**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?

In the industry sector we usually face the weak or easily guessable default passwords in the IoT devices which causes severe threats in the industry.

1. Who might exploit it? Explain.

Default and easily guessable passwords can be easily exploited by Cybercriminals, Competitors, and Script-Kiddies. Cybercriminals are the individuals who use automated tools to try the common default passwords to gain the login information into the IoT devices. Competitors can also use some hacking techniques to find the easily guessable passwords and can access to the IoT devices. Moreover, Script-Kiddies can also use some built in tools to hack into the IoT devise which have default or easily guessable passwords.

1. Why does the vulnerability exist?

The vulnerability may exist because of the following reasons:

* + - 1. Convenience: Many manufacturers choose to use default passwords for their devices in order to make them easier for users to set up and use. However, these default passwords are often simple and easy to guess, making the devices vulnerable to hacking.
      2. Complexity of IoT devices: IoT devices often have a wide range of functionalities and are interconnected with other devices and systems, which can make it difficult to implement security measures that are effective against all potential threats.
      3. Limited resources: Many IoT devices have limited resources (memory, computational power, etc) which can make it hard to implement complex security features or to perform regular security updates.

1. What could be done to limit the vulnerability?

The following can be done to overcome or prevent from this vulnerability:

Use strong, unique passwords: IoT devices should be configured with strong, unique passwords that are at least 12 characters long, contain a mix of uppercase and lowercase letters, numbers, and special characters. Avoid using personal information or common words and phrases in your password.

Multi-factor authentication: IoT devices should have multi-factor authentication enabled whenever possible. This will add an additional layer of security, making it more difficult for unauthorized users to gain access to the device.

Regular software updates: IoT devices should receive regular software updates to address known security vulnerabilities. Users should be prompted to update the device's software regularly.

Apart from the above-mentioned preventions we can also VPNs or use a firewall.