



DEPARTMENT OF COMPUTER SCIENCE
TERMINAL EXAMINATION FALL - 2023
BS (SE)– VIII SEMESTER
BS (DS)– III-V-VI SEMESTER

Course: CSC432-Information Security

Maximum Marks: 50

Course Instructor: Dr. Tehsin Kanwal

Dated: January 16, 2024

Time Allowed: 180 Minutes

- All questions are self-explanatory and require no further explanations during exam time.
- Make sure that you have signed the attendance sheet before leaving the examination room.
- Return the question paper along with the answer sheet.
- Attempt all questions.

CLO-1. Discuss the fundamental concepts, policies, standards and ethical issues of information security.

Question 1. Short Question Answers [2*5=10 Marks]

- 1.1 Suppose you have a new smartphone and are excited about the range of apps available for it. You read about a really interesting new game that is available for your phone. You do a quick Web search for it, and see that a version is available from one of the free marketplaces. When you download and start to install this app, you are asked to approve the access permissions granted to it. You see that it wants permission to "Send SMS messages" and to "Access your address-book". Should you be suspicious that a game wants these types of permissions? What threat might the app pose to your smartphone, should you grant these permissions and proceed to install it? What types of malware might it be?
- 1.2 In a Unix Kerberos implementation, each user's tickets (including the TGT ticket for the TGS service) are stored in a per-user file in /tmp. The Unix permissions on this file are such that the user's UID has access to that file, but the group and others do not. Ben Bitdiddle wants to send an email to Alyssa, and to include a copy of the Kerberos paper as an attachment, but because he stayed up late studying for this quiz, he accidentally sends his Kerberos ticket file as an attachment instead. What can Alyssa do given Ben's ticket file? Be precise.
- 1.3 Suppose you receive a letter from a finance company stating that your loan payments are in arrears, and that action is required to correct this. However, as far as you know, you have never applied for, or received, a loan from this company! What may have occurred that led to this loan being created? What type of malware, and on which computer systems, might have provided the necessary information to an attacker that enabled them to successfully obtain this loan?
- 1.4 Consider an automated teller machine (ATM) in which users provide a personal identification number (PIN) and a card for account access. Explain with examples of confidentiality, integrity, and availability requirements associated with the system.
- 1.5 Differentiate between a bot, spyware, and a rootkit?

CLO-2 Investigate various counter measures and security controls exposure.

Question 2 [5 points]: Risk Management.

Consider a formal risk assessment of desktop systems in a small accounting firm with limited IT support, you have identified the asset "integrity of customer and financial data files on desktop systems" and the threat "corruption of these files due to import of a worm/virus onto system." Identify reasonable values for the items in the risk register/risk analysis process for this asset and threat, and provide justifications for your choices.

CLO-3 Analyze various information security technologies.

Question 3 [2.5 + 2.5 = 05 points]: Firewall, IDS.

- 3.1 Analyze the working mechanism of different types of Firewalls with the help of sample scenario.
- 3.2 Intrusion Detection Systems is one of the defense mechanisms use to detect attempts to circumvent security measures. Discuss different analysis Approaches for IDS.

Question 4 [10 + 10 + 5 = 25 points]: Cryptography.

- 4.1 Perform encryption and decryption using the RSA algorithm for given values, $p = 5$; $q = 11$, $e = 3$; M (Message) = R-18, S-19, A-1.
- 4.2 Apply knowledge of hashing and digital signatures and explain the working mechanism both in text and with the help of diagrams.
- 4.3 Steganography is an information hiding mechanism that can be used for constructive and destructive purposes, support the given statement with concise description.

CLO-4 Describe the policies and procedures to information security implementation and maintenance.

Question 5 [2.5 + 2.5 = 05 points]: Information Security Standards and Security Management.

- 5.1 The UMAS are gearing up for a major IT project that will automate the processing of medical aid claims from GPs. You have been asked to upgrade information security and privacy best practices. The available options COBIT, FISMA or Health Insurance Portability and Accountability Act HIPAA? State which one you would select as best practice and why you have made that decision.
- 5.2 Explain Digital Forensic process along with different Types, When is Digital Forensics used in a Business Setting?

-----End-----