Understanding Security Layers

Lesson 1

Objectives

Skill/Concept	Exam Objective	Objective Number
Introducing Core Security Principles	Understand core security principles	1.1
Understanding Physical Security as the First Line of Defense	Understand physical security	1.2
Performing Threat Modeling	Understand core security principles	1.1

Security

- What you are trying to protect
- Why does it needs to be protected
- What you're protecting it from

CIA

- Confidentiality
- Integrity
- Availability

Confidentiality

- Confidentiality is the characteristic of a resource ensuring access is restricted to only permitted users, applications, or computer systems.
- Confidentiality deals with keeping information, networks, and systems secure from unauthorized access.
- There are several technologies that support confidentiality in an enterprise security implementation.
  - Strong encryption
  - Strong authentication
  - Stringent access controls

Integrity

- Integrity is defined as the consistency, accuracy, and validity of data or information.
- One of the goals of a successful information security program is to ensure that data is protected against any unauthorized or accidental changes.

Availability

- Availability describes a resource being accessible to a user, application, or computer system when required.
  - In other words, availability means that when a user needs to get to information, he or she has the ability to do so.
- Typically, threats to availability come in two types: accidental and deliberate.

Risk Management

- Risk management is the process of identifying, assessing, and prioritizing threats and risks.
- A risk is generally defined as the probability that an event will occur.
- A threat, which is defined as an action or occurrence that could result in the breach, outage, or corruption of a system by exploiting known or unknown vulnerabilities.
- The goal of any risk management plan is to remove risks when possible and to minimize the consequences of risks that cannot be eliminated.
- Risk assessments are used to identify the risks that might impact your particular environment.

Dealing with Risks

- After you have prioritized your risks, you are ready to choose from among the four generally accepted responses to these risks. They include:
  - Avoidance
  - Acceptance
  - Mitigation
  - Transfer

Principle of Least Privilege

- The principle of least privilege is a security discipline that requires that a particular user, system, or application be given no more privilege than necessary to perform its function or job.

Separation of Duties

- ***Separation of duties*** is a principle that prevents any single person or entity from being able to have full access or complete all the functions of a critical or sensitive process.
- It is designed to prevent fraud, theft, and errors.

Attack Surface

- An attack surface consists of the set of methods and avenues an attacker can use to enter a system and potentially cause damage.
- The larger the attack surface of a particular environment, the greater the risk of a successful attack.

Performing an Attack Surface Analysis

- An attack surface analysis helps to identify the attack surface that an organization may be susceptible to.
- Because the network infrastructure and necessary services and applications are usually complicated, particularly for medium and large organizations, performing an ***attack surface analysis*** can also be just as complicated.

Social Engineering

- Social engineering is a method used to gain access to data, systems, or networks, primarily through misrepresentation.
- This technique typically relies on the trusting nature of the person being attacked.

Security and Cost

- Security costs money.
- You should also strive to make the security measures as seamless as possible to authorized users who are accessing the confidential information or resource.
- If security becomes a heavy burden, users will often look for methods to circumvent the measures you have established.
- Training goes a long way in protecting your confidential information and resources because it shows users what warning signs to watch for.

Physical Security

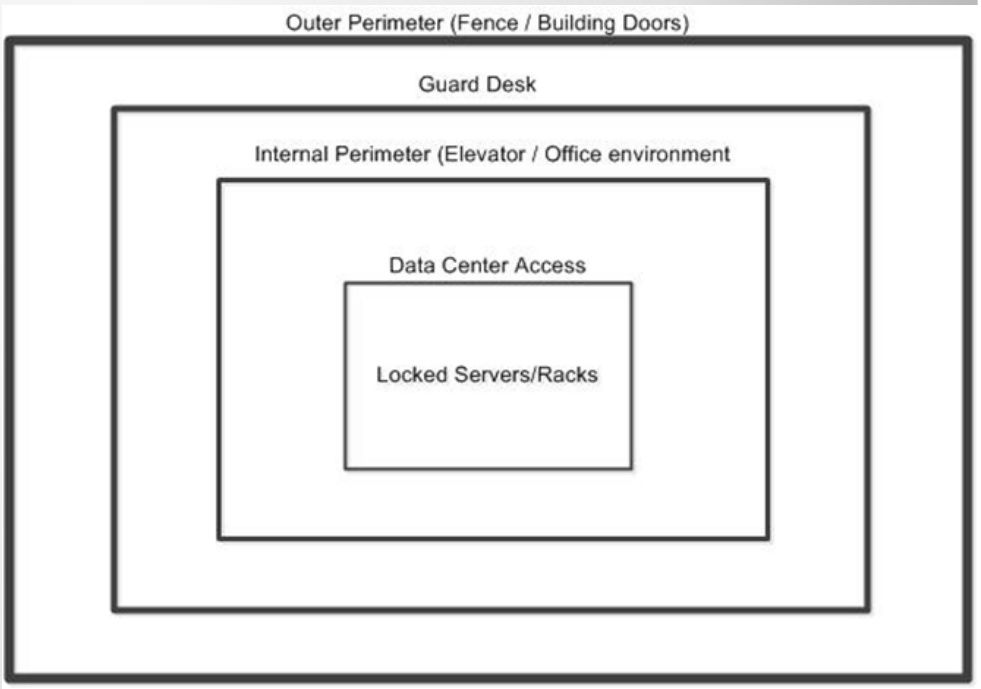
- Physical security is the first line of defense.
- There are a number of factors to consider when designing, implementing, or reviewing physical security measures taken to protect assets, systems, networks, and information.
- These include understanding site security and computer security; securing removable devices and drives; access control; mobile device security; disabling the Log On Locally capability; and identifying and removing keyloggers.

