if any vulnerabilities are detected they can be remediated with automation that is much quicker and efficient that manual remediation.

The use of encryption can be used to prevent attackers gaining access to data even if they did manage to intercept of gain access to data as they would need to Decrypt the data to see what it actually is.

The use of backup and site recovery policies can be used to prevent any data loss as servers could be restored from the backups or information and systems can automatically fail over to another site if 1 is attacked.

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

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