Security Threats and Vulnerabilities

16.1.1

Types of Threats

Wired and wireless computer networks are essential to everyday activities. Individuals and organizations depend on their computers and networks. Intrusion by an unauthorized person can result in costly network outages and loss of work. Attacks on a network can be devastating and can result in a loss of time and money due to damage, or theft of important information or assets.

Intruders can gain access to a network through software vulnerabilities, hardware attacks, or through guessing someone's username and password. Intruders who gain access by modifying software or exploiting software vulnerabilities are called threat actors.

After the threat actor gains access to the network, four types of threats may arise.

Click each button for information about each threat.

Information Theft | Data Loss and Manipulation | Identity Theft | Disruption of Service

Disruption of service is preventing legitimate users from accessing services to which they are entitled. Examples include denial of service (DoS) attacks on servers, network devices, or network communications links.

16.1.2

Types of Vulnerabilities

Vulnerability is the degree of weakness in a network or a device. Some degree of vulnerability is inherent in routers, switches, desktops, servers, and even security devices. Typically, the network devices under attack are the endpoints, such as servers and desktop computers.

There are three primary vulnerabilities or weaknesses: technological, configuration, and security policy. All three of these sources of vulnerabilities can leave a network or device open to various attacks, including malicious code attacks and network attacks.

Click each button for a table with examples and a description of each type of vulnerability.

Technological Vulnerabilities | Configuration Vulnerabilities | Policy Vulnerabilities

Policy Vulnerabilities

Vulnerability	Description
Lack of written security policy	A security policy cannot be consistently applied or enforced if it is not written down.
Politics	Political battles and turf wars can make it difficult to implement a consistent security policy.
Lack of authentication continuity	Poorly chosen, easily cracked, or default passwords can allow unauthorized access to the network.
Logical access controls not applied	Inadequate monitoring and auditing allow attacks and unauthorized use to continue, wasting company resources. This could result in legal action or termination against IT technicians, IT management, or even company leadership that allows these unsafe conditions to persist.
Software and hardware installation and changes do not follow policy	Unauthorized changes to the network topology or installation of unapproved application create or enable holes in security.
Disaster recovery plan is nonexistent	The lack of a disaster recovery plan allows chaos, panic, and confusion to occur when a natural disaster occurs or a threat actor attacks the enterprise.

16.1.3

Physical Security

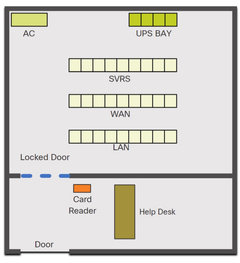
An equally important vulnerable area of the network to consider is the physical security of devices. If network resources can be physically compromised, a threat actor can deny the use of network resources.

The four classes of physical threats are as follows:

- **Hardware threats** – This includes physical damage to servers, routers, switches, cabling plant, and workstations.
- **Environmental threats** – This includes temperature extremes (too hot or too cold) or humidity extremes (too wet or too dry).
- **Electrical threats** – This includes voltage spikes, insufficient supply voltage (brownouts), unconditioned power (noise), and total power loss.
- **Maintenance threats** – This includes poor handling of key electrical components (electrostatic discharge), lack of critical spare parts, poor cabling, and poor labeling.

A good plan for physical security must be created and implemented to address these issues. The figure shows an example of physical security plan.

Plan Physical Security to Limit Damage to Equipment



- Secure computer room.
- Implement physical security to limit damage to the equipment.

Step 1. Lock up equipment and prevent unauthorized access from the doors, ceiling, raised floor, windows, ducts, and vents.

Step 2. Monitor and control closet entry with electronic logs.

Step 3. Use security cameras.

16.1.4

Check Your Understanding - Security Threats and Vulnerabilities

Check your understanding of security threats by choosing the correct answer to the following questions.

1. What kind of threat is described when a threat actor sends you a virus that can reformat your hard drive?
   - (•) data loss or manipulation
   - ( ) disruption of service
   - ( ) identify theft
   - ( ) information theft
2. What kind of threat is described when a threat actor makes illegal online purchases using stolen credit information?
   - ( ) data loss or manipulation
   - ( ) disruption of service
   - (•) identify theft
   - ( ) information theft
3. What kind of threat is described when a threat actor prevents legal users from accessing data services?
   - ( ) data loss or manipulation
   - (•) disruption of service
   - ( ) identify theft
   - ( ) information theft
4. What kind of threat is described when a threat actor steals scientific research data?
   - ( ) data loss or manipulation
   - ( ) disruption of service
   - ( ) identify theft
   - (•) information theft
5. What kind of threat is described when a threat actor overloads a network to deny other users network access?
   - ( ) data loss or manipulation
   - (•) disruption of service
   - ( ) identify theft
   - ( ) information theft
6. What kind of threat is described when a threat actor alters data records?
   - (•) data loss or manipulation
   - ( ) disruption of service
   - ( ) identify theft
   - ( ) information theft
7. What kind of threat is described when a threat actor is stealing the user database of a company?
   - ( ) data loss or manipulation
   - ( ) disruption of service
   - ( ) identify theft
   - (•) information theft
8. What kind of threat is described when a threat actor impersonates another person to obtain credit information about that person?
   - ( ) data loss or manipulation
   - ( ) disruption of service
   - (•) identify theft
   - ( ) information theft

Check | Show Me | Reset