1. **Information Security**
2. **Chapter 5: Principles of Network Security**
4. Lab 19 - Anatomy of Malware

# Objectives

Research and analyze malware.

# Background / Scenario

Malware, or malicious software, refers to a variety of malicious software programs that can be used to cause harm to computer systems, steal data, and bypass security measures. Malware can also attack critical infrastructure, disable emergency services, cause assembly lines to make defective products, disable electric generators, and disrupt transportation services. Security experts estimate that more than one million new malware threats are released each day. McAfee Labs Threats Report 2019 indicates the discovery of new ransomware techniques, the exposing of billions of accounts through high profile data dumps, significant HTTP web exploitation, defects in Windows, Microsoft Office, and Apple iOS, and continued attacks on IoT personal devices. Find the most current version of the report by doing a web search for McAfee Labs Threats Report.

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

# Required Resources

* PC or mobile device with internet access

# Instructions

## Conduct a Search of Recent Malware

* + - 1. Using your favorite search engine, conduct a search for recent malware. During your search, choose four examples of malware, each one from a different malware type, and be prepared to discuss details on what each does, how it each is transmitted and the impact each cause.

Examples of malware types include: Ransomware, Trojan, Hoax, Adware, Malware, PUP, Exploit, Exploit Kit and Vulnerability. Search for malware by visiting the following websites using the following search terms:

* McAfee Threat Center Threat Landscape Dashboard
* Malwarebytes Labs Threat Center (Top 10 Malware)
* Securityweek.com > virus-threats > virus-malware
* Technewsworld.com > security > malware
  + - 1. Read the information about the malware found from your search in the previous step, choose one and write a short summary that explains what the malware does, how it is transmitted, and the impact it causes.

***Ans:*** A Trojan is a form of harmful software that pretends to be a benign file or program to gain entry to a computer system. Once it's installed, it can execute various malicious activities, including seizing sensitive data, installing more malware, or taking over the victim's computer. Trojans can be distributed through different ways, such as email attachments, infected websites, or peer-to-peer file-sharing networks. They can also be camouflaged as authentic software downloads or updates. The severity of a Trojan's impact is dependent on its specific capabilities and the intentions of its creator. While some Trojans may only generate frustrating pop-ups or slow down the victim's computer, others can capture sensitive data, including login credentials, financial information, or personal documents. In certain circumstances, Trojans may allow an attacker to take control of the victim's computer, converting it into a botnet component utilized for conducting additional attacks or sending spam emails.