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 – I

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

1. You are working as a Chief Information Security Officer (CISO) for a telecommunication service provider. Most of the business of the service provider is running online and requires the clients to use the web service for different tasks like recharging balance, creating/updating profiles, billing details, switching to/from another network, etc. Your job is to secure online business transactions. Highlight four areas that you think are critical in web businesses, give examples of two possible threats in each area, and the countermeasures that can be taken to avoid those threats. [10 Marks]

Critical Areas in Web Businesses, Threats, and Countermeasures:

a. Data Protection:
Threats: Data breaches, unauthorized access
Countermeasures: Encryption, access controls, regular vulnerability assessments, employee training on data handling.

b. Network Security:
Threats: DDoS attacks, network sniffing
Countermeasures: Firewalls, intrusion detection/prevention systems, network segmentation, encryption, monitoring and logging.

c. User Authentication:
Threats: Password cracking, phishing attacks
Countermeasures: Strong password policies, multi-factor authentication, user awareness training, anti-phishing measures.

d. Application Security:
Threats: SQL injection, cross-site scripting (XSS)
Countermeasures: Secure coding practices, input validation, regular security testing, patch management.

---

2. Viruses, worms, Trojan horses, and hacking are all security issues in our computer network. Each of these malwares or programs attaches and spreads in different ways. Through hacking hackers can infect computers with various types or malware and viruses. Explain what viruses are, how it occurs and the types of cybercrimes that can result from it, and how to better protect computers. [10 Marks]

A virus is a type of malicious code or program written to alter the way a computer operates and is designed to spread from one computer to another. A virus operates by inserting or attaching itself to a legitimate program or document that supports macros in order to execute its code. In the process, a virus has the potential to cause unexpected or damaging effects, such as harming the system software by corrupting or destroying data.

Viruses can occur through email and text message attachments, Internet file downloads, and social media scam links. Mobile devices and smartphones can become infected with mobile viruses through shady app downloads. Viruses can hide disguised as attachments of socially shareable content such as funny images, greeting cards, or audio and video files.

The various types of cybercrimes that can result from computer viruses are:

- Illegal use of an infected computer's resources
- Stealing Electronic Currency
- Stealing Online Banking Information
- Ransomware & Cyber Blackmail
- Advertise products or services on a victim's computer
- Identity theft
- Stealing personal information
- Cyberstalking

Some ways in which we can better protect our computers are

- Keeping your software updated
- Enabling your system firewall
- Usage of different/strong passwords
- Use of antivirus and anti-malware software
- Shop only from secure and well-known websites
- Not downloading unknown files from the web

---

3. Design a robust authentication system for the following scenario: Dr. Harry wants to take attendance in his class Information Security. However, he also wants to make sure only people actually present in the class can submit the attendance form. He is using a QR code which the students scan to access the attendance form.

What type or types of authentication factor(s) will you choose to make sure that only students present in the class are able to authenticate themselves and submit the attendance form? Explain the reasons

behind your design decision. What are the advantages and disadvantages of the mechanism you chose?

[10 Marks]

There are a few different types of authentication factors that could be used in this scenario. The best authentication factor or combination of factors would depend on a number of factors, including the security requirements of the system and the ease of use for the users. The pupils could, for instance, need to submit a class password to view the form.

Explanation:

There are a few different types of authentication factors that could be used in this scenario in order to make sure that only students present in the class are able to submit the attendance form.

One option would be to use a physical token, such as a keycard, that the students would need to have in order to scan the QR code and access the form. This would ensure that only students who are physically present in the class would be able to access the form. However, this option could be disadvantageous as it would require the students to remember to bring their keycards to class with them.

Another option would be to use a biometric authentication factor, such as a fingerprint scanner. This would require the students to have their fingerprints registered in order to access the form. This option would be more secure than the keycard option, as it would be more difficult to spoof a fingerprint than it would be to spoof a keycard. However, this option could also be disadvantageous as it would require the students to have their fingerprints registered in advance, which could be logistically difficult to implement.

A third option would be to use a combination of an authentication factor and a knowledge-based factor. For example, the QR code might be utilized as an authentication mechanism, with students needed to submit a class password to access the form. This option would be more secure than using just the QR code as the authentication factor, as it would require the students to have both the QR code and the class password in order to access the form. However, this option could be disadvantageous as it would require the students to remember the class password in addition to the QR code.

Ultimately, the best authentication factor or combination of factors to use in this scenario would depend on a number of factors, including the security requirements of the system, the ease of use for the users, and the feasibility of implementation.

---

4. A multinational IT services company consisting of 120,000 computers that have Internet access and 45,000 servers. All employees communicate using smartphones and e-mail. Many employees work from home and travel extensively. In such scenario, identify the data that would need to be protected. Recommend how you would implement one or more of the access controls for the given scenario. Justify your recommendations. [10 Marks]

Data to be protected: Employee and client information, proprietary software code, financial reports, intellectual property, confidential business data etc.

