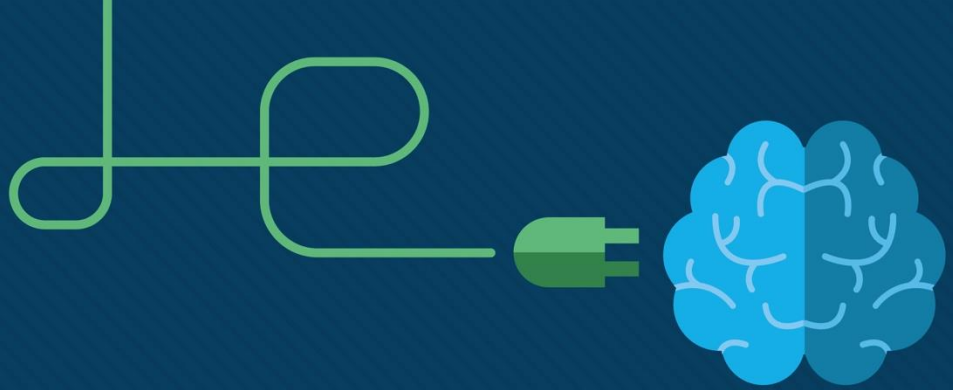


Module 1: The Danger

CyberOps Associate v1.0

Module Objectives

Module Title: The Danger

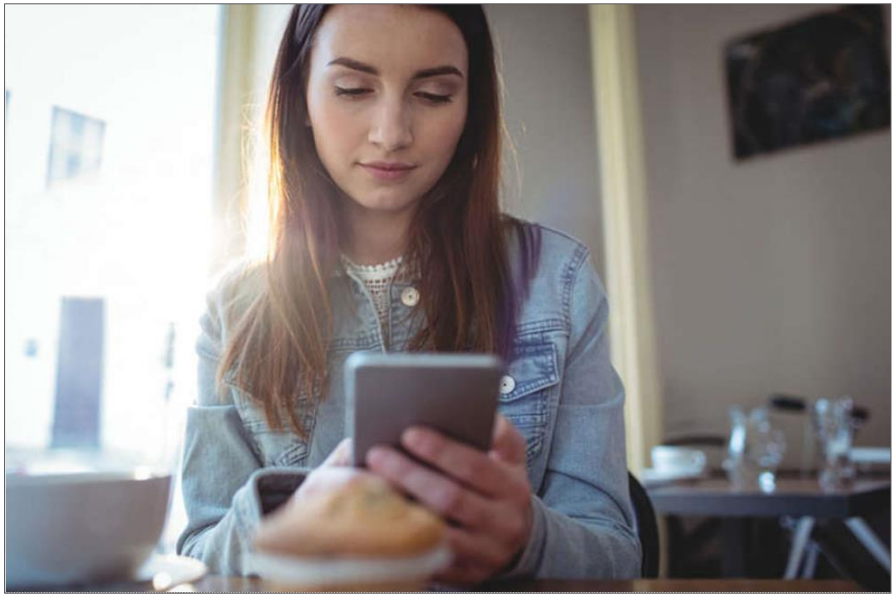
Module Objective: Explain why networks and data are attacked.

Topic Title	Topic Objective
War Stories	Explain why networks and data are attacked.
Threat Actors	Explain the motivations of the threat actors behind specific security incidents.
Threat Impact	Explain the potential impact of network security attacks.

