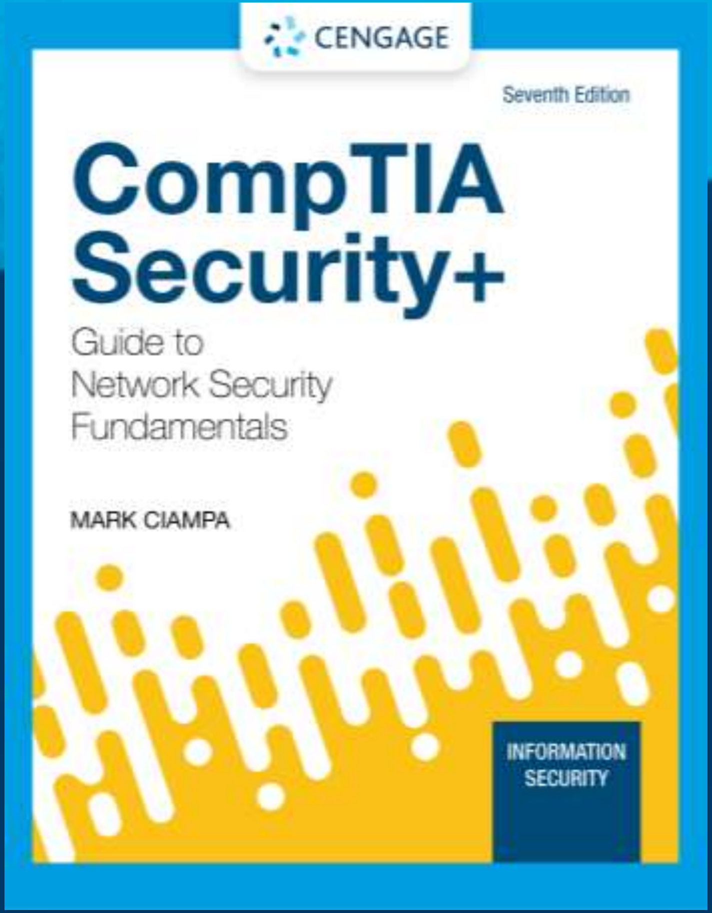


CompTIA Security+ Guide to Network Security Fundamentals, 7th Edition

Module 1: Introduction to Security

CENGAGE

Icebreaker: Class Introduction and Discussion

1. Question: Why is it important for all computer users, not just IT professionals, to understand the importance of network and computer security?
2. Each student should introduce themselves, explain why they are taking the class, and give their answer to the question.
3. If this is an online class, responses can be posted in the discussion board and each student should respond with a minimum of 100 words.

Module Objectives

By the end of this module, you should be able to:

1. Define information security and explain why it is important
2. Identify threat actors and their attributes
3. Describe the different types of vulnerabilities and attacks
4. Explain the impact of attacks

What is Information Security?

- The first step in understanding security is to define exactly what it is
- Understanding Security
  - *Security* is:
    - To be free from danger, which is the goal of security
    - The process that achieves that freedom
  - As security is increased, convenience is often decreased
    - The more secure something is, the less convenient it may become to use

Defining Information Security (1 of 2)

- Information security describes the tasks of securing digital information, whether it is:
  - Manipulated by a microprocessor
  - Preserved on a storage device
  - Transmitted over a network
- There are three types of information protection (often called the CIA Triad) :
  - *Confidentiality*
    - Only approved individuals may access information
  - *Integrity*
    - Ensures information is correct and unaltered
  - *Availability*
    - Ensures information is accessible to authorized users

Defining Information Security (2 of 2)

