CSC 321 REVISION

a) Define the following terms [5 marks]

i) System

A system refers to a collection of interconnected elements or components that work together to achieve a common goal or purpose. It can be a physical or conceptual entity, such as a computer system, a network of computers, or an organizational system.

ii) Security

Security is the state or condition of being protected against potential harm, loss, or unauthorized access. It involves implementing measures and safeguards to ensure the confidentiality, integrity, and availability of assets or resources, such as information, systems, networks, or physical infrastructure.

System security

System security focuses on protecting the integrity, availability, and confidentiality of a computer system or network. It involves implementing measures, policies, and controls to prevent unauthorized access, misuse, disruption, or destruction of system resources.

iv) Information security

Information security is concerned with protecting the confidentiality, integrity, and availability of information. It involves safeguarding information from unauthorized access, modification, disclosure, disruption, or destruction. Information security aims to ensure that information is only accessible to authorized individuals or entities and is accurate and reliable.

v) Information assurance

Information assurance encompasses the processes and practices used to protect and manage information assets. It includes measures to ensure the confidentiality, integrity, availability, authenticity, and non-repudiation of information. Information assurance focuses on establishing trust in the information and the systems that store, process, and transmit it.

b) Identify and discuss the fundamental goals of system security [8 marks]

i) Confidentiality: Confidentiality ensures that information is accessible only to authorized individuals or entities. It involves protecting sensitive or classified information from unauthorized disclosure or access. Confidentiality measures, such as encryption, access controls, and secure communication channels, help prevent unauthorized users from obtaining sensitive information.

ii) Integrity: Integrity ensures that information remains accurate, complete, and unaltered during storage, processing, and transmission. It involves protecting information from unauthorized modification, deletion, or corruption. Integrity mechanisms, such as data validation, checksums,

and digital signatures, help verify the integrity of information and detect any unauthorized changes.

iii) Availability: Availability ensures that information and system resources are accessible and usable when needed. It involves preventing or minimizing disruptions that could lead to system downtime or unavailability of resources. Availability measures, such as redundancy, backup systems, and disaster recovery plans, help ensure continuous access to information and services.

iv) Authenticity: Authenticity ensures that the identities of users, systems, or entities involved in a communication or transaction can be verified. It involves verifying the genuineness and credibility of information, the source of information, or the identity of individuals or systems. Authentication mechanisms, such as passwords, digital certificates, and biometric authentication, help establish the authenticity of entities in a system.

c) A computer can be either or both the subject of an attack and/or the object of an attack, explain the statement [5 marks]

When we say that a computer can be either the subject or object of an attack, it means that a computer can play different roles in the context of a security incident.

1. Subject of an attack: In this case, the computer is the entity or actor that initiates an attack on another system or network. It can be a compromised computer that is used by an attacker to launch various types of attacks, such as malware propagation, network scanning, or launching denial-of-service attacks. The subject of an attack is typically under the control of an attacker and is used as a tool or weapon to target other systems.

2. Object of an attack: In this case, the computer is the target of an attack. It can be a victim system that is being targeted by an attacker or a malicious entity. The purpose of attacking the computer can be to gain unauthorized access, steal sensitive information, disrupt services, or compromise the integrity of the system. The object of an attack is typically the system that needs to be protected from potential threats and vulnerabilities.

d) State and explain the components of information security [6 marks]

i) Policies: Information security policies are high-level guidelines, rules, or principles that define the organization's approach to information security. They outline the expectations, responsibilities, and procedures for protecting information assets and provide a framework for implementing security controls.

ii) Procedures: Procedures are detailed step-by-step instructions that describe how to carry out specific information security practices or activities. They provide specific guidance on implementing security controls, incident response, access management, data backup, and other security-related processes.

iii) Technical Controls: Technical controls are mechanisms implemented within information systems to protect the confidentiality, integrity, and availability of information. Examples include firewalls, intrusion detection systems, encryption, access controls, antivirus software, and secure network protocols. Technical controls provide automated or technical means to enforce security policies and protect information.

iv) Physical Controls: Physical controls involve measures taken to protect the physical environment where information systems are housed. This includes physical access controls, such as locks, biometric authentication systems, video surveillance, and secure facilities. Physical controls aim to prevent unauthorized physical access, theft, damage, or disruption of information systems and infrastructure.

