W/D/TY

VIT
Vellore Institute of Technology

Final Assessment Test – April 2025

Course: BCSE317L - Information Security
Class NBR(s): 1840/1861/1871/1875/1933/1936/1945
Time: Three Hours

Slot: B1+TB1
Max. Marks: 100

- KEEPING MOBILE PHONE/ANY ELECTRONIC GADGETS, EVEN IN 'OFF' POSITION IS TREATED AS EXAM MALPRACTICE
- DON'T WRITE ANYTHING ON THE QUESTION PAPER

Answer ALL Questions
(10 X 10 = 100 Marks)

1. A company employee downloads a software update from an unofficial website. Once installed, the software appears to function normally, but in the background, it silently exfiltrates sensitive information to an external server controlled by the attacker.
Identify the attack given in the scenario and what steps should the company take immediately after detecting the attack to contain and prevent further data exfiltration?

2. A company uses a single sign-on (SSO) solution for its internal applications, allowing employees to log in once and gain access to multiple systems without re-entering their credentials. Recently, security audits have revealed that users are using weak passwords, and some employees share their credentials.
Recommend and explain the authentication protocols that could be implemented to enhance the security of the single sign-on (SSO) system.

3. A financial organization deploys an OS with a kernelized design to ensure that sensitive transactions and data processing are handled in a highly secure environment. This design isolates critical functions in the kernel, preventing unauthorized access to core resources.
   (i) Discuss the key security benefits of a kernelized design in an operating system. [5]
   (ii) How does isolating critical functions in the kernel help prevent unauthorized access or manipulation? [5]

4. A system administrator detects unusual activity on a high-security server, including changes to system logs and processes that appear to be hidden. The administrator suspects that a rootkit has been installed on the system, allowing attackers to maintain privileged access while hiding their tracks.
   (i) How does a rootkit typically function to conceal malicious activities and evade detection by system administrators or security software? [5]
   (ii) What steps should the administrator take to detect and remove a rootkit from a compromised system? [5]

5. Discuss how browser vulnerabilities can be exploited by attackers to carry out attacks like malware distribution or unauthorized data access. Provide examples of specific browser vulnerabilities and explain the methods attackers use to exploit these vulnerabilities.

6. A company employee receives an email from a trusted internal source, requesting that they follow a link to complete a security update. The email contains a link with a URL that looks similar to the company's internal domain but has minor variations.
Articulate how can an employee identify a phishing URL, and what measures should the organization implement to prevent employees from falling victim to phishing attacks through internal emails?

7. Elaborate on the steps that individuals and organizations can take to protect against privacy loss.

8. Consider a scenario where a company shares sensitive client data with an external vendor. Describe how cryptographic techniques, such as encryption and secure protocols, can ensure that the data remains confidential during transmission.

9.a) A company's internal network uses private IP addresses, but they need to access external services on the internet. To hide internal IP addresses and protect the internal network, the company is considering implementing Network Address Translation (NAT) on their firewall.

a) Illustrate how does Network Address Translation (NAT) work to protect internal networks, and what are its benefits in this scenario. [5]

b) Compare and contrast NAT with application gateway firewall. [5]

OR

9.b) A security team has deployed both signature-based and anomaly-based Intrusion Detection Systems (IDS) to monitor for potential threats in their network. They are now reviewing the effectiveness of each type of IDS and evaluating which method would best suit their organization.
Summarize the key differences, strengths, limitations, and ideal use cases for signature-based IDS and anomaly-based IDS in detecting and responding to attacks?

10.a) An e-commerce platform's database includes sensitive customer information, including order history and payment details. A security vulnerability has been identified that could lead to the unauthorized disclosure of personal information.

Explain the various types of disclosures that can happen in a database, and how do they threaten user privacy and the organization's reputation?

OR

10.b) Describe the various types of SQL injection attacks. Provide examples for each type and explain how they take advantage of vulnerabilities in web applications to gain unauthorized access to a database.

⇔⇔⇔ W/D/TY ⇔⇔⇔