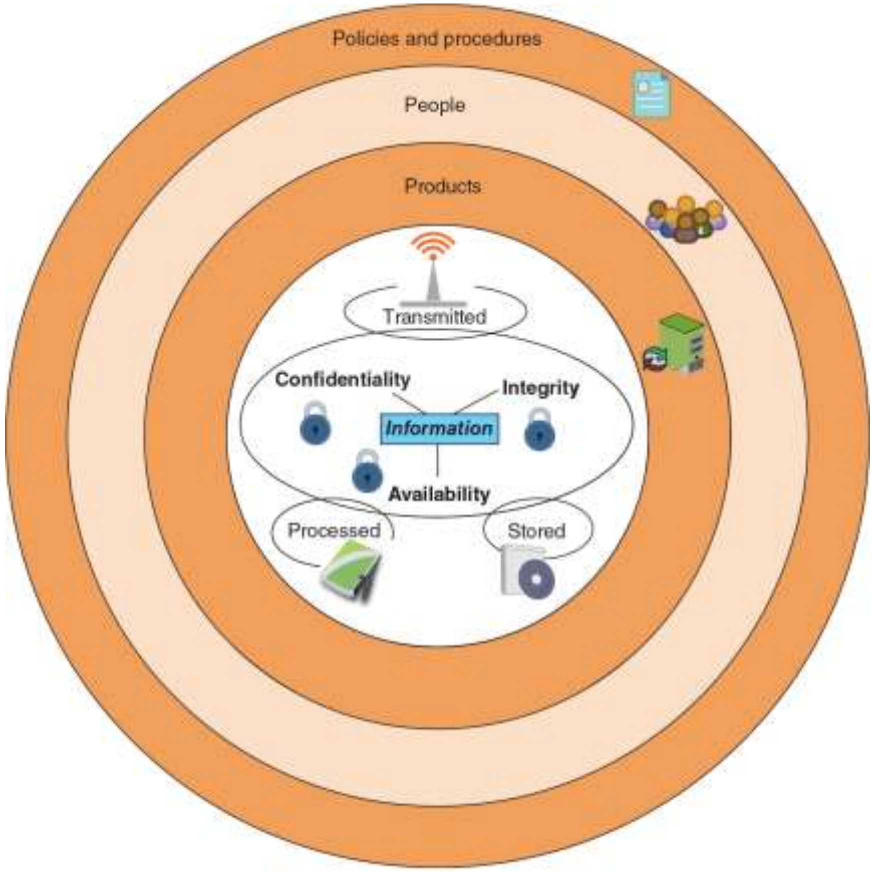


Figure 1-2 Information security layers

Figure 1-2 Information security layers

Knowledge Check Activity 1

As security increases, the convenience of using a system is also increased.

a. True

b. False

Knowledge Check Activity 1: Answer

As security increases, the convenience of using a system is also increased.

Answer: b. False

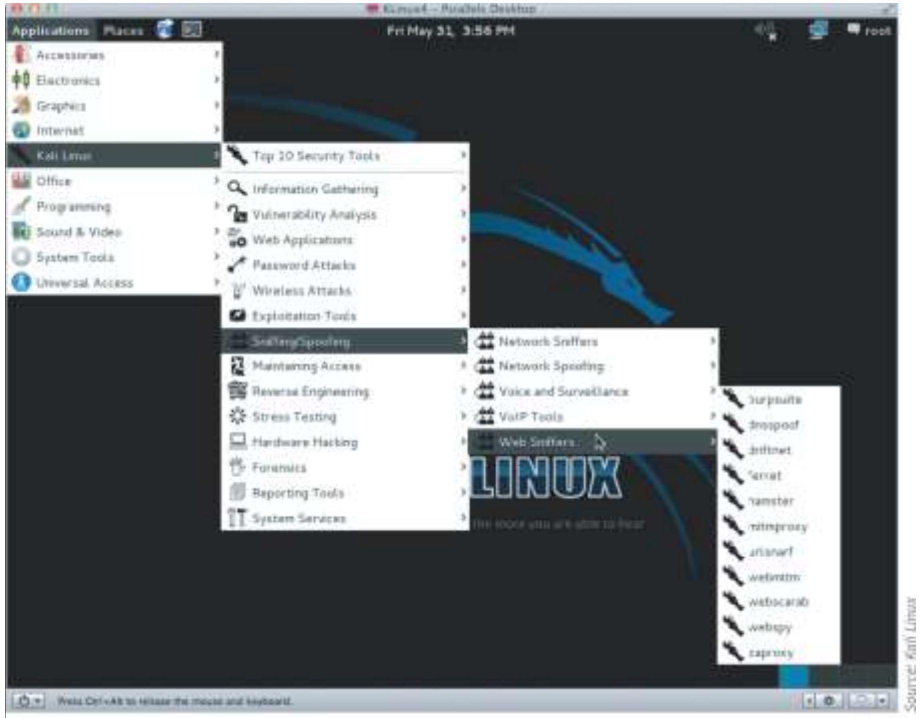
As security increases, users of computer systems and software are usually required to perform additional tasks to abide by the security policies, making the use of they systems less convenient but more secure.