Access Control Recommendation: Implement a combination of administrative controls, logical/technical controls, software controls, and physical controls. Establish comprehensive security policies, including access control policies, incident response procedures, and regular security awareness training.

Explanation

Utilize **role-based access controls (RBAC)** for managing user permissions. Implement strong authentication mechanisms, such as smart cards or security tokens. Employ network firewalls, intrusion detection systems, and encryption technologies. Physically secure data centers and restrict access to critical infrastructure.

---

5. Imagine you work as an IT security specialist for a medium-sized company that relies heavily on Windows-based systems for its day-to-day operations. You've recently been informed about a potential security breach in the Windows operating system used throughout the organization. You need to assess the situation and make critical decisions to protect the company's data and infrastructure.

Given this scenario, please outline the steps you would take to investigate and mitigate the security breach in the Windows operating system. What security measures and best practices would you recommend to prevent such incidents in the future? [10 Marks]

According to the given question below **Investigating and mitigating** a security breach in a Windows-based system is a critical task that requires a systematic approach.

Below is a step-by-step guide on what we should do to address the situation and prevent future incidents:

1. **Isolate the Affected System(s):** The first step is to isolate the compromised system to prevent further damage. Disconnect it from the network and power it down if necessary.
2. **Contain the Breach:** Assess the extent of the breach to determine if other systems have been compromised. If so, isolate those as well. This containment prevents the attacker from moving laterally within the network.
3. **Gather Evidence:** Collect all relevant logs, records, and evidence of the breach. This may include system logs, firewall logs, network traffic captures, and any suspicious files or activities on the affected systems.

4. **Analyze the Breach:** Investigate how the breach occurred. Look for signs of exploitation, malware, or unauthorized access. Determine the attack vector and the vulnerabilities that were exploited.
5. **Patch and Remediate:** Identify the specific vulnerabilities that were exploited and apply patches and updates to fix them. Ensure that all systems are up to date with the latest security patches.
6. **Review Access Control:** Examine user accounts and privileges. Remove or restrict unnecessary permissions and reset passwords for affected accounts. Implement multi-factor authentication (MFA) where possible.
7. **Scan for Malware and Intrusions:** Use reputable antivirus and intrusion detection tools to scan for malware and signs of compromise on affected systems. Remove any detected malware.
8. **Change All Passwords:** Promptly change all passwords, especially for privileged accounts. Encourage strong, unique passwords and the use of a password manager.
9. **Monitor and Analyze Network Traffic:** Continuously monitor network traffic for any suspicious activities. Invest in intrusion detection and prevention systems (IDS/IPS) to identify and block potential threats.

10. **Educate and Train Employees**: Security awareness and training programs are crucial. Ensure employees are aware of best practices, social engineering tactics, and how to report suspicious activities.

11. **Review and Enhance Security Policies:** Review and update your organization's security policies. Implement a formal incident response plan that outlines roles and responsibilities during a security incident.
12. **Backup and Disaster Recovery:** Regularly back up critical data and test your disaster recovery plan to ensure data can be restored in the event of a breach or data loss.
13. **Engage External Experts:** Consider bringing in external cybersecurity experts to assist with the investigation, remediation, and to provide guidance on improving your security posture.

To prevent future incidents, below are some security measures and best practices to implement:

1. **Regularly Update and Patch:** Keep all Windows-based systems, software, and applications up to date with the latest security patches and updates.
2. **Firewall and Intrusion Prevention:** Use firewalls and intrusion prevention systems to monitor and control network traffic.
3. **Endpoint Protection:** Deploy robust antivirus and anti-malware solutions on all devices.
4. **Access Control:** Implement the principle of least privilege, limiting users' access to only what they need to perform their jobs.
5. **Network Segmentation:** Segment your network to isolate critical systems from less critical ones, reducing the attack surface.
6. **User Training:** Continuously educate and train employees on security best practices and how to recognize phishing and social engineering attempts.
7. **Encryption:** Encrypt sensitive data at rest and in transit.
8. **Multi-Factor Authentication (MFA)**: Enable MFA for all critical systems and accounts.
9. **Regular Security Audits:** Conduct periodic security audits and vulnerability assessments.
10. **Incident Response Plan:** Maintain a well-documented incident response plan and regularly test it through tabletop exercises.
11. **Backup and Recovery:** Regularly back up data and test the restoration process.
12. **External Penetration Testing:** Periodically engage external penetration testers to identify vulnerabilities from an external perspective.
13. **Secure Configuration Management:** Implement security baselines and configurations for your Windows systems to reduce vulnerabilities.
