CYBRARY

CASP+

Instructor Name : **Jim Hollis**

Study Guide By: **Ridwan Sachroni, Teaching Assistant**

Prerequisites : A minimum of ten years of experience in IT administration, including at least five years of hands-on technical security experience.
The following recommended prerequisites: CompTIA Network+, Security+, CySA+, Pentest+ or equivalent experience.

Course Description : CompTIA Advanced Security Practitioner Plus or CASP+ is advanced certification is aimed at IT security professionals who have a minimum of ten years of experience in IT administration, including at least five years of hands-on technical security experience. This course provides the knowledge needed to implement security solutions within an enterprise policy framework, using a vendor-neutral format. This includes risk and vulnerability management programs, organizational policies and training, applied cryptography, system security, network security, identity management, and incident response.

Course Goals: By the end of the course, students should be able to:

a. Conceptualize, engineer, integrate and implement secure solutions across complex environments to support a resilient enterprise
b. Apply critical thinking and judgment across a broad spectrum of security disciplines to propose, implement and advocate sustainable security solutions that map to organizational strategies, balance security requirements with business/regulatory requirements, analyze risk impact and respond to security incidents

Lab Used: these labs can be use by students to test their knowledge and implement security solutions for enterprise environments:

- **CASP+ practice test labs from Kaplan**
  https://app.cybrary.it/browse/transcender_tests/compcert-comptia-advanced-security-practitioner002
- **CASP+ practice test form Practice Labs**
  https://app.cybrary.it/browse/practice_labs/exam/casp-exam

- **CASP+ labs for version 003 from Practice Labs**
  https://app.cybrary.it/browse/practice_labs/comptia-casp
- **CASP labs version 002 from Practice Labs**
  https://app.cybrary.it/browse/practice_labs/comptia-advanced-security-practitioner-casp

Contents

Module 1 Risk Management

Risk management is identification, assessment, and prioritization of risks followed by coordinated and economic application of resources to minimize, monitor and control properly an impact of unfortunate events or to maximize the realization of opportunities. When you thinks about risk management, planning is everything. Risk management is forward looking, anticipating and is not reactive but proactive.

1.1 Understanding Security Concepts

We can know the state of information security in 2019 by reading reports from the internet. Here are some link to recent reports:

1. https://enterprise.verizon.com/resources/reports/dbir/
2. https://www.varonis.com/blog/cybersecurity-statistics/

Before we learned more about security concepts, we need to understand this first:

1. What we are trying to protect?
2. Why does it needs to be protected?
3. What you're protecting it from?

CIA Triad

CIA triad is important security concepts because all security controls and mechanism to safeguard are implementing one or more of these protection, confidentiality, integrity and availability. On another side, attacker try to compromise one or more of this CIA triad.

Confidentiality

- Assurance that information can be read, interpreted, or accessed in any way only by persons and processes explicitly authorized to do so.
- Protecting confidentiality involves implementing procedures and measures to prevent malicious and accidental disclosure of information to unauthorized users.
    - Access Control Lists (ACLs)
    - Locked file cabinet or safe
    - Concealing content

- Encryption
- Print or storage restrictions
- Shredding materials

Integrity

- Assurance that information remains intact, accurate, and authentic.
- Protecting the integrity involves preventing and detecting unauthorized creation, modification, or destruction of information.
    - Input validation
    - Parity bit checking
    - Cyclic redundancy checking
    - Hashing

Availability

- Assurance that authorize users can access and work with information assets, resources, and systems when needed with sufficient response and performance.
- Protecting availability involves measure to sustain accessibility to information in spite of possible source of interference, including system failures and deliberate attempts to obstruct availability.
    - Redundancy
    - Fail over
    - Fault/Disaster tolerance

Classifying Asset

- An asset is any data, device, or other component of the environment that supports information-related activities. Assets generally include hardware (e.g. servers and switches), software (e.g. mission critical applications and support systems) and confidential information.
- Assets can be tangible, that is, perceptible by touch.
    - An asset can be hardware, product or infrastructure that is of value to an organization, and hence, needs protection.
- Assets can be intangible, that is, not have physical presence.
    - An example of an intangible asset could be a corporate image or an intellectual property, such as patents.