Who Are the Threat Actors?

- A **threat actor** is an individual or entity responsible for cyber incidents against the technology equipment of enterprises and users
    - The generic term *attacker* is also commonly used
- Financial crime is often divided into three categories based on targets:
    - *Individual users*
    - *Enterprises*
    - *Governments*
- There are three types of hackers
    - **Black hat hackers**
    - **White hat hackers**
    - **Gray hat hacker**

Script Kiddies

- **Script kiddies** are individuals who want to perform attacks, yet lack technical knowledge to carry them out
  - They download freely available automated attack software and use it to attack



Source: Kali Linux

Figure 1-3 Menu of attack tools

Hacktivists

- Individuals that are strongly motivated by ideology (for the sake of their principles or beliefs) are **hacktivists**
- The types of attacks by hacktivists often involved breaking into a website and changing its contents as a means of a political statement
- Other attacks were retaliatory: hacktivists have disabled a bank’s website that didn’t allow online payments deposited into accounts belonging to groups supported by hacktivists

State Actors

- Governments are increasingly employing their own state-sponsored attackers for launching cyberattacks against their foes
  - These attackers are known as **state actors**
- Many security researchers believe that state actors might be the deadliest of any threat actors
- State actors are often involved in multiyear intrusion campaigns targeting highly sensitive economic, proprietary, or national security information
  - A new class of attacks called **advanced persistent threat** (**APT**)
- APTs are most commonly associated with state actors

Insiders

- Employees, contractors, and business partners can pose an **insider threat** of manipulating data from the position of a trusted employee
- These attacks are harder to recognize because they come from within the enterprise
- Six out of 10 enterprises reported being a victim of at least one insider attack during 2019
- The focus of the insiders was:
  - Intellectual property (IP) theft – 43%
  - Sabotage – 41%
  - Espionage – 32%

Other Threat Actors

Threat Actor	Description	Explanation
Competitors	Launch attacks against an opponent’s system to steal classified information.	May steal new product research or a list of current customers to gain a competitive advantage.
Criminal syndicates	Move from traditional criminal activities to more rewarding and less risky online attacks.	Usually run by a small number of experienced online criminal networks that do not commit crimes themselves but act as entrepreneurs.
Shadow IT	Employees become frustrated with the slow pace of acquiring technology, so they purchase and install their own equipment or resources in violation of company policies.	Installing personal equipment, unauthorized software, or using external cloud resources can create a weakness or expose sensitive corporate data.
Brokers	Sell their knowledge of a weakness to other attackers or governments.	Individuals who uncover weaknesses do not report it to the software vendor but instead sell them to the highest bidder who is willing to pay a high price for the unknown weakness.
Cyberterrorists	Attack a nation’s network and computer infrastructure to cause disruption and panic among citizens.	Targets may include a small group of computers or networks that can affect the largest number of users, such as the computers that control the electrical power grid of a state or region.

Knowledge Check Activity 2

Which type of threat actor is often involved in multiyear intrusion campaigns targeting highly sensitive economic, proprietary, or national security information?

a. Insider

b. State actor

c. Hacktivist

d. Script kiddie

Knowledge Check Activity 2: Answer

Which type of threat actor is often involved in multiyear intrusion campaigns targeting highly sensitive economic, proprietary, or national security information?

b. State actor

A state actor differs from other threat actors in that their attacks are sponsored by their government. The attacks are targeted at foreign governments and state infrastructures with the goal of gaining a competitive advantage on the world stage or in an actual warfare situation.

