Lab - Learning the Details of Attacks

Objectives

Research and analyze IoT application vulnerabilities.

Part 1: Conduct a Search of IoT Application Vulnerabilities

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.

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.

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:

a. What is the vulnerability?

b. Who might exploit it? Explain.

c. Why does the vulnerability exist?

d. What could be done to limit the vulnerability?