Networking Academy

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. **My choice: The Stuxnet Virus**

a. Who were the victims of the attacks?

The main targets were the Natanz uranium enrichment facility and the Bushehr nuclear power plant, both located in Iran. However, Stuxnet's spread was not entirely limited to these targets, as it affected systems worldwide due to its sophisticated and contagious nature.

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

Stuxnet employed multiple technologies and tools, including:

Exploits: It exploited zero-day vulnerabilities in Windows operating systems and Siemens Step7 software.
Rootkits: Used to hide its presence on infected systems.
PLC Code Injection: Modified code in Siemens programmable logic controllers to manipulate centrifuge speeds.
Propagation Methods: Utilized USB drives and network shares for spreading.
Worm Capabilities: Self-replicated and spread through networks autonomously.

c. When did the attack happen within the network?

The Stuxnet attack on the Iranian nuclear program's network occurred around 2009 and was discovered in June 2010.

d. What systems were targeted?

The Stuxnet attack primarily targeted industrial control systems, specifically Siemens programmable logic controllers (PLCs) used in centrifuge cascades at Iran's Natanz uranium enrichment facility.

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 or delay Iran's nuclear program, specifically its uranium enrichment efforts.

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

The Stuxnet attack's primary outcome was physical damage to centrifuges at Iran's Natanz uranium enrichment facility, resulting in setbacks to Iran's nuclear program. There was no data theft or ransom involved; the goal was to sabotage rather than to steal or extort.