Vulnerabilities and Attacks

- One of the most successful types of attack is social engineering
  - Social engineering does not even exploit technology vulnerabilities
- Each successful attack has serious ramifications

Vulnerabilities (1 of 4)

- A *vulnerability* is the state of being exposed to the possibility of being attacked or harmed
- Cybersecurity vulnerabilities can be categorized into platforms, configurations, third parties, patches, and zero-day vulnerabilities
- Platforms
  - A computer platform is a system that consists of the hardware device and an OS that runs software
  - All platforms have vulnerabilities to some degree, some platforms have serious vulnerabilities including:
    - **Legacy platforms**
    - **On-premises platforms**
    - **Cloud platforms**

Vulnerabilities (2 of 4)

- Configuration settings are often not properly implemented
  - Results in weak configurations
- See Table 1-3 for a list of several weak configurations that can result in vulnerabilities

Vulnerabilities (3 of 4)

- Third Parties
  - Almost all businesses use external entities known as third parties
  - Examples of third parties include: outsourced code development, data storage facilities
  - Vendor management is the process organizations use to monitor and manage the interactions with all of their external third parties
  - Connectivity between the organization and the third party is known as system integration
  - One of the major risks of third-party system integration involves the principle of the weakest link

Vulnerabilities (4 of 4)

- Patches
  - As important as patches are, they can create vulnerabilities:
    - *Difficulty patching firmware*
    - *Few patches for application software*
    - *Delays in patching OSs*
- Zero Day
  - Vulnerabilities can be exploited by attackers before anyone else even knows it exists
  - This type of vulnerability is called a zero day because it provides zero days of warning
  - Zero-day vulnerabilities are considered extremely serious

Attack Vectors

- An **attack vector** is a pathway or avenue used by a threat actor to penetrate a system
- Attack vectors can be grouped into the following general categories:
  - *Email*
  - *Wireless*
  - *Removable media*
  - *Direct access*
  - *Social media*
  - *Supply chain*
  - *Cloud*

Social Engineering Attacks (1 of 8)

- **Social engineering** is a means of **eliciting information** (gathering data) by relying on the weaknesses of individuals
  - It is also used as influence campaigns to sway attention and sympathy in a particular direction
  - These campaigns can be found exclusively on social media or may be combined with other sources
- Psychological Principles
  - Attackers use a variety of techniques to gain trust:
    - *Provide a reason*
    - *Project confidence*
    - *Use evasion and diversion*
    - *Make them laugh*

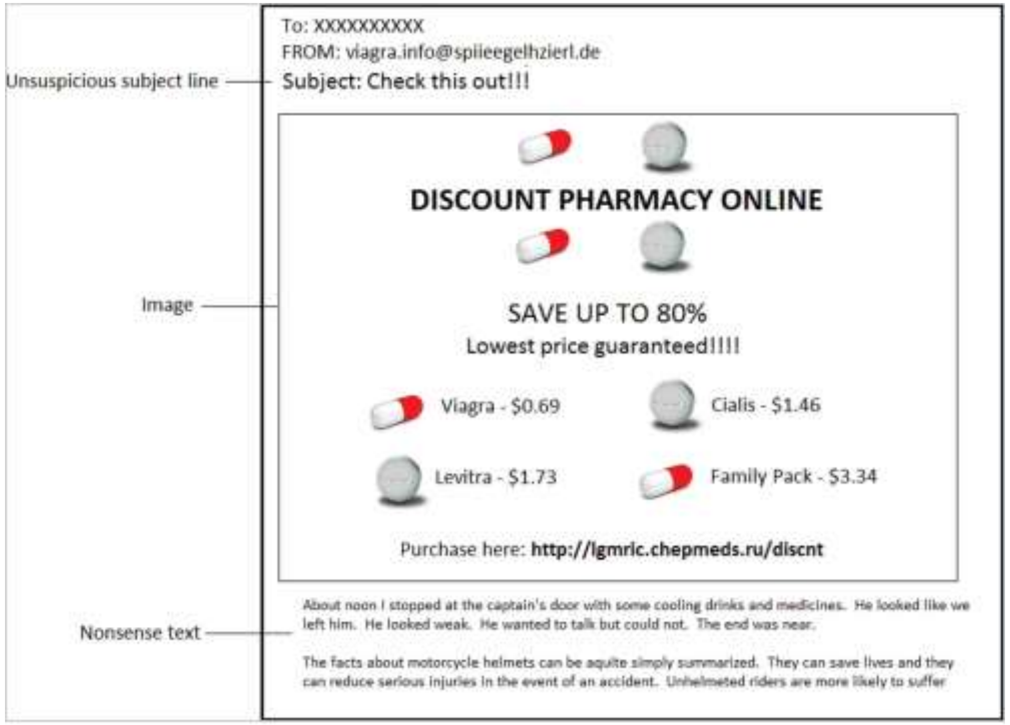
Social Engineering Attacks (2 of 8)

