**Information Security**

**Chapter 1: Cybersecurity and the Security Operations Center**

1. Lab 3 - Cybersecurity Case Studies

# Objectives

Research and analyze cyber security incidents.

Part 1: Conduct search of high profile cyberattacks.

Part 2: Write an analysis of a cyberattack.

# Background / Scenario

Governments, businesses, and individual users are increasingly the targets of cyberattacks and experts predict that these attacks are likely to increase in the future. Cybersecurity education is a top international priority as high-profile cyber-security related incidents raise the fear that attacks could threaten the global economy. The Center for Strategic and International Studies estimates that the cost of cybercrime to the global economy is more than $600 billion annually. In this lab, you will study four high profile cyberattacks and be prepared to discuss the who, what, why and how of each attack.

# Required Resources

* PC or mobile device with internet access

# Instructions

## Conduct search of high profile cyberattacks.

* + 1. Using your favorite search engine conduct a search for each of the cyberattacks listed below. Your search will likely turn up multiple results ranging from news articles to technical articles.
* The Stuxnet Virus
* Marriott data breach
* United Nations data breach
* Microsoft customer support database breach
* Lifelabs data breach

**Note**: You can use the web browser in virtual machine installed in a previous lab to research the hack. By using the virtual machine, you may prevent malware from being installed on your computer.

* + 1. Read the articles found from your search in Step 1a and be prepared to discuss and share your research on the who, what, when, where, and why of each attack.

## Write an analysis of a cyberattack.

Select one of the high-profile cyberattacks from Step 1a and write an analysis of the attack that includes answers to the questions below.

### Questions:

* + 1. **Who were the victims of the attacks?**

The primary victims of the Stuxnet virus were primarily Iranian industrial facilities, specifically the Natanz nuclear facility. The virus was designed to target and sabotage the centrifuges used to enrich uranium at the facility. However, the virus also spread to other countries, including Indonesia, India, and Pakistan, causing damage to their industrial systems as well.

* + 1. **What technologies and tools were used in the attack?**

The Stuxnet virus was a highly sophisticated and complex piece of malware that employed a number of technologies and tools to carry out its attack. Some of the key technologies and tools used in the attack include:

1. Zero-day vulnerabilities: The virus exploited several previously unknown (or "zero-day") vulnerabilities in Windows operating systems to gain initial access to the targeted systems.

2. Rootkit: The virus used a rootkit to hide its presence on the infected systems and evade detection by antivirus software.

3. Digital certificates: The virus used digital certificates stolen from legitimate companies to sign its malicious code, making it appear as if it was from a trusted source.

4. PLC (Programmable Logic Controller) attack: The virus specifically targeted PLCs, which are used to control industrial systems such as centrifuges, and caused them to spin out of control, damaging the equipment.

5. Propagation: The virus propagated through USB drives, and spread via several Windows vulnerabilities, including the LNK vulnerability, which allows malware to spread via removable drives.

* + 1. **When did the attack happen within the network?**

The exact date when the Stuxnet virus was first introduced into the targeted networks is not publicly known. However, it is believed that the virus was first discovered in June 2010 by the Belarus-based computer security company VirusBlokAda. It is believed that the virus had been active and spreading for several months before it was discovered, possibly even a year or more. Some experts estimate that the attack may have begun as early as 2005. It is also believed that the attackers behind the Stuxnet virus used a multi-stage attack, with the initial infection followed by a period of reconnaissance before the actual attack was launched.

* + 1. **What systems were targeted?**

The Stuxnet virus was specifically designed to target industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems that are used to control and monitor critical infrastructure such as power plants, water treatment facilities, and other industrial facilities. The primary target of the Stuxnet attack was believed to be the Natanz nuclear facility in Iran, which used Siemens SIMATIC S7 programmable logic controllers (PLCs) to control the speed and operation of its centrifuges used to enrich uranium. Additionally, the virus also spread to other industrial facilities in Iran and other countries including Indonesia, India, and Pakistan, causing damage to their industrial systems as well, but not to the same extent as in Iran.

* + 1. **What was the motivation of the attackers in this case? What did they hope to achieve?**

The motivation behind the Stuxnet attack is believed to be primarily political and strategic. Many experts believe that the virus was created by a state-sponsored group, possibly with the involvement of multiple countries, with the goal of sabotaging Iran's nuclear program. The Natanz nuclear facility was a key component of Iran's nuclear program, and the attackers likely hoped to disrupt and delay the progress of the program by damaging the centrifuges used to enrich uranium.

It's also believed that the attackers sought to send a message to Iran and other countries that their critical infrastructure is vulnerable to cyber attacks, and that their nuclear programs could be disrupted by cyber means. Additionally, the attack may have been intended to demonstrate the capability of the attackers to carry out such a sophisticated attack, and to send a warning to other countries that they too could be targeted.

There are also theories that the attack was a sabotage attempt to slow down or disrupt Iran's nuclear program as a way to avoid potential military action by other countries.

In any case, the Stuxnet attack was a major demonstration of the destructive potential of cyber attacks, and served as a wake-up call for organizations and governments around the world to improve their cybersecurity defenses.

* + 1. **What was the outcome of the attack? (stolen data, ransom, system damage, etc.)**

The outcome of the Stuxnet attack was primarily physical damage to the targeted industrial systems

It should be noted that the Stuxnet attack did not steal any data, or use the typical techniques of ransomeware, the goal of the attack was to cause physical damage to the equipment.

The Stuxnet attack was a major demonstration of the destructive potential of cyber attacks and it highlighted the vulnerability of industrial control systems and the critical infrastructure they control. The attack also served as a reminder of the importance of improving cybersecurity defenses to protect against advanced persistent threats and nation-state sponsored cyber attacks.