Risk Management Overview

- Concepts

Threats

- Any circumstance or event with the potential to harm an information resource by exploiting a vulnerability.
- Categorized as:
    - Natural
        - Flood, fire, cyclones, earthquake, etc.
    - Unintentional
        - Fire, water, loss of utility service, equipment failure, etc.
    - Intentional – physical threats
        - Bombs, fire, water, theft, etc.
    - Intentional – nonphysical threats
        - Fraud, espionage, hacking, identity theft, social engineering, etc.

Risks

- Risk is inherent part of business.
    - All risks cannot be eliminated.
    - Every organization has a level of risk that it will accept.

    - Risk appetite
- To determine the reasonable level of acceptable risk
    - Determine an optimal point where cost of loss intersects with cost of mitigation

Types of risks

- **Technical risk:** includes problem with languages, project size, and project functionality.
- **Management risk:** it includes lack of management experience and lack of planning.
- **Financial risk:** includes cash flow, capital and budget issues.
- **Project risks:** affect project schedule or resources.
- **Product risks:** affect product quality or performance of software.
- **Personnel risk:** include staffing lags, experience and training problems.

Vulnerability

- Vulnerability is a cyber-security term that refers to a flaw in a system that can leave it open to attack.
- A Vulnerability may also refer to any type of weakness in computer system itself, in a set of procedures, or in anything that may be exploited in order for a threat to destroy, damage, or compromise an assets.
    - Unpatched operating systems, antivirus not installed, not implement separation of duty, not have backup power source, etc.

Identification of risks

- The first step is to generate a comprehensive list of threat sources, risks, and events that may impact the achievement of each of the objectives identified in the definition of scope and framework.
- Risk can be related to or characterized by:
    - Origin – activity, event, or incident
    - Consequences – specific reason for occurrence
    - Protective mechanisms and controls
    - Time/place of occurrence

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.

Key standards and guidelines

- FIPS Publication 199 (Security Categorization)
- FIPS Publication 200 (Minimum Security Controls)
- NIST Special Publication 800-18 (Security Planning)
- NIST Special Publication 800-30 (Risk Assessment)
- NIST Special Publication 800-37 (System Risk Management Framework)
- NIST Special Publication 800-39 (Enterprise-Wide Risk Management)
- NIST Special Publication 800-53 (Recommended Security Controls)
- NIST Special Publication 800-53A (Security Control Assessment)
- NIST Special Publication 800-59 (National Security Systems)
- NIST Special Publication 800-60 (Security Category Mapping)

Controls

- Are designed as part of risk management framework, which incorporates policies, standards, procedures, practices and organizational structures.
- Provide reasonable assurance that business objectives are achieved and undesired events are:
    - Prevented
    - Detected
    - Addressed

Countermeasures

- Any process that serves to counter specific threats and can be considered targeted control
    - Reducing internal threats
    - Reengineering and modifications to architecture
    - Awareness programs for employees

Residual risk

- Residual risk is the risk that remains after you apply controls. It's not feasible to eliminate all risks. Instead, you take steps to reduce the risk to an acceptable level. The risk that's left is residual risk.
    - Risk = Threat x Vulnerability
    - Total Risk = Threat x Vulnerability x Asset Value
- You can calculate residual risk with the following formula:
    - Residual Risk = Total Risk - Controls

- Senior management is responsible for any losses due to residual risk. They decided whether a risk should be avoided, transferred, mitigated or accepted. They also decided what controls to implement. Any resulting loss due to their decisions falls on their shoulders.

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

- **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 perimeter security**
    - 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 no 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, etc.)
        - Security doors
        - X-ray scanners and metal detectors
        - Cameras
        - Intrusion detection systems (light beam, infrared, microwave, and/or ultrasonic)

Events and incidents

- Event – it is an action that occurs as a result of the user or another source, such as a mouse being clicked, or a key being pressed.
- Incident – ITIL 2011 defines it as an unplanned interruption to an IT service or reduction in the quality of an IT service.

1.2 Understanding Threats and Vulnerabilities

After completed this lessons, students will gain knowledge about:

- How to identify threats and vulnerabilities
- Pairing of threats and vulnerabilities
- Sources of vulnerability

Threats

In the lesson before we have learned about threat. A threat, in computer security, refers to anything that has the potential to cause serious harm to a computer system. A threat is something that may or may not happen, but has the potential to cause serious damage. Threats can lead to attacks on computer systems, networks and more.