v) Human Controls: Human controls involve security measures related to the behavior, actions, and awareness of individuals within an organization. This includes security awareness training, user access management, background checks, security policies enforcement, and incident response procedures. Human controls address the human factor in information security, emphasizing the role of employees in safeguarding information

e) Explain the three causes of information security [6 marks]

i) Human Factors: Human factors are one of the primary causes of information security incidents. They include human errors, negligence, lack of awareness, and malicious actions. Examples of human factors causing security breaches include weak passwords, improper handling of sensitive information, falling victim to phishing attacks, and unauthorized disclosure of information.

ii) Technical Vulnerabilities: Technical vulnerabilities refer to weaknesses or flaws in hardware, software, or network systems that can be exploited by attackers. These vulnerabilities can arise from design flaws, programming errors, misconfigurations, or outdated software. Attackers can exploit technical vulnerabilities to gain unauthorized access, inject malware, or disrupt systems, leading to information security breaches.

iii) External Threats: External threats come from external entities or attackers who target an organization's information systems or assets. These threats can include hackers, cybercriminals, nation-state actors, or organized crime groups. External threats exploit vulnerabilities in systems or use social engineering techniques to gain unauthorized access, steal information, or disrupt services.

QUESTION TWO

a) Identify five threat categories and in each category, give a relevant example [10 marks]

i) Malware:

Example: Computer viruses - Programs designed to replicate and spread to other computers, often causing damage to files or disrupting system operations.

ii) Phishing:

Example: Email phishing - Attackers send deceptive emails pretending to be from legitimate sources, tricking recipients into revealing sensitive information or clicking on malicious links.

iii) Denial-of-Service (DoS) attacks:

Example: Distributed Denial-of-Service (DDoS) - Attackers flood a target system or network with a massive volume of traffic from multiple sources, causing it to become overwhelmed and unavailable to legitimate users.

iv) Insider Threats:

Example: Employee sabotage - Disgruntled or malicious insiders intentionally misuse their privileges to steal sensitive data, manipulate systems, or disrupt operations.

v) Social Engineering:

Example: Pretexting - Attackers deceive individuals by inventing a scenario or pretext to trick them into disclosing confidential information, such as passwords or account details.

b) Differentiate between a hacker and a cracker [4 marks]

Hacker: A hacker is a person who enjoys exploring the limits of what is possible, typically in computer programming or networking. They may engage in ethical hacking, using their skills to improve security by identifying vulnerabilities and weaknesses in systems. Hackers may work in cybersecurity professions or engage in white-hat hacking activities to enhance security.

Cracker: A cracker, on the other hand, is someone who engages in malicious activities, such as unauthorized access to computer systems, data theft, or system manipulation. Crackers exploit vulnerabilities for personal gain, causing harm to individuals, organizations, or systems. They are often associated with black-hat hacking activities and are motivated by financial gain, ideology, or personal gratification.

c) State and explain any three types of attack to information systems [6 marks]

i) Malware attacks: Malicious software, such as viruses, worms, trojans, and ransomware, infects systems to steal data, damage files, disrupt operations, or extort money from victims. Malware can be spread through infected files, email attachments, malicious websites, or compromised software.

ii) Phishing attacks: Phishing attacks involve sending deceptive emails, messages, or websites that impersonate legitimate entities to trick users into revealing sensitive information, such as passwords, credit card numbers, or personal details. Phishing attacks often exploit human vulnerabilities, relying on social engineering tactics to manipulate victims into taking actions that benefit the attackers.

iii) Man-in-the-Middle (MitM) attacks: In MitM attacks, attackers intercept and eavesdrop on communication between two parties, such as between a user and a website or between two networked devices. By positioning themselves between the communication flow, attackers can intercept and manipulate data, steal sensitive information, or inject malicious code to compromise the integrity and confidentiality of the communication.

