Tutorial 2

Question 1

What are the three components of the CIA triad in information security?

Answer: Confidentiality , Integrity and Availability

Question 2

Define "Operating System Hardening" and list two examples of hardening measures.

Answer: System hardening is by closing open vulnerabilities that might exist in our system such as open ports or open smb server. So some hardening measures include closing open ports, disabling unneeded services.

Question 3

a) What is the principle of Least Privilege in operating system security?  
b) Why is this principle important in reducing internal threats?  
c) Provide an example scenario where applying least privilege could prevent a security breach.

Answer: This is so that we can control who have access to the most core functions of the database and server.

Question 4

a) Explain the Economy of Mechanism security principle.  
b) How does this principle help in debugging and securing systems?  
c) What practical steps can system administrators take to apply this principle?

1. Answer: Use minimalistic software with only necessary features enabled.
2. Avoid overcomplicating configurations; use standard tools instead of custom-built ones unless absolutely necessary.

Question 5

a) What does the Fail-Safe Defaults principle mean in system security?  
b) How is this principle related to system access policies?  
c) Give an example of how a fail-safe default setting could enhance system security.

Answer: a) Fail-Safe Defaults: Systems should be designed to default to a secure state in case of failure or unexpected conditions.

b) In terms of access policies, if there's a failure in authentication or authorization, the system should deny access by default rather than allowing unrestricted access.

c) Example:  
If a firewall fails, it should default to blocking all traffic until it can be restored, rather than allowing all traffic through unchecked.

Question 6

Why is a password policy important?

Answer: A password policy is important because it enforces strong, unique passwords across the organization, preventing the use of weak or easily guessable passwords. It helps protect against brute-force attacks, credential stuffing, and unauthorized access due to reused or generic credentials.

Question 7

What is the goal of "Continuous Validation" in system configuration?

Answer: The goal of Continuous Validation is to ensure that systems remain compliant with defined security policies and configurations at all times by constantly monitoring and verifying system settings, detecting deviations, and remediating issues automatically or alerting administrators.

Question 8

List three measures to ensure system availability.

1. Answer: Implement regular backups and offsite storage.
2. Use redundant systems and hardware (e.g., RAID arrays, load balancers).
3. Employ failover mechanisms and disaster recovery plans.

Question 9

1. What is the principle of Complete Mediation in the context of system security?

b) Why is it important not to rely on previously granted permissions or trust?  
c) Describe a scenario where the absence of complete mediation could lead to a security vulnerability.

Answer: a) Complete Mediation: Every access request to a resource must be checked for authorization every time it is made, rather than assuming previous checks still apply.

b) Relying on past permissions can create vulnerabilities if the user’s role has changed or if a session has been hijacked. Continuous verification ensures ongoing security.

c) Scenario:  
In a web application, if a user logs in and gains access without re-checking permissions for each action, a malicious script could perform unauthorized operations under the user’s session. Complete mediation prevents this by validating each request independently.

Question 10

Identify three components of a security architecture.

Answer: Three components of a security architecture include:

1. Access Control Mechanisms (e.g., authentication, authorization)
2. Network Security Devices (e.g., firewalls, intrusion detection/prevention systems)
3. Security Policies and Procedures (e.g., incident response plans, encryption standards)