**Information Security**

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

1. Lab 4 - Understand Vulnerabilities of Wireless and Other Common Technologies

**Objectives**

Understand vulnerabilities of wireless and other common technologies.

**Background / Scenario**

Nearly every “secure” system that is used today can be vulnerable to some type of cyberattack.

**Required Resources**

PC or mobile device with internet access.

**Instructions**

* + 1. Click on the below links and watch the videos.

[How hacking actually looks like](https://www.youtube.com/watch?v=jTIUgshJjds)

[Pegasus: the spyware technology that threatens democracy](https://www.youtube.com/watch?v=G7H9uo3j5FQ&t=9s)

["I Remove It Before Using The Phone!" Edward Snowden](https://www.youtube.com/watch?v=0dGqR4ue8dg)

[Top hacker shows us how it's done](https://www.youtube.com/watch?v=hqKafI7Amd8&t=777s)

* + 1. Choose one of the hacks discussed in the videos and use your favorite search engine to conduct some additional research on the hack.
    2. For the hack chosen in Step 1b, answer the questions below. Be prepared to share your work in a full class discussion.

## Answer the following questions.

Questions:

* + 1. **What is the vulnerability being exploited?**

Pegasus malware exploits a vulnerability in the operating system of the targeted device in order to gain access and take control of it. One of the key vulnerabilities that Pegasus was known to exploit was a zero-day vulnerability in Apple's iOS operating system. A zero-day vulnerability is a security hole that is unknown to the software vendor and can be used to exploit the system before a patch or fix is released.

In the case of Pegasus, the malware was able to use this zero-day vulnerability to gain access to the device and install itself without the user's knowledge. This allowed the attackers to take control of the device and access personal information, track the device's location, and intercept phone calls and text messages.

* + 1. **What information, data, or control can be gained by a hacker exploiting this vulnerability?**

When a hacker exploits the zero-day vulnerability in the iOS operating system used by Pegasus malware, they can gain a significant amount of information, data, and control over the infected device. Some of the capabilities of the malware include:

1. Remote access: The malware can take control of the infected device remotely, allowing the attacker to access the device as if they were sitting in front of it.

2. Data collection: Pegasus can collect a wide range of personal information from the device, including contacts, text messages, call logs, emails, and even keystrokes.

3. Location tracking: The malware can track the location of the infected device, allowing the attacker to know where the device is at all times.

4.Interception of communication: Pegasus can intercept phone calls and text messages on the infected device, allowing the attacker to listen in on conversations and read text messages.

5.Camera and microphone access: The malware can also gain access to the device's camera and microphone, allowing the attacker to take photos and record audio without the user's knowledge.

* + 1. **How is the hack performed?**

Pegasus malware is typically delivered to the target device through a phishing attack. In a phishing attack, the attacker sends an email or text message that appears to be from a legitimate source, but contains a link or attachment that, when clicked, will install the malware on the device.

Once the malware is installed, it uses the zero-day vulnerability in the iOS operating system to gain access and take control of the device. The malware is able to do this without the user's knowledge or consent, and once it has access, it can begin collecting information and monitoring the device's activities.

* + 1. **What about this particular hack interested you specifically?**

Pegasus malware is an interesting topic because it is a sophisticated piece of malware that was used in targeted attacks against individuals and organizations, and it exploited a zero-day vulnerability in the iOS operating system, which is widely used by many people around the world.

* + 1. **How do you think this particular hack could be mitigated?**

There are several steps that can be taken to mitigate the risk of falling victim to a hack like the one used by Pegasus malware:

1. Keep the software up to date

2. Be cautious when clicking on the links

3. Use a reputable antivirus software