QUESTION THREE [20 MARKS]

a) What is authentication

Authentication is the process of verifying the identity of an entity, such as a user, device, or application, to ensure that they are who they claim to be before granting access to resources or performing certain actions. It is a fundamental security mechanism used to prevent unauthorized access and protect sensitive information from being compromised.

b) Describe three authentication methods [9 marks]

i) Password-based authentication: This method involves users providing a unique combination of characters, known as a password, to authenticate their identity. The system compares the entered password with a stored version to determine if they match. Password-based authentication is widely used due to its simplicity and familiarity but is susceptible to vulnerabilities such as weak passwords, password reuse, and password guessing attacks.

ii) Biometric authentication: Biometric authentication uses unique biological characteristics or behavioral traits of individuals to verify their identity. Common biometric identifiers include fingerprints, iris patterns, facial features, voiceprints, and hand geometry. Biometric authentication provides a high level of security as biometric traits are difficult to forge or replicate, but it may raise privacy concerns and requires specialized hardware for capturing and processing biometric data.

iii) Multi-factor authentication (MFA): Multi-factor authentication requires users to provide two or more different authentication factors to verify their identity. These factors typically fall into three categories: something you know (e.g., password), something you have (e.g., smartphone or security token), and something you are (e.g., biometric trait). By combining multiple factors, MFA enhances security by adding layers of protection against unauthorized access, even if one factor is compromised.

c) Discuss three forms of access control [9 marks]

i) Mandatory Access Control (MAC): In mandatory access control, access rights are assigned and enforced by the system administrator based on security labels and security classifications. Users have limited control over their access permissions, and access decisions are typically determined by predefined security policies and rules. MAC is commonly used in environments

with strict security requirements, such as government and military systems, to ensure data confidentiality and integrity.

ii) Discretionary Access Control (DAC): Discretionary access control allows owners of resources to control access permissions and determine who can access their resources and what actions they can perform. Access decisions are based on user identities and associated access control lists (ACLs) or permissions set by resource owners. DAC provides flexibility and user autonomy but may lead to security risks if permissions are not properly managed or if users misuse their privileges.

iii) Role-Based Access Control (RBAC): Role-based access control assigns access permissions to users based on their roles or job functions within an organization. Users are grouped into roles, and access rights are predefined for each role based on the tasks and responsibilities associated with that role. RBAC simplifies access management by centralizing permissions at the role level and streamlining the assignment of access rights. It enhances security by minimizing the risk of overprivileged users and simplifying access control administration.

QUESTION FOUR [20 MARKS]

a) State and explain five forms of physical security [10 marks]

i) Perimeter security: Perimeter security involves securing the boundaries of a physical location to prevent unauthorized access. This may include measures such as fences, walls, gates, and barriers to restrict entry points and deter intruders from gaining access to the premises.

ii) Access control systems: Access control systems regulate and monitor entry to buildings, rooms, or restricted areas by verifying the identity of individuals and granting or denying access based on their authorization level. Examples include keycard readers, biometric scanners, PIN pads, and security guards stationed at entry points.

iii) Surveillance systems: Surveillance systems use cameras, motion sensors, and other monitoring devices to observe and record activities in and around a facility. Video surveillance allows security personnel to monitor for suspicious behavior, deter potential intruders, and provide evidence in case of security incidents.

iv) Locks and keys: Locks and keys are fundamental physical security measures used to secure doors, cabinets, safes, and other storage units. Different types of locks, such as deadbolts, padlocks, and electronic locks, provide varying levels of security based on their design and resistance to tampering or picking.

v) Security lighting: Security lighting illuminates' outdoor areas, entrances, and dark corners to enhance visibility and deter intruders during nighttime hours. Bright lights,

motion-activated lighting, and strategically placed fixtures help to improve surveillance and increase the perceived risk for potential trespassers.

b) Discus how an intrusion detections system and different from a firewall [10 marks]

Intrusion Detection System (IDS):

- An IDS is a security tool that monitors network or system activities for signs of malicious behavior or policy violations.

- It operates by analyzing network traffic, system logs, and other data sources to detect suspicious patterns, anomalies, or known attack signatures.

- IDS can be classified into two types: network-based IDS (NIDS) that monitors network traffic and host-based IDS (HIDS) that monitors activities on individual systems.

- When suspicious activity is detected, an IDS generates alerts or triggers response actions, such as logging the event, notifying security personnel, or initiating automated countermeasures.

