Lab - 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

Part 1: Conduct search of high profile cyberattacks.

a. 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.

b. 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.

Part 2: 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.

a. Who were the victims of the attacks?

The primary victims of the Stuxnet attacks were the Iranian nuclear facilities, specifically the Natanz enrichment plant, which is believed to have been the main target of the attack. The virus is thought to have caused significant damage to the centrifuges used in the uranium enrichment process, disrupting Iran's nuclear program and setting it back by several years.

b. What technologies and tools were used in the attack?

Zero-day exploits, rootkit technology, stolen digital certificates, advanced encryption, targeted distribution

c. When did the attack happen within the network?

The virus was first introduced into the Iranian nuclear network in 2009, and it began to spread rapidly throughout the network over the following months.

d. What systems were targeted?

Programmable Logic Controllers
Supervisory Control and Data Acquisition systems
Windows-based operating systems

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

The motivation behind the Stuxnet attack is widely believed to have been to disrupt Iran's nuclear program, which was a major source of concern for the United States and Israel at the time

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

It was widely seen as a major escalation in the ongoing conflict between Iran and the United States and Israel over Iran's nuclear program, and it raised concerns about the potential for cyberattacks to disrupt critical infrastructure and national security. Up to 1,000 centrifuges may have been destroyed or disabled as a result of the attack.