VIT

Vellore Institute of Technology

Slot: E2

School of Computer Science Engineering and Information Systems

Fall Semester 2024-2025

Continuous Assessment Test – I

Programme Name & Branch: M.Tech SE

Course Name & code: CSE 3501 & Information Security Analysis and Audit

Class Number (s): VL2024250103022/3006/3038/3053

Faculty Name (s): Kumaresan P, Nadesh R K, Mohana Priya P, Charanya R

Exam Duration: 90 Min. **Maximum Marks: 50**

Answer ALL Questions

1. Identify the malware that invade your computer by hiding its original identity and install malicious operational program on the targeted victim. The malware is related to cavalry kingdom attack which has many shades to generate cyber security attacks. Discuss its types providing suitable examples.

2. It is as much important to secure banking transactions of a customer by deploying suitable cryptographic techniques. ABC bank has introduced security measures for their bank customers by providing cryptographic key systems. Explain technical elements of cryptography and types of cryptographic key systems in order to secure customers data with appropriate illustration.

3. As a network administrator, illustrate the established campus network with installed network devices. Discuss about the deployed firewall and its types for safeguarding their employee privacy by constructing sample firewall rules for social network sites.

4. Imagine you are a network security engineer for a mid-sized company. Your organization has recently been experiencing a series of cyber-attacks, including unauthorized access attempts, malware infiltration, and insider threats. The company's network infrastructure includes web servers, databases, and employee workstations, all connected to a central network. Implement the Intrusion detection system to enhance its security mechanism with suitable illustration.

5. You are the lead security analyst at a medium-sized e-commerce company that handles thousands of online transactions daