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

School of Computer Science and Engineering

Winter Semester 2023-24

Continuous Assessment Test – I1

SLOT: F1 + TF1

Programme Name & Branch: B. Tech (BCE, BCI)

Course Name & Code: Information Security, BCSE317L

Class Number (s): VL2023240502374, VL2023240502376, VL2023240502379, VL2023240502381

Faculty Name (s): Dr. Viswanathan A, Dr. Rajeshkannan, Dr. Kathiravan S, Dr. Mukku Nisanth Kartheek

Exam Duration: 90 Min. **Maximum Marks: 50**

Answer all the questions

Q. No.	Question	Max Marks	CO	BL
1.	A financial institution operates a critical online banking platform that handles millions of transactions daily. They are concerned about the increasing sophistication of cyber threats targeting their customers' financial data. The institution is exploring the adoption of trusted systems to bolster the security of their online banking infrastructure. How would you recommend integrating trusted systems into the online banking platform of the financial institution, and what security benefits would they achieve from this implementation?	10	CO4	BL5
A.	Integrating trusted systems into the online banking platform of the financial institution requires a comprehensive approach to enhance the security of the infrastructure and protect sensitive financial data. Here's how the institution can leverage trusted systems and the associated security benefits: **Secure Operating System:** Deploy a trusted operating system with built-in security features and capabilities, such as secure boot, integrity verification, and mandatory access controls. This ensures a secure foundation for hosting critical banking applications and services. **Secure Authentication and Access Control:** Implement trusted authentication mechanisms, such as multifactor authentication and biometric authentication, to verify the identity of users accessing the online banking platform. Combine this with fine-grained access controls to limit access to sensitive data and transactions based on user roles and privileges.			

	Data Encryption and Integrity Protection: Utilize trusted encryption protocols and cryptographic mechanisms to encrypt sensitive data in transit and at rest, safeguarding it from unauthorized interception or tampering. Implement measures to ensure data integrity, such as digital signatures and hash functions, to detect and prevent data manipulation attempts. **Continuous Monitoring and Intrusion Detection:** Deploy trusted monitoring and intrusion detection systems to continuously monitor network traffic, system activities, and user behaviors for signs of suspicious or malicious activities. Leverage anomaly detection algorithms and threat intelligence feeds to identify and mitigate potential security threats in real-time. **Secure Software Development Practices:** Adhere to trusted software development practices, such as secure coding guidelines, code review processes, and vulnerability assessments, to minimize the risk of introducing security vulnerabilities into the online banking platform. Regularly update and patch the system software and applications to address known security vulnerabilities and mitigate emerging threats. By integrating trusted systems into the online banking platform, the financial institution can bolster the security of its infrastructure, protect customer financial data from cyber threats, and maintain the trust and confidence of its customers in the security of their online banking transactions.			
2.	A global manufacturing company operates multiple production facilities and relies on Industrial Control Systems (ICS) to automate manufacturing processes and control critical infrastructure. The company is concerned about the security risks posed by cyber threats targeting its ICS environment and seeks a firewall solution to protect its industrial assets from unauthorized access and cyberattacks. How would you propose implementing a firewall solution to secure the Industrial Control Systems (ICS) environment of the manufacturing company, and what security measures should be prioritized to safeguard critical infrastructure and production processes?	10	CO2	BL4
A.	To secure the Industrial Control Systems (ICS) environment of the manufacturing company, I would recommend implementing a specialized firewall solution designed specifically for			

	operational technology (OT) environments with the following security measures: **Segmentation and zoning:** Implement network segmentation and zoning to isolate critical ICS components, such as Programmable Logic Controllers (PLCs) and Supervisory Control and Data Acquisition (SCADA) systems, from non-critical networks and devices. Establish strict access controls and firewall rules to regulate communication between different network zones and prevent unauthorized access to ICS assets. **Deep packet inspection:** Deploy deep packet inspection capabilities to analyze network traffic at the application layer and detect anomalous or malicious activities targeting ICS protocols and communication patterns. Configure firewall rules to filter out unauthorized commands or data packets that could compromise the integrity or availability of industrial assets and production processes. **Application whitelisting:** Enforce application whitelisting policies to allow only authorized software and processes to interact with ICS devices and systems. Restrict the execution of unapproved applications and services to mitigate the risk of malware infections and unauthorized access to critical infrastructure components. **Protocol filtering and validation:** Filter and validate incoming network protocols and data packets to ensure compliance with industry standards and best practices for ICS communication. Block or quarantine network traffic that deviates from expected protocol specifications or exhibits suspicious behavior indicative of cyberattacks or tampering attempts. **Continuous monitoring and anomaly detection:** Implement continuous monitoring and anomaly detection mechanisms to detect and respond to security incidents and abnormal behavior in the ICS environment. Integrate firewall logs and security event data with centralized monitoring and incident response systems to facilitate timely detection, investigation, and remediation of security threats. By implementing a specialized firewall solution tailored to the unique security requirements of Industrial Control Systems (ICS), the manufacturing company can effectively safeguard its critical infrastructure and production processes			