Access Control

- Access control is the process of restricting access to a resource to only permitted users, applications, or computer systems.

Defense in Depth

- Defense in depth means using multiple layers of security to defend your assets.
- That way, even if an attacker breaches one layer of your defense, you have additional layers to keep that person out of the critical areas of your environment.



Goals in Physical Security

- There are several other goals to keep in mind when designing a physical security plan:
  - **Authentication:** Site security must address the need to identify and authenticate the people who are permitted access to an area.
  - **Access control:** Once a person's identity has been proven and authenticated, site security must determine what areas that person has access to.
  - **Auditing:** Site security must also provide the ability to audit activities within the facility. This can be done by reviewing camera footage, badge reader logs, visitor registration logs, or other mechanisms.

Physical Premises

- For the purposes of this lesson, we will break the physical premises into three logical areas:
  - External perimeter
  - Internal perimeter
  - Secure areas

External Perimeter Security

- The external security perimeter is the first line of defense surrounding your office.
- Common security measures you may encounter with respect to an organization's external perimeter include the following:
  - Security cameras
  - Parking lot lights
  - Perimeter fence
  - Gate with guard
  - Gate with access badge reader
  - Guard patrols

Internal Security Perimeter

- The internal security perimeter starts with the building walls and exterior doors and includes any internal security measures, with the exception of secure areas within the building.
- Some of the features you may use to secure an internal perimeter include the following:
  - Locks (on exterior doors, internal doors, office doors, desks, filing cabinets, etc.)
  - Security cameras
  - Badge readers (on doors and elevators)
  - Guard desks and patrols
  - Smoke detectors
  - Turnstiles and mantraps

Secure Areas

- Areas that not only to restrict external attackers, but also to limit internal employee access.
- Secure area security technologies include the following:
  - Badge readers and Keypads
  - Biometric technologies (e.g., fingerprint scanners, retinal scanners, voice recognition systems, etc.)
  - Security doors
  - X-ray scanners and Metal detectors
  - Cameras
  - Intrusion detection systems (light beam, infrared, microwave, and/or ultrasonic)

Computer Security

- Computer security consists of the processes, procedures, policies, and technologies used to protect computer systems.
  - Servers
  - Desktop Computers
  - Mobile Computers

Mobile Devices

- Mobile devices are one of the largest challenges facing many security professionals today.
- Mobile devices such as laptops, PDAs, and smartphones are used to process information, send and receive mail, store enormous amounts of data, surf the internet, and interact remotely with internal networks and systems.
  - Docking stations
  - Laptop security cables
  - Laptop safes
  - Theft recovery software
  - Laptop alarms:

Removable Devices (1 of 3)

- A removable device or drive is a storage device that is designed to be taken out of a computer without turning the computer off.
- Include memory cards, flash drives, floppy disks, CDs, and DVDs.
- Removable devices typically connect to a computer through a drive, through external communications ports like USB or Firewire, or, in the case of memory cards, through built-in or USB-based readers.

Removable Devices (2 of 3)

Removable Devices (3 of 3)

- There are three basic types of security issues associated with removable storage:
  - Loss
  - Theft
  - Espionage

Keylogger

- A keylogger is a physical or logical device used to capture keystrokes.
- An attacker will either place a device between the keyboard and the computer or install a software program to record each keystroke taken, and then he or she can use software to replay the data and capture critical information like user IDs and passwords, credit card numbers, Social Security numbers, or even confidential emails or other data.

Threat Modeling

- ***Threat modeling*** is a procedure for optimizing network security by identifying vulnerabilities, identifying their risks, and defining countermeasures to prevent or mitigate the effects of the threats to the system.
- It addresses the top threats that have the greatest potential impact to an organization.

Summary (1 of 5)

- Before you can start securing your environment, you need to have a fundamental understanding of the standard concepts of security.
- CIA, short for confidentiality, integrity, and availability, represents the core goals of an information security program.
- Confidentiality deals with keeping information, networks, and systems secure from unauthorized access.
- One of the goals of a successful information security program is to ensure integrity, or that information is protected against any unauthorized or accidental changes.

Summary (2 of 5)

- Availability is defined as the characteristic of a resource being accessible to a user, application, or computer system when required.
- Threat and risk management is the process of identifying, assessing, and prioritizing threats and risks.
- A risk is generally defined as the probability that an event will occur.
- Once you have prioritized your risks, there are four generally accepted responses to these risks: avoidance, acceptance, mitigation, and transfer.

Summary (3 of 5)

- The principle of least privilege is a security discipline that requires that a user, system, or application be given no more privilege than necessary to perform its function or job.
- An attack surface consists of the set of methods and avenues an attacker can use to enter a system and potentially cause damage. The larger the attack surface of an environment, the greater the risk of a successful attack.
- The key to thwarting a social engineering attack is employee awareness. If your employees know what to look out for, an attacker will find little success.

Summary (4 of 5)

- Physical security uses a defense in depth or layered security approach that controls who can physically access an organization's resources.
- Physical premises can be divided into three logical areas: the external perimeter, the internal perimeter, and secure areas.
- Computer security consists of the processes, procedures, policies, and technologies used to protect computer systems.

Summary (5 of 5)

- Mobile devices and mobile storage devices are among the biggest challenges facing many security professionals today because of their size and portability.
- A keylogger is a physical or logical device used to capture keystrokes.
- Threat modeling is a procedure for optimizing network security by identifying vulnerabilities, identifying their risks, and defining countermeasures to prevent or mitigate the effects of the threats to the system.