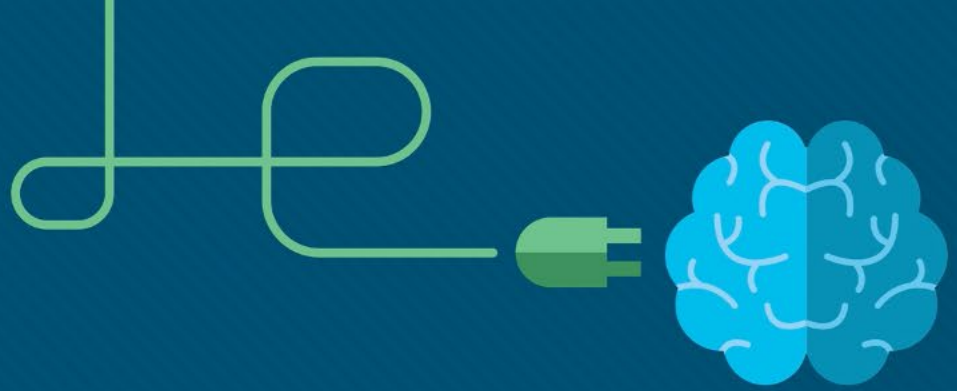


Module 2: Securing Networks

Cybersecurity Essentials 3.0

Module Objectives

Module Title: Securing Networks

Module Objective: Explain network security principles.

Topic Title	Topic Objective
Current State of Affairs	Explain the threats, vulnerabilities, and attacks that occur in the various domains.
Who is Attacking Our Network?	Explain how network threats have evolved.

2.1 Current State of Affairs

Video - Anatomy of an Attack

This video shows a sampling of what cybersecurity professionals do. Cisco Security Architect, Matt Carling, offers the defender's point of view and why a "Defense in Depth" layer approach is best.

Networks Are Targets

- Computer networks are routinely under attack.
- Kapersky maintains the interactive Cyberthreat Real-Time Map display of current network attacks.
- The attack data is submitted from Kapersky network security products deployed worldwide.
- Many similar tools are available on the internet and can be found by searching for cyber threat maps.

Reasons for Network Security

- Network security relates directly to the business continuity of an organization.
- Network security breaches can disrupt e-commerce, cause the loss of business data, threaten people's privacy, and compromise the integrity of information.
- These breaches can result in lost revenue for corporations, theft of intellectual property, lawsuits, and even threaten public safety.
- Maintaining a secure network ensures the safety of network users and protects commercial interests.
- Keeping a network secure requires vigilance from an organization's network security professionals.
- Many tools help network administrators adapt, develop, and implement threat mitigation techniques. Two examples are:
  - Cisco Talos Intelligence Group website
  - Cisco Product Security Incident Response Team (PSIRT)

Vectors of Network Attacks

- An attack vector is a path by which a threat actor can access a server, host, or network.

- Attack vectors originate from inside or outside the corporate network.
  - An internal user, such as an employee, can accidentally or intentionally:
    - Steal and copy confidential data to removable media, email, messaging software, and other media.
    - Compromise internal servers or network infrastructure devices.
    - Disconnect a critical network connection and cause a network outage.
    - Connect an infected USB drive to a corporate computer system.
  - Internal threats have the potential to cause more significant damage than external threats.

- Network security professionals must implement tools and apply techniques to mitigate external and internal threats.

Data Loss

Term	Definition
Email/Social Networking	The most common vector for data loss includes instant messaging software and social media sites. For instance, intercepted email or IM messages could be captured and reveal confidential information.
Unencrypted Devices	A stolen corporate laptop typically contains confidential organizational data. The thief can retrieve valuable personal data if the data is not stored using an encryption algorithm.
Cloud Storage Devices	Saving data to the cloud has many potential benefits. However, sensitive data can be lost if access to the cloud is compromised due to weak security settings.
Removable Media	One risk is that an employee could perform an unauthorized transfer of data to a USB drive. Another chance is that a USB drive containing valuable corporate data could be lost.
Hard Copy	Corporate data should be disposed of thoroughly. For example, confidential data should be shredded when no longer required. Otherwise, a thief could retrieve discarded reports and gain valuable information.
Improper Access Control	Passwords are the first line of defense. Stolen passwords or weak passwords which have been compromised can provide an attacker easy access to corporate data.