	against cyber threats, ensure operational continuity, and maintain the integrity and availability of industrial assets.			
3.	A healthcare organization manages a vast amount of sensitive patient information within its network, including electronic health records (EHRs) and personally identifiable information (PII). The organization is concerned about the increasing frequency of cyberattacks targeting healthcare data and wants to deploy an Intrusion Detection and Prevention System (IDPS) to protect its network infrastructure and safeguard patient confidentiality. How would you advise the healthcare organization to deploy and configure the IDPS effectively to mitigate the risk of data breaches and unauthorized access to patient information?	10	CO2	BL2
A.	To protect its network infrastructure and sensitive patient information effectively, the healthcare organization should deploy and configure the IDPS with a focus on the following key considerations: **HIPAA Compliance:** Ensure that the IDPS deployment and configuration align with the requirements of the Health Insurance Portability and Accountability Act (HIPAA) to protect patient privacy and maintain compliance with healthcare data security regulations. **Sensitive Data Monitoring:** Configure the IDPS to monitor and analyze network traffic for signs of unauthorized access, data exfiltration, or other suspicious activities involving sensitive patient information, such as EHRs and PII. Implement signature-based detection rules and anomaly-based detection mechanisms tailored to detect healthcare-specific threats and attack vectors. **Medical Device Protection:** Extend IDPS coverage to include medical devices connected to the network, such as MRI machines, infusion pumps, and patient monitors. Collaborate with medical device vendors to ensure compatibility and interoperability with the IDPS solution while minimizing disruptions to patient care. **Secure Remote Access:** Implement secure remote access solutions, such as virtual private networks (VPNs) or remote desktop gateways, to facilitate remote access to healthcare systems and resources while maintaining strong authentication and encryption controls. Integrate the IDPS with remote access gateways to monitor and protect remote connections from potential security threats.			

	Incident Response Planning: Develop and document comprehensive incident response procedures and workflows to guide the organization's response to security incidents detected by the IDPS. Define roles and responsibilities, escalation paths, and communication protocols to facilitate timely incident detection, investigation, containment, and recovery efforts. **Data Loss Prevention (DLP):** Integrate DLP capabilities with the IDPS to prevent the unauthorized transmission of sensitive patient information outside the organization's network boundaries. Configure DLP policies to monitor and enforce data handling rules, such as encryption requirements and access controls, to prevent data leakage and compliance violations. **Continuous Monitoring and Evaluation:** Establish continuous monitoring processes to assess the effectiveness of the IDPS in detecting and mitigating security threats within the healthcare organization's network environment. Conduct regular security assessments, penetration tests, and audits to validate the IDPS's configuration and performance against evolving cybersecurity threats and regulatory requirements. By deploying and configuring the IDPS according to these recommendations, the healthcare organization can enhance its cybersecurity defenses, protect sensitive patient information from unauthorized access and data breaches, and demonstrate a commitment to patient privacy and regulatory compliance.			
4.	A research institution conducts groundbreaking research and development projects, storing valuable intellectual property and proprietary information in its database systems. The institution is concerned about the potential risks of intellectual property theft, industrial espionage, and cyberattacks targeting its database infrastructure. How would you advise the research institution to implement database security measures to protect its valuable intellectual property and proprietary information effectively, considering the risks of intellectual property theft and industrial espionage?	10	CO5	BL3
A.	To protect valuable intellectual property and proprietary information effectively in its database environment, the research institution should implement robust database security measures tailored to address the risks of intellectual property theft, industrial espionage, and cyberattacks			