Firewall:

- A firewall is a network security device or software that acts as a barrier between a trusted internal network and untrusted external networks, such as the internet.

- It examines incoming and outgoing network traffic based on predefined rules or policies and determines whether to allow, block, or filter traffic based on specified criteria, such as IP addresses, ports, protocols, or application types.

- Firewalls can be implemented as hardware appliances, software applications, or cloud-based services and are typically deployed at network entry points, such as perimeter gateways or between network segments.

- Firewalls help to enforce access control policies, prevent unauthorized access, and protect against common network threats, such as unauthorized access attempts, malware infections, and denial-of-service attacks.

QUESTION FIVE [20 MARKS]

Hillary Clinton was accused of keeping classified information on her private email server she used during her tenure as a secretary of state.

a.) As a security professional, briefly describe the steps you will take to prevent occurrence of such information security lapses. [6 marks]

1. Implement Strict Email Policies: Enforce strict policies mandating the use of only authorized and secured email servers for official communications. Employees should be educated on the importance of using approved channels for sensitive information.

2. Regular Security Audits: Conduct regular audits to identify any unauthorized devices or services being used for official purposes. This includes monitoring network traffic for any anomalies that might indicate the use of unapproved email servers.

3. Encryption and Access Controls: Implement strong encryption protocols for emails containing sensitive information and enforce strict access controls to ensure that only authorized personnel can access classified data.

4. Employee Training and Awareness: Provide comprehensive training to employees on proper data handling procedures and the risks associated with using unauthorized communication channels. Regular awareness campaigns can help reinforce the importance of compliance with security policies.

5. Continuous Monitoring: Deploy robust monitoring solutions that can detect and alert administrators to any unauthorized attempts to access or transmit classified information.

b.) The USA government discovered the Hillary Clinton was using her private email server after she had left the position of secretary of state. Briefly suggest the best course of action you would take to prevent any possible attack as a result of the incident giving your reasons for the chosen course of action [3 marks]

Immediate Investigation: Launch a thorough investigation into the incident to determine the extent of the breach and assess any potential damage. This would involve forensically analyzing the email server to identify any security vulnerabilities or unauthorized access.

Enhanced Security Measures: Implement enhanced security measures to mitigate any potential risks stemming from the incident. This could include strengthening network security, implementing stricter access controls, and enhancing encryption protocols for sensitive data.

Transparent Communication: Maintain open and transparent communication with relevant stakeholders, including government agencies and the public, regarding the steps being taken to address the situation and prevent similar incidents in the future.

Collaboration with Law Enforcement: Cooperate fully with law enforcement agencies to investigate any potential legal implications of the incident and ensure that appropriate action is taken.

c.) Discuss the security risks posed by her action with respect to information assurance core principles. [4 marks]

1. Confidentiality: By using a private email server, Clinton potentially compromised the confidentiality of classified information by exposing it to unauthorized access or interception.

2. Integrity: The integrity of the information may have been compromised if it was altered or tampered with during transmission or storage on the private server.

3. Availability: Depending on the security measures implemented on the private server, there may have been risks to the availability of the information if the server experienced downtime or if access was restricted by unauthorized parties.

4. Authenticity: The authenticity of the information could be called into question if it was not transmitted or stored using secure, authenticated channels, potentially leading to issues of trust and reliability.

d.) Discuss the techniques used by antivirus in detecting virus in a computer system [7 marks]

1. Signature-Based Detection: This technique involves comparing files on the system to a database of known virus signatures. If a match is found, the antivirus software flags the file as malicious.

2. Heuristic Analysis: Antivirus programs use heuristic analysis to identify suspicious behavior or patterns in files that may indicate the presence of a virus. This allows the software to detect previously unknown or zero-day threats.

3. Behavioral Analysis: Some antivirus solutions monitor the behavior of programs in real-time to identify suspicious activities, such as attempts to modify system files or network communication with known malicious servers.

4. Sandboxing: Advanced antivirus programs may execute suspicious files in a controlled environment known as a sandbox to observe their behavior without risking harm to the system. This helps in identifying and analyzing potential threats safely.

By employing a combination of these techniques, antivirus software can effectively detect and mitigate the risk of viruses and other malware infecting a computer system.