Packet Tracer - Investigate a Threat Landscape

In this Packet Tracer activity, you will meet the following objectives:

- Part 1: Investigate the Bottom Toolbar
- Part 2: Investigate Devices in a Wiring Closet
- Part 3: Connect End Devices to Networking Devices
- Part 4: Install a Backup Router
- Part 5: Configure a Hostname
- Part 6: Explore the Rest of the Network

2.2 Who is Attacking Our Network?

Threat, Vulnerability, and Risk

We are under attack and attackers want access to our assets (data, intellectual property, servers, computers, smart phones, tablets, and more).

Term	Explanation
Threat	A potential danger to an asset such as data or the network itself.
Vulnerability	A weakness in a system or its design that a threat could exploit.
Attack surface	An attack surface is the total sum of the vulnerabilities in a given system that is accessible to an attacker. The attack surface describes different points where an attacker could get into a plan and where they could get data out of the system.
Exploit	The mechanism that is used to leverage a vulnerability to compromise an asset. Exploits may be remote or local. A remote exploit works over the network without prior access to the target system. The attacker does not need an account in the end system to exploit the vulnerability. In a local exploit, the threat actor has some user or administrative access to the end system. A local exploit does not necessarily mean the attacker has physical access to the end system.
Risk	The likelihood that a particular threat will exploit a specific vulnerability of an asset and result in an undesirable consequence.

Threat, Vulnerability, and Risk (Cont.)

There are four common ways to manage risk:

Risk Management Strategy	Explanation
Risk acceptance	This is when the cost of risk management options outweighs the cost of the risk itself. The risk is accepted, and no action is taken.
Risk avoidance	This means avoiding any exposure to the risk by eliminating the activity or device that presents the danger. Removing an activity to prevent risk, and any possible benefits from the training are also lost.
Risk reduction	This reduces exposure to risk or the impact of risk by taking action to decrease the risk. It is the most commonly used risk mitigation strategy. This strategy requires careful evaluation of the costs of loss, the mitigation strategy, and the benefits gained from the operation or activity at risk.
Risk transfer	Some or all of the risk is transferred to a willing third party, such as an insurance company.

Hacker vs. Threat Actor

The term “hacker” has a variety of meanings:

- A clever programmer capable of developing new programs and coding changes to existing programs to make them more efficient.
- A network professional that uses sophisticated programming skills to ensure that networks are not vulnerable to attack.
- A person who tries to gain unauthorized access to devices on the internet.
- An individual who run programs to prevent or slow network access to many users, or corrupt or wipe out data on servers.

An attack vector is a path by which a threat actor can gain access to a server, host, or network.

Hacker vs. Threat Actor (Cont.)

White hat hacker, black hat hacker, and grey hat hacker:

- White hat hackers are ethical hackers who use their programming skills for good, ethical, and legal purposes. They may perform network penetration tests in an attempt to compromise networks and systems by using their knowledge of computer security systems to discover network vulnerabilities.
- Grey hat hackers are individuals who commit crimes and do arguably unethical things, but not for personal gain or to cause damage. An example would be someone who compromises a network without permission and then discloses the vulnerability publicly.
- Black hat hackers are unethical criminals who violate computer and network security for personal gain or for malicious reasons, such as attacking networks. Black hat hackers exploit vulnerabilities to compromise computer and network systems.

Evolution of Threat Actors

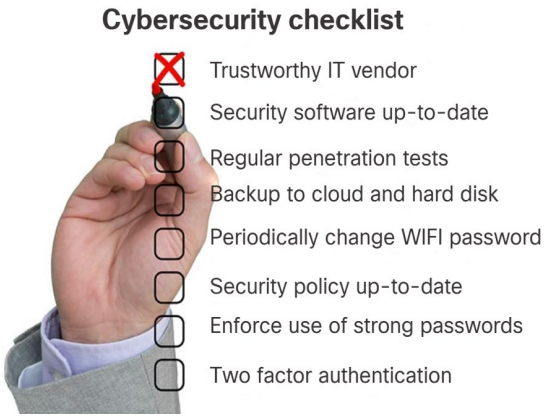
Threat Actors	Explanation
Script kiddies	Script kiddies emerged in the 1990s and refer to teenagers or inexperienced threat actors running existing scripts, tools, and exploits to cause harm, but typically not for profit.
Vulnerability brokers	Vulnerability brokers typically refer to grey hat hackers who attempt to discover exploits and report them to vendors, sometimes for prizes or rewards.
Hacktivists	Hacktivists is a term that refers to grey hat hackers who rally and protest against different political and social ideas. Hacktivists publicly protest against organizations or governments by posting articles, and videos, leaking sensitive information and performing distributed denial of service (DDoS) attacks.
Cybercriminals	Cybercriminal is a term for black hat hackers who are self-employed or working for large cybercrime organizations. Cybercriminals steal billions of dollars from consumers and businesses each year.
State-sponsored	State-Sponsored hackers are threat actors who steal government secrets, gather intelligence, and sabotage networks of foreign governments, terrorist groups, and corporations. Most countries in the world participate to some degree in state-sponsored hacking. Depending on a person's perspective, these are either white or black hat hackers.