- Social engineering psychological approaches often involve:
  - **Impersonation** is masquerading as a real or fictitious character and then playing the role of that person with a victim
  - **Phishing** is sending an email message or displaying a web announcement that falsely claims to be from a legitimate enterprise in an attempt to trick the user into surrender private information or taking action
    - Variations on phishing attacks:
      - *Spear phishing*
      - *Whaling*
      - *Vishing*
      - *Smishing*

Social Engineering Attacks (3 of 8)

- Social engineering psychological approaches often involve (continued):
  - **Redirection** is when an attacker directs a user to a fake lookalike site filled with ads for which the attacker receives money for traffic generated to the site
    - Attackers purchase fake sites because the domain names of sites are spelled similarly to actual sites (called **typo squatting**)
    - Another redirection technique is **pharming** where the attacker attempts to exploit how a URL is converted into its corresponding IP address
  - **Spam** is unsolicited email that is sent to a large number of recipients
    - Text-based spam messages can be filtered
    - Image spam cannot be filtered
    - **Spim** is spam delivered through instant messaging (IM) instead of email

Social Engineering Attacks (4 of 8)



To: XXXXXXXXXX
FROM: viagra.info@spiieegelhzierl.de
Subject: Check this out!!!

DISCOUNT PHARMACY ONLINE

SAVE UP TO 80%
Lowest price guaranteed!!!!

Viagra - $0.69	Cialis - $1.46
Levitra - $1.73	Family Pack - $3.34

Purchase here: **http://lgmrlc.chepmeds.ru/discnt**

About noon I stopped at the captain's door with some cooling drinks and medicines. He looked like we left him. He looked weak. He wanted to talk but could not. The end was near.

The facts about motorcycle helmets can be aquite simply summarized. They can save lives and they can reduce serious injuries in the event of an accident. Unhelmeted riders are more likely to suffer

Figure 1-6 Image spam

Figure 1-6 Image spam

Social Engineering Attacks (5 of 8)

- Social engineering psychological approaches often involve (continued):
  - **Hoaxes** are false warnings, often contained in an email message claiming to come from the IT department
    - The hoax purports that there is a “deadly virus” circulating through the Internet and the recipient should erase specific files or change security configurations
  - A **watering hole attack** is directed toward a smaller group of specific individuals

Social Engineering Attacks (6 of 8)

- Physical Procedures
  - Physical attacks take advantage of user actions that can result in compromised security
  - Three of the most common physical procedures are dumpster diving, tailgating, and shoulder surfing
  - **Dumpster Diving** involves digging through trash receptacles to find information that can be useful in an attack
    - An electronic variation of physical dumpster diving is to use the Google search engine to look for documents and data posted online that can be used in an attack (called *Google dorking*)

Social Engineering Attacks (7 of 8)

Item retrieved	Why useful
Calendars	A calendar can reveal which employees are out of town at a particular time.
Inexpensive computer hardware, such as USB flash drives or portal hard drives	These devices are often improperly disposed of and might contain valuable information.
Memos	Seemingly unimportant memos can often provide small bits of useful information for an attacker who is building an impersonation.
Organizational charts	These identify individuals within the organization who are in positions of authority.
Phone directories	A phone directory can provide the names and telephone numbers of individuals in the organization to target or impersonate.
Policy manuals	These may reveal the true level of security within the organization.
System manuals	A system manual can tell an attacker the type of computer system that is being used so that other research can be conducted to pinpoint vulnerabilities.