	targeting its database infrastructure: **Data Classification and Access Controls:** Classify sensitive intellectual property and proprietary information based on its value, sensitivity, and confidentiality requirements. Implement access controls and privilege management mechanisms to restrict access to classified data based on user roles, responsibilities, and the principle of least privilege. **Database Encryption and Tokenization:** Encrypt sensitive intellectual property and proprietary information at rest and in transit to protect it from unauthorized access or interception. Utilize encryption techniques, such as transparent data encryption (TDE) and application-level encryption, to encrypt data stored in the database. Consider implementing tokenization techniques to replace sensitive data with surrogate tokens or pseudonyms to further reduce the risk of data exposure. **Database Activity Monitoring and Auditing:** Deploy database activity monitoring (DAM) and auditing solutions to track and log all database transactions, including data accesses, modifications, and administrative activities. Enable real-time alerting mechanisms to notify security personnel of suspicious database activities or policy violations, such as unauthorized data accesses or data exfiltration attempts. **Insider Threat Detection:** Implement user behavior analytics (UBA) solutions to monitor and analyze user activities, behaviors, and access patterns within the database environment. Utilize machine learning algorithms and anomaly detection techniques to identify suspicious user behaviors indicative of insider threats, such as unauthorized data accesses, data downloads, or abnormal data retrieval patterns. **Database Firewalling and Intrusion Detection:** Deploy database firewall solutions and intrusion detection systems (IDS) to enforce access controls and traffic filtering rules at the network perimeter, protecting the database server from unauthorized access attempts and SQL injection attacks. Configure firewall policies to allow only authorized clients and applications to access the database server and block or alert on suspicious database traffic. **Continuous Monitoring and Threat Intelligence:** Establish continuous monitoring processes and			

	threat intelligence feeds to detect and respond to emerging cyber threats targeting the database infrastructure. Monitor dark web forums, hacker communities, and threat intelligence sources for indicators of compromise (IOCs) and cyber attack trends relevant to the research institution's industry sector. By implementing these database security measures, the research institution can enhance the protection of its valuable intellectual property and proprietary information, mitigate the risks of intellectual property theft and industrial espionage, and safeguard its competitive advantage and innovation capabilities.			
5.	A government agency manages a centralized database containing sensitive information about citizens, including social security numbers, tax records, and employment history. The agency's database is vulnerable to SQL injection attacks due to legacy systems and outdated security controls. As a cybersecurity expert, how would you evaluate the potential consequences of a successful SQL injection attack on the government agency's database, and what recommendations would you provide to prevent such attacks and minimize the impact?	10	CO5	BL5
A.	Assessing the potential consequences of a successful SQL injection attack on the government agency's database involves considering the criticality of the information stored, regulatory compliance requirements, and the impact on citizens' privacy and trust. Here's how I would evaluate the consequences and provide recommendations: **Impact Assessment:** **Data Breach:** A successful SQL injection attack could lead to unauthorized access to sensitive citizen information stored in the database, including social security numbers, tax records, and personal identifiers, compromising individuals' privacy and confidentiality. **Identity Theft and Fraud:** Attackers may exploit stolen personal information obtained from the database to perpetrate identity theft, financial fraud, or other criminal activities, causing financial losses and reputational damage to affected individuals and the government agency. **Regulatory Non-Compliance:** Data breaches resulting from SQL injection attacks may violate regulatory requirements, such as the Health Insurance Portability and Accountability Act			

	(HIPAA) or the General Data Protection Regulation (GDPR), exposing the government agency to regulatory fines and penalties. **Public Trust and Confidence:** Public disclosure of a SQL injection attack and data breach can erode citizens' trust and confidence in the government agency's ability to protect their sensitive information, leading to reputational damage and loss of public trust. **Recommendations:** **Database Hardening:** Secure the database infrastructure by implementing rigorous security controls, including encryption of sensitive data, regular patching of database software, and disabling unnecessary features and services to reduce the attack surface. **Input Validation and Sanitization:** Strengthen input validation mechanisms to sanitize user input and prevent SQL injection attacks. Use parameterized queries or prepared statements to separate user input from SQL code and mitigate injection vulnerabilities. **Access Controls:** Implement least privilege access controls to restrict database user permissions and privileges, limiting the ability of attackers to execute unauthorized SQL queries or access sensitive data. Utilize role-based access control (RBAC) and access control lists (ACLs) to enforce data access policies. **Monitoring and Logging:** Deploy database activity monitoring (DAM) solutions to track and log all database transactions, including SQL queries, data modifications, and user access events. Enable real-time alerting mechanisms to notify administrators of suspicious database activities or policy violations. **Incident Response Planning:** Develop and document comprehensive incident response procedures and workflows to guide the government agency's response to SQL injection attacks and data breaches. Define roles and responsibilities, escalation paths, and communication protocols to facilitate timely incident detection, containment, and recovery efforts. By implementing these recommendations, the government agency can mitigate the risk of SQL injection attacks, protect citizen data from unauthorized access and manipulation, and minimize the financial, legal, and reputational consequences of security breaches on its database infrastructure.			