1.1 War Stories

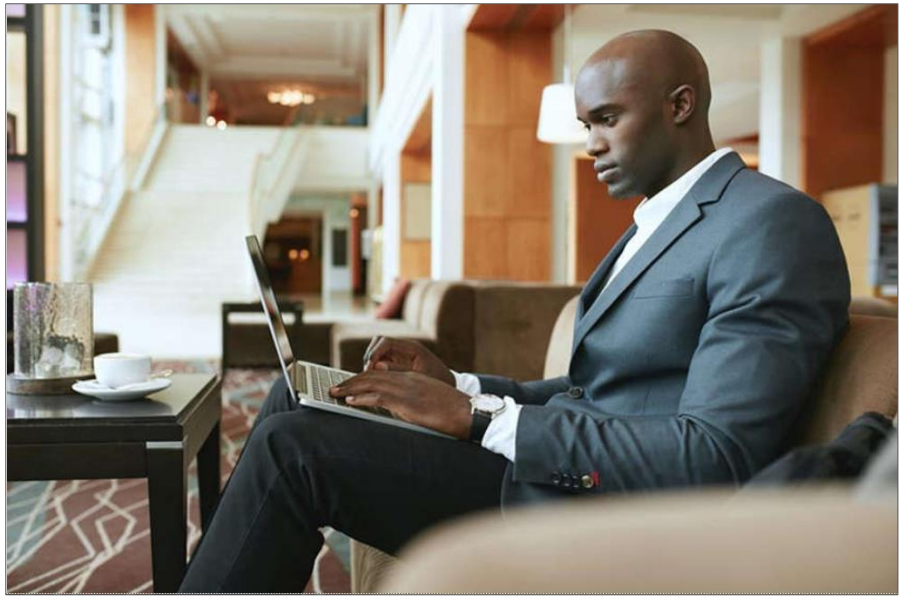
Hijacked People

- Hackers can set up open “rogue” wireless hotspots posing as a genuine wireless network.
- Rogue wireless hotspots are also known as “evil twin” hotspots.



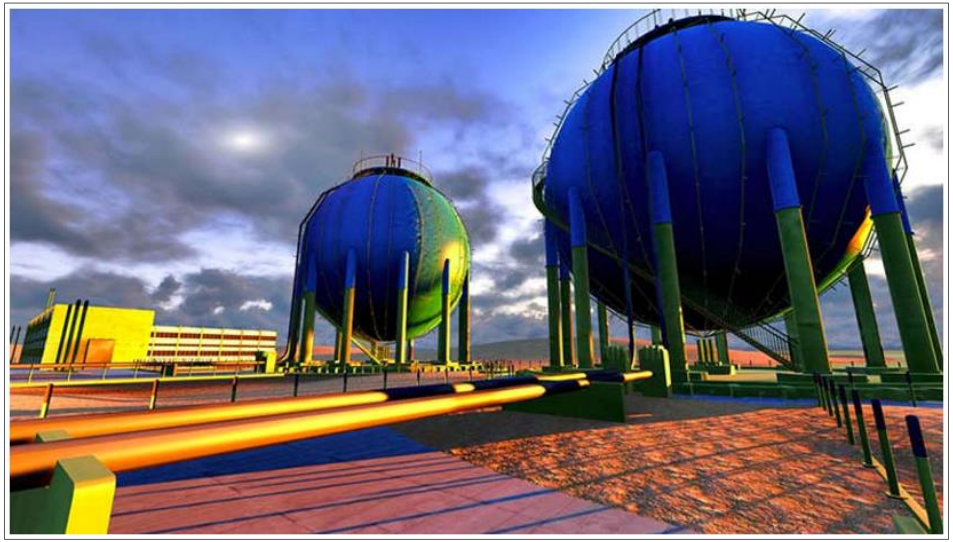
Ransomed Companies

- Employees of an organization are often lured into opening attachments that install ransomware on the employees' computers.
- This ransomware, when installed, begins the process of gathering and encrypting corporate data.
- The goal of the attackers is financial gain, because they hold the company's data for ransom until they are paid.



Targeted Nations

- Some of today's malware is so sophisticated and expensive to create that security experts believe only a nation state or group of nations could possibly have the influence and funding to create it.
- Such malware can be targeted to attack a nation's vulnerable infrastructure, such as the water system or power grid.
- One such malware was the Stuxnet worm that infected USB drives and infiltrated Windows operating systems. It then targeted Step 7 software that was developed by Siemens for their Programmable Logic Controllers (PLCs).



