**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?

I have chosen The Stuxnet Virus. The initial victims of this virus were the Iranian nuclear centrifuges. Later different modifications have been done to the original code of Stuxnet and used to attack water pipelines, gas pipelines, treatment plants, and power plants. This modified virus was used to attack different countries and viruses around the world.

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

Mainly the centrifuges in the Iranian nuclear plants. Other technologies are Programmable Logic Controllers (PLCs) are targeted by the Stuxnet. Siemens Step 7 software is also used to attack. Stuxnet spread via USB sticks.

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

In 2010 Stuxnet virus attacked the Iranian nuclear centrifuges.

* + 1. What systems were targeted?

Iranian nuclear centrifuges were targeted by the Stuxnet. Later the modification versions also targeted power plants, gas pipelines, and many others.

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

The motivation behind the attack on the Iranian nuclear plant was to destabilize the Iranian nuclear enrichment system. The attackers wanted destroy the nuclear centrifuges by rotating them irregularly.

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

They try to completely destroy Iranian nuclear centrifuges, but they did not succeed completely, though they succeed to disturb them. They tried to damage the system completely.