Social Engineering Attacks (8 of 8)

- Physical Procedures (continued)
  - **Tailgating** occurs when an authorized person opens an entry door, one or more individuals can follow behind and also enter
  - **Shoulder Surfing** allows an attacker to casually observe someone entering secret information, such as the security codes on a door keypad

Knowledge Check Activity 3

Which type of attack is NOT a form of social engineering attack?

a. Watering hole

b. Hoax

c. Zero day

d. Tailgating

Knowledge Check Activity 3: Answer

Which type of attack is NOT a form of social engineering attack?

c. Zero day

Zero day attacks are attacks on vulnerabilities in software systems that are discovered by threat actors before the system developers can issue a patch to correct the vulnerability.

Impacts of Attacks (1 of 3)

- A successful attack always results in several negative impacts
- These impacts can be classified as:
  - Data impacts
  - Effects on the organization

Impacts of Attacks (2 of 3)

Impact	Description	Example
Data loss	Destroying data so that it cannot be recovered	Maliciously erasing patient data used for cancer research
Data exfiltration	Stealing data to distribute it to other parties	Taking a list of current customers and selling it to a competitor
Data breach	Stealing data to disclose it in an unauthorized fashion	Stealing credit card numbers to sell to other threat actors
Identity theft	Taking personally identifiable information to impersonate someone	Stealing a Social Security number to secure a bank loan in the victim's name

Impacts of Attacks (3 of 3)

- Effects on the Enterprise
  - The attack may make systems inaccessible (**availability loss**)
    - This results in lost productivity (**financial loss**)
  - Attacks may effect the public perception of the enterprise (**reputation**)

Knowledge Check Activity 4

Which type of data impact would result if an attacker stole a list of customers for the purpose of selling the list to a competitor?

a. Data loss

b. Data exfiltration

c. Data breach

d. Identity theft

Knowledge Check Activity 4: Answer

Which type of data impact would result if an attacker stole a list of customers for the purpose of selling the list to a competitor?

b. Data exfiltration

Data exfiltration is the stealing of data for the purpose of distributing it or selling it to other parties. Data exfiltration is a specific type of data breach but not all data breaches involve data exfiltration. For example, a data breach might change or corrupt data or deny access to the data by its owner.

Self-Assessment

Rate your competence of the following module objectives on a scale of 1 to 5 where 5 indicates you have full confidence in your competence of that objective and 1 indicates you have very little to no confidence in your competence of that objective. If you self-score less than 4 you should consider reviewing the module and related exercises:

1. Define information security and explain why it is important

2. Identify threat actors and their attributes

3. Describe the different types of vulnerabilities and attacks

4. Explain the impact of attacks

Summary (1 of 2)

- Attacks against information security have grown astronomically in recent years
- The information security workforce is usually divided into two broad categories: information security managerial personnel and information security technical personnel
- Security can be defined as the necessary steps to protect from harm
- The threat actors fall into several categories and exhibit different attributes
- Script kiddies do their work by downloading automated attack software from websites and using it to break into computers
- Cybersecurity vulnerabilities are often categorized into five broad categories: platforms, configurations, third parties, patches, and zero-day vulnerabilities
- Modern hardware and software platforms provide a wide array of features and security settings

Summary (2 of 2)

- An attack vector is a pathway or avenue used by a threat actor to penetrate a system
- Social engineering is a means of eliciting information by relying on the weaknesses of individuals
- A successful attack always results in several negative impacts: data loss, data exfiltration, data breach, and identity theft