VIT®
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

School of Computer Science and Engineering
Fall Semester 2024-25
CAT I-Answer Key

SLOT:F1+TF1

Programme Name & Branch: B.Tech (CSE)

Course Name & Code: Information Security (BCSE317L)

1. What potential threats could a voting system face during an election? Who might target such a system, and what are their possible motivations? Identify five vulnerabilities within the system that could be exploited to cause disruption or manipulation.

Potential Threats to a Voting System

- Cyber Attacks
- Denial of Service (DoS) Attacks
- Insider Threats
- Physical Attacks
- Disinformation Campaigns

Potential Actors and Their Motivations

- Nation-State Actors
- Political Opponents or Extremist Groups
- Hacktivists
- Cybercriminals
- Insiders

Five Vulnerabilities Within the Voting System

- Insecure Voting Machines
- Weak Voter Registration Database Security
- Lack of Network Security
- Poorly Managed Software and Hardware Updates
- Insufficient Physical Security Measures

2. A financial institution's IT department begins receiving reports of unusual activity from employees. There are indications of unauthorized financial transactions and changes to sensitive documents. The IT team discovers that a new software application was recently installed in one of the client machines in the network. Identify the malware and list out the steps the IT team need to take to determine this. Also, mention the ways to recover from the attack.

The IT team needs to identify if the new application is **a Trojan horse** and take appropriate actions to mitigate the threat and secure the network.

Steps to Analyze and Handle the Trojan Horse:

- Collect and Review Reports
- Incident Reports
- Application Details
- Preliminary Analysis
- Antivirus and Anti-Malware Scan
- Behavior Analysis

Investigate Trojan Characteristics:

- Remote Access
- Payload Actions
- Check for Persistence Mechanisms
- Scheduled Tasks

Network Monitoring:

- Traffic Analysis
- Contain and Eradicate
- Isolate Infected Systems
- Remove the Trojan
- Restore and Secure
- Data Restoration
- Patch Vulnerabilities
- Communicate and Educate
- Notify Affected Parties
- Training and Awareness

3. GlobalTech Corp is a multinational company with various departments, each with its own network resources, including file servers, databases, and application services. The company has recently upgraded its internal IT infrastructure to a more modern setup with the following requirements:

a) Secure authentication for users accessing company resources across different departments and locations.
b) Seamless Single Sign-On experience for users, allowing them to access multiple services without needing to log in multiple times.
c) Integration with existing Active Directory (AD) infrastructure, which is already in place for managing user accounts and permissions.

With a neat diagram, explain how would Kerberos can be implemented in this scenario to meet GlobalTech Corp's requirements?

Implementation of Kerberos:

1. Integration with Active Directory (AD):

Kerberos is well-integrated with Active Directory, which can serve as the Kerberos Key Distribution Center (KDC) in this scenario. AD will handle the authentication requests and issue Kerberos tickets.

2. Kerberos Components:

Key Distribution Center (KDC): In this case, the KDC will be part of the Active Directory Domain Controllers. It consists of the Authentication Server (AS) and the Ticket Granting Server (TGS).

Tickets: Users authenticate to the AS to receive a Ticket Granting Ticket (TGT). This TGT is then used to request Service Tickets from the TGS to access specific services within the network.

3. Single Sign-On (SSO):

Once users authenticate with Kerberos (by logging into their AD accounts), they receive a TGT. This ticket is used to access various network services without needing to re-enter credentials. This seamless access improves user experience and security.

4. Accessing Resources:

When a user needs to access a network resource (e.g., a file server or database), the application server will request a service ticket from the TGS. The service ticket is then used to authenticate the user to the resource server.

4. Describe each of the following three kinds of access control mechanisms in terms of (a) ease of determining authorized access during execution, (b) ease of adding access for a new subject, (c) ease of deleting access by a subject, and (d) ease of creating a new object to which all subjects by default have access.

i) per-subject access control list (that is, one list for each subject tells all the objects to which that subject has access)

ii) per-object access control list (that is, one list for each object tells all the subjects who have access to that object)

iii) access control matrix

i) Per-Subject Access Control List (ACL)

- **Ease of Determining Authorized Access During Execution**:
  - **Moderate**: The system needs to check the subject's list to determine access, which can be straightforward but may require searching through potentially large lists.
- **Ease of Adding Access for a New Subject**:
  - **Easy**: Simply add a new list for the new subject and specify the objects they can access.
- **Ease of Deleting Access by a Subject**:
  - **Easy**: Remove the subject's list or specific entries within it.
- **Ease of Creating a New Object to Which All Subjects by Default Have Access**:
  - **Difficult**: Each subject's list would need to be updated individually to include the new object.

ii) Per-Object Access Control List (ACL)

- **Ease of Determining Authorized Access During Execution:**
    - **Easy:** The system checks the object's list to see if the subject is authorized, which is typically efficient.
- **Ease of Adding Access for a New Subject:**
    - **Moderate:** Each object's list needs to be updated to include the new subject, which can be cumbersome if there are many objects.
- **Ease of Deleting Access by a Subject:**
    - **Moderate:** Each object's list must be checked and updated to remove the subject's access.
- **Ease of Creating a New Object to Which All Subjects by Default Have Access:**
    - **Easy:** The new object's list can be initialized to include all subjects.

iii) Access Control Matrix

- **Ease of Determining Authorized Access During Execution**:
    - **Easy**: The matrix provides a direct lookup to check if a subject has access to an object.
- **Ease of Adding Access for a New Subject**:
    - **Moderate**: A new row must be added to the matrix, and each cell corresponding to objects must be initialized.
- **Ease of Deleting Access by a Subject**:
    - **Moderate**: The subject's row must be removed or updated, which can be straightforward but may involve many entries.
- **Ease of Creating a New Object to Which All Subjects by Default Have Access**:

Moderate: A new column must be added to the matrix, and each cell corresponding to subjects must be initialized.

5. Memory protection implements both separation and sharing. Elaborate any four mechanisms using which Operating Systems enforce memory protection.

Answer any 4 Techniques:

- Virtualization
- Sandbox
- Honeypots
- Separation and Sharing
- Hardware Protection of Memory
- Base/Bounds Registers
- Tagged Architecture
- Segmentation
- paging