J/L/TX

Reg. No:

# Final Assessment Test – November 2024

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

Course: **BCSE410L - Cyber Security**

Class NBR(s): **1875/1882/1887/1901/1916/1918/1922/1924/1928**

Slot: **F2+TF2**

Time: **Three Hours**

Max. Marks: **100**

- **KEEPING MOBILE PHONE/ELECTRONIC DEVICES 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. | Let assume that, your organization is migrating to a cloud-based infrastructure, and you need to assess the security implications. Discuss the specific security assessment principles should be applied in this scenario and explain the unique risks might you encounter in a cloud environment. | | **BL1** | **CO1** |
| 2. | An e-commerce company has decided to conduct a penetration test on its web application to identify security vulnerabilities before the holiday shopping season. The test is aimed at assessing the security posture of their online platform, which handles sensitive customer data, including payment information.<br>i. How important is it to define the scope of a penetration test clearly? What potential issues could arise from an improperly defined scope?<br>ii. What specific reconnaissance techniques can be employed to gather information about the web application? How might attackers exploit information gathered during this phase? | | **BL2** | **CO1** |
| 3. | a) How should organizations adapt their security training based on the results of social engineering tests conducted with SET (Social Engineering Toolkit)? | **[5]** | **BL3** | **CO2** |
| | b) What measures can organizations implement to mitigate the risk of social engineering attacks? Can you give example of real-world social engineering incidents. | **[5]** | | |
| 4. | a) What are the primary methods used by keyloggers to capture keystrokes, and how do these methods impact the effectiveness of different keylogger types? | **[5]** | **BL4** | **CO2** |
| | b) In what ways can keylogger attacks be used in conjunction with other types of attacks (e.g., phishing or social engineering) to enhance their effectiveness? How do keyloggers bypass traditional security measures such as firewalls and antivirus software? | **[5]** | | |
| 5. | A mid-sized company has implemented a wireless network for employees to access internal resources. The IT department has enforced MAC address filtering as a basic security measure, allowing only registered devices to connect to the network. An attacker, aiming to gain unauthorized access to the network, identifies a registered device's MAC address through social engineering techniques (e.g., observing the device in a public area) or network sniffing. | | **BL4** | **CO3** |

i. What specific countermeasures could the organization implement to defend against MAC spoofing attacks? Discuss both technical and administrative controls.
ii. How can enhanced network monitoring and anomaly detection help in identifying unauthorized access attempts, even when MAC addresses are spoofed?

6. A mid-sized corporation relies heavily on a Windows-based operating system for its internal applications and data storage. Recently, the IT department noticed unusual network activity, followed by multiple reports of users being unable to access their files. Upon investigation, it was determined that a ransomware attack had compromised several endpoints. **BL4 CO3**

i) How would you assess the operating system vulnerabilities that were exploited? What tools or methods would you use to identify these weaknesses?

ii) What immediate actions should be taken by IT team? How would you isolate infected systems while minimizing disruption?

7. Explain the mechanism of buffer overflow attacks. What are the common causes of buffer overflow vulnerabilities in operating systems? Discuss the potential consequences of a successful buffer overflow exploit. Analyze various countermeasures that can be implemented to prevent buffer overflow attacks. **BL4 CO3**

8. In March 2023, XYZ Corp experienced a significant security breach when attackers exploited vulnerabilities in their web application. Sensitive customer data, including personal information and payment details, were compromised. This incident led to reputational damage, legal repercussions, and financial losses. **BL3 CO4**

As a security engineer, conduct security assessment to identify the vulnerabilities and recommend precautionary measures for this scenario.

9.a) Explore the role of encryption in protecting sensitive data within databases. How can organizations implement encryption both at rest and in transit to minimize exposure to data breaches? **BL5 CO4**

**OR**

9.b) Discuss the critical role of data backup and recovery processes in minimizing storage security risks. How can organizations implement effective backup strategies to ensure data integrity and availability in the event of a security incident? **BL5 CO5**

10.a) Explore emerging technologies, such as block chain and quantum computing, and their potential impact on cyber security. How might these innovations shape the future of threat detection and data protection? **BL5 CO4**

**OR**

10.b) Examine the cyber security challenges posed by the increase in remote work due to the COVID-19 pandemic. Explain the strategies can organizations implement to secure remote access and protect sensitive data in distributed environments. **BL5 CO4**

⇔⇔⇔ **J/L/TX** ⇔⇔⇔