Unintentional Threats	Intentional Threats
Environmental: ● Fire, wind ● Lighting, flooding	Individual or organization: ● Hackers ● Criminals

• Accident • Equipment failures	• Disgruntled employees
Human: • Keystroke errors • Procedural errors • Programming bugs	

Types of threats

- Brute-force password attacks
- Dictionary password attacks
- IP address spoofing
- Hijacking
- Replay attacks
- Man-in-the-middle attacks
- Masquerading
- Social engineering
- Phishing
- Phreaking
- Pharming

Vulnerabilities

In the lesson before we have learned definition about vulnerabilities. Vulnerability is anything that leaves information security exposed to a threat. Next, we will see some examples of vulnerabilities:

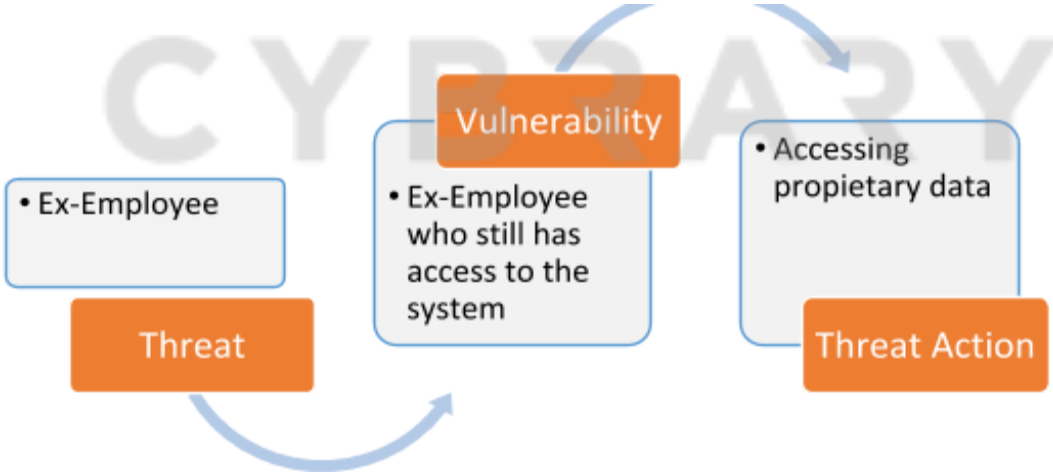
- Defective software
- Equipment configured improperly
- Inadequate enforcement of compliance
- Substandard network design
- Inadequate management
- Insufficient staff/personnel
- Lack of security functionality
- Weak passwords
- Untested technology

- Insufficient redundancy

Risk identification and management techniques

Risk Identification	Management Techniques
Threats	• Understand • Control • Plan
Vulnerabilities	• Audit • History • Certification • Accreditation • Systems logs • Trouble reports

Pairing of threats and vulnerabilities



Below are some examples of threat vulnerability pairs and potential losses

Threat	Vulnerability	Harmful event or lose
Fire	Lack of fire detection and suppression equipment	Can be total loss of business
Hurricane, earthquake, tornado	Location	Can be total loss of business
Malware	Lack of antivirus software Outdated definitions	Infection (impact of loss determined by payload of malware)
Equipment failure	Data not backed up	Loss of data availability (impact of loss determined by value of data)
Stolen data	Access control not properly implemented	Loss of confidentiality of data
Denial of service (DoS) or distributed denial of service (DDos) attack	Public-facing servers not protected with firewalls and intrusion detection systems	Loss of service availability
Users	Lack of access controls	Loss of confidentiality
Social engineer	Lack of security awareness	Loss depends on the goals and success of attacker

Vulnerability	Threat-Source	Threat Action
Terminated employee ID's are not removed from the system	Terminated employees	Dialing into company's network and accessing proprietary info
Water sprinklers used for fire suppression and no protective coverings in place	Fire; negligent persons	Water sprinklers being turned on
Vulnerability	Threat-Source	Threat Action
Vendor has identified security flaws in system and patches have not been applied	Unauthorized users (e.g. terminated employees, hackers)	Obtaining unauthorized access to sensitive files based on known vulnerabilities

Sources of vulnerability

- Procedures
- Design
- Internal controls
- Implementation

Importance of risk management

- Identifies threat and vulnerabilities
- Reduces adverse impact
- Improves organization survivability
- Enhances cost-benefit awareness
- Shows the need for risk reduction