الجامعة اللبنانية
كلية الإعلام
الفرع الأول

الجامعة اللبنانية
كلية الإعلام

Third Year

Semester VI

Duration: 120 minutes

Advanced Data Security

Second Session
2022 / 2023

Date:

Instructor : Dr. K. Danach

Part I: **Very** Short Questions:

Question 1: What is confidentiality in the context of information security? Why is confidentiality important to protect sensitive information? How can confidentiality be achieved in a system or communication?

Question 2: What is authentication and why is it crucial in information security? How does authentication help verify the identity of users or systems? What methods or techniques can be employed for authentication?

Question 3: What is SSL (Secure Sockets Layer)? How does SSL work to establish secure communication over the internet? What are the advantages or benefits of using SSL for websites or online services in terms of security and user trust?

Question 4: What is the concept of access and availability in the context of information systems? Why are access control and availability essential for maintaining system security and functionality? What strategies or measures can be implemented to achieve proper access control and ensure high availability?

Question 5: What is message integrity and why is it significant in secure communication? How can message integrity be ensured to prevent unauthorized modification or tampering of data during transmission? What techniques or mechanisms are used to achieve message integrity?

Part II: Case Study

Your organization, a large financial services company that handles sensitive customer data, has decided to conduct a penetration test to assess the security of its systems. As the head of the security team, you are aware that conducting such a test in a large, complex organization can present several challenges.

- Identify and explain three challenges you might face when conducting a penetration test of a large, complex organization.
- How would you address each of these challenges to ensure a successful penetration test? Provide specific strategies or approaches that you would implement.
- What are the potential risks associated with conducting a penetration test in a live production environment? How would you mitigate these risks and ensure minimal impact on critical systems and operations?
- Outline the key stakeholders and teams that need to be involved in the penetration testing process within your organization. Explain the roles and responsibilities of each stakeholder and how their collaboration is crucial for a successful penetration test.
- Considering the sensitive nature of the customer data your organization handles, what legal and compliance considerations should be taken into account when conducting a penetration test? Discuss the importance of obtaining proper authorization and maintaining confidentiality throughout the testing process.
- Once the penetration test is complete, how would you ensure that the identified vulnerabilities and weaknesses are properly addressed and remediated? Describe the steps you would take to ensure that the organization's security posture is improved based on the test findings.

Part III: Comprehension Questions:

1. Can you outline the six phases involved in a typical penetration testing process?
2. For each phase of penetration testing, what specific objectives or goals should be achieved?
3. During each phase of penetration testing, what are some common challenges that testers may face?

4. How can the findings and results obtained from a penetration test be effectively utilized to enhance the overall security posture of an organization?
5. Could you explain the advantages and benefits associated with the utilization of S-HTTP (Secure HTTP)?