Cybercriminals

- Cybercriminals are threat actors motivated to make money using any means necessary.
- While sometimes cybercriminals work independently, they are more often financed and sponsored by criminal organizations.
- Cybercriminals operate in an underground economy where they buy, sell, and trade exploits and tools.
- They also buy and sell the personal information and intellectual property they steal from victims.
- Cybercriminals target small businesses, consumers, and large enterprises and industries.

Cybersecurity Tasks

- Threat actors target the vulnerable end devices of home users, small-to-medium-sized businesses, and large public and private organizations.
- To make the internet and networks safer and more secure, we must develop good cybersecurity awareness.
- Cybersecurity is a shared responsibility that all users must practice.
- Organizations must take action and protect their assets, users, and customers. They must develop and practice cybersecurity tasks like those listed in the figure.



Cyber Threat Indicators

- Many network attacks can be prevented by sharing information about indicators of compromise (IOC).
- IOCs can be features that identify malware files, IP addresses of servers used in attacks, filenames, and characteristic changes made to end system software, among others.
- IOCs help cybersecurity personnel identify what has happened in an attack and develop defenses against the attack.
- Indicators of attack (IOA) focus more on the motivation behind an attack and the potential means by which threat actors have, or will, compromise vulnerabilities to gain access to assets.
- IOAs are concerned with the strategies that attackers use. For this reason, IOAs can help generate a proactive security approach rather than responding to a single threat.
- Defending against a strategy can prevent future attacks that utilize the same or similar strategy.

Threat Sharing and Building Cybersecurity Awareness

- Governments are now actively promoting cybersecurity. The US Cybersecurity Infrastructure and Security Agency (CISA) is leading efforts to automate cybersecurity information sharing with public and private organizations at no cost.
- CISA uses a system called Automated Indicator Sharing (AIS). AIS enables the sharing of attack indicators between the US government and the private sector as soon as threats are verified.
- The CISA and the National Cyber Security Alliance (NCSA) promote cybersecurity to all users.
- The CISA and NCSA have an annual October campaign called “National Cybersecurity Awareness Month” (NCASM). This campaign promotes and raises awareness about cybersecurity.

Threat Sharing and Building Cybersecurity Awareness (Cont.)

- The CISA and NCSA have an annual campaign every October called “National Cybersecurity Awareness Month” (NCASM). The campaign provides material on a wide variety of security topics, including:
  - Social media safety
  - Updating privacy settings
  - Awareness of device app security
  - Keeping software up-to-date
  - Safe online shopping
  - Wi-Fi safety
  - Protecting customer data

2.3 Securing Networks Summary

What Did I Learn in this Module?

- Network security relates directly to an organization's business continuity.
- Network security breaches can disrupt e-commerce, cause the loss of business data, threaten people's privacy, and compromise the integrity of information.
- Many tools, including the Cisco Talos Intelligence Group, are available to help network administrators adapt, develop, and implement threat mitigation techniques.
- An attack vector is a path by which a threat actor can access a server, host, or network.
- Risk management is the process that balances the operational costs of providing protective measures with the gains achieved by protecting the asset.
- Hacker is a term used to describe a threat actor. Threat actors include script kiddies, vulnerability brokers, hacktivists, cybercriminals, and state-sponsored hackers.
- Many network attacks can be prevented by sharing information about IOCs. Many governments are promoting cybersecurity. CISA and NCSA are examples of such organizations.