**Information Security**

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

1. Lab 2 - Learning the Details of Attacks
2. **Objectives**

Research and analyze IoT application vulnerabilities.

**Part 1:** Conduct a Search of IoT Application Vulnerabilities.

1. **Background / Scenario**

The Internet of Things (IoT) consists of digitally connected devices that are connecting every aspect of our lives, including our homes, offices, cars, and even our bodies to the internet. With the accelerating adoption of IPv6 and the near universal deployment of Wi-Fi networks, the IoT is growing at an exponential pace. According to Statista, industry experts estimate that by 2030, the number of active IoT devices will approach 50 billion.

However, IoT devices are particularly vulnerable to security threats because security has not always been considered in IoT product design. Also, IoT devices are often sold with old and unpatched embedded operating systems and software.

1. **Required Resources**

* PC or mobile device with internet access.

**Instructions**

**Part 1: Conduct a Search of IoT Application Vulnerabilities**

Using your favorite search engine, conduct a search for Internet of Things (IoT) vulnerabilities. During your search, find an example of an IoT vulnerability for each of the IoT verticals: industry, energy systems, healthcare, and government. Be prepared to discuss who might exploit the vulnerability and why, what caused the vulnerability, and what could be done to limit the vulnerability.

[IoT Security Foundation](https://iotsecurityfoundation.org/)

[Business Insider IoT security threats](http://www.businessinsider.com/iot-cyber-security-hacking-problems-internet-of-things-2016-3)

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

From your research, choose an IoT vulnerability and answer the following questions:

1. What is the vulnerability?

Energy systems: One example of an IoT vulnerability in the energy systems vertical is a vulnerability found in smart grid systems. Smart grids are used to manage and distribute electrical power, and they can be controlled remotely through the internet. A vulnerability in the smart grid software allows an attacker to gain unauthorized access and take control of the grid. This can be exploited to disrupt power supply and cause blackouts.

1. Who might exploit it? Explain.

There might be several actors who may exploit the vulnerabilities in IoT devices to gain unauthorized access and control of the energy grid. These include:

1. Cybercriminals: Cybercriminals can exploit vulnerabilities in energy systems to gain unauthorized access to the grid and steal sensitive information or cause disruptions to the power supply.

2. Nation-state actors: Nation-state actors may exploit vulnerabilities in energy systems as part of cyber espionage or cyber warfare operations, seeking to gain access to sensitive information or disrupt the power supply.

3. Hacktivists: Hacktivists may exploit vulnerabilities in energy systems to make political statements or cause disruption as a form of protest.

4. Terrorists: Terrorists may exploit vulnerabilities in energy systems to cause widespread disruption and panic.

5. Industrial competitors: Industrial competitors may exploit vulnerabilities in energy systems to gain an advantage over their rivals, either by stealing sensitive information or causing disruptions to their competitors' operations.

1. Why does the vulnerability exist?

The vulnerability in energy systems exists due to a variety of reasons, including:

a. Lack of security by design: Many IoT devices used in energy systems, such as smart grid systems, are designed with a focus on functionality and convenience, with minimal consideration given to security. This can leave these devices vulnerable to hacking, malware, and other security threats.

b. Outdated software and firmware: Many IoT devices used in energy systems are sold with old and unpatched embedded operating systems and software, which can leave them vulnerable to known security flaws that have already been discovered and patched in more recent versions of the software.

c. Weak passwords: Many IoT devices used in energy systems come with default passwords that are easily guessable, making it easy for attackers to gain unauthorized access to the device.

d. Lack of encryption: Some IoT devices used in energy systems do not use encryption to protect the data they transmit and receive, making it easy for attackers to intercept and read this data.

e. Insecure communications: Some IoT devices used in energy systems use outdated or insecure communication protocols, making it easy for attackers to intercept or disrupt communications.

f. Lack of secure update mechanisms: Some IoT devices used in energy systems do not have the ability to receive software updates and patches, leaving them vulnerable to known security flaws.

g. Inadequate physical security: Some IoT devices used in energy systems are easily accessible and can be tampered with physically, making it easy for attackers to gain unauthorized access to the device or the network it is connected to.

h. Lack of user awareness: Many users are not aware of the security risks associated with IoT devices used in energy systems, and may not take steps to secure these devices.

I. Lack of government regulations: There is a lack of government regulations regarding IoT security in energy systems, which can make it difficult to ensure that devices are secure.

j. Outdated protocols: Some devices used in energy systems are built on outdated protocols and standards, which can make them vulnerable to newer attack methods.

1. What could be done to limit the vulnerability?

There are several steps that can be taken to limit the vulnerability in energy systems, including:

1. Prioritizing security in the design and development of IoT devices used in energy systems: This can include implementing robust security measures such as encryption, secure authentication, and regular software updates and patches.

2. Conducting regular security audits and testing: Regular security audits and testing can help identify and address vulnerabilities in energy systems.

3. Implementing security controls: Implementing security controls such as firewalls, intrusion detection and prevention systems, and VPNs can help protect energy systems from cyber threats.

4. Securing communication protocols: Using secure communication protocols such as HTTPS and SSL to protect the data that is transmitted and received can help to limit the vulnerability in energy systems

5. Securely managing access to the devices: Implementing secure user authentication, access controls, and monitoring to limit the vulnerability in energy systems

6. Keeping devices and software updated: Installing software updates and patches as soon as they become available can help to address known security vulnerabilities in energy systems.