Video - Anatomy of an Attack

Watch this video to view details of a complex attack.

Lab - Installing the Virtual Machine

In this lab, you will complete the following objectives:

- Install VirtualBox on your personal computer
- Download and install the CyberOps Workstation Virtual Machine (VM).

Lab - Cybersecurity Case Studies

In this lab, you will analyze the given cases and answer questions about them.

1.2 Threat Actors

Threat Actors

- Threat actors are individuals or groups of individuals who perform cyberattacks. They include, but are not limited to:
  - Amateurs
  - Hacktivists
  - Organized crime groups
  - State-sponsored groups
  - Terrorist groups
- Cyberattacks are intentional malicious acts meant to negatively impact another individual or organization.

Threat Actors (Contd.)

Amateurs

- They are also known as script kiddies and have little or no skill.
- They often use existing tools or instructions found on the internet to launch attacks.
- Even though they use basic tools, the results can still be devastating.

Hacktivists

- These are hackers who publicly protest against a variety of political and social ideas.
- They post articles and videos, leaking sensitive information, and disrupting web services with illegitimate traffic in Distributed Denial of Service (DDoS) attacks.

Financial Gain

- Much of the hacking activity that consistently threatens our security is motivated by financial gain.
- Cybercriminals want to gain access to bank accounts, personal data, and anything else they can leverage to generate cash flow.

Trade Secrets and Global Politics

- At times, nation states hack other countries, or interfere with their internal politics.
- Often, they may be interested in using cyberspace for industrial espionage.
- The theft of intellectual property can give a country a significant advantage in international trade.

How Secure is the Internet of Things?

- The Internet of Things (IoT) helps individuals connect things to improve their quality of life.
- Many devices on the internet are not updated with the latest firmware. Some older devices were not even developed to be updated with patches. These two situations create opportunity for threat actors and security risks for the owners of these devices.

Lab - Learning the Details of Attacks

In this lab, you will research and analyze IoT application vulnerabilities.

1.3 Threat Impact

PII, PHI, and PSI

- Personally Identifiable Information (PII) is any information that can be used to positively identify an individual, for example, name, social security number, birthdate, credit card numbers etc.
- Cybercriminals aim to obtain these lists of PII that can then be sold on the dark web. Stolen PII can be used to create fake financial accounts, such as credit cards and short-term loans.
- The medical community creates and maintains Electronic Medical Records (EMRs) that contain Protected Health Information (PHI), a subset of PII.
- Personal Security Information (PSI), another type of PII, includes usernames, passwords, and other security-related information that individuals use to access information or services on the network.

Lost Competitive Advantage

- The loss of intellectual property to competitors is a serious concern.
- An additional major concern is the loss of trust that comes when a company is unable to protect its customers' personal data.
- The loss of competitive advantage may come from this loss of trust rather than another company or country stealing trade secrets.

Politics and National Security

- It is not just businesses that get hacked.
- State-supported hacker warriors can cause disruption and destruction of vital services and resources within an enemy nation.
- The internet has become essential as a medium for commercial and financial activities. Disruption of these activities can devastate a nation’s economy.

Lab - Visualizing the Black Hats

In this lab, you will research and analyze cybersecurity incidents to create scenarios highlighting how organizations can prevent or mitigate an attack.

1.4 The Danger Summary

What Did I Learn in this Module?

- Threat actors can hijack banking sessions and other personal information by using “evil twin” hotspots.
- Threat actors include, but are not limited to, amateurs, hacktivists, organized crime groups, state sponsored, and terrorist groups.
- As the Internet of Things (IoT) expands, webcams, routers, and other devices in our homes are also under attack.
- Personally Identifiable Information (PII) is any information that can be used to positively identify an individual.
- The medical community creates and maintains Electronic Medical Records (EMRs) that contain Protected Health Information (PHI), a subset of PII.
- Personal Security Information (PSI) includes usernames, passwords, and other security-related information that individuals use to access information or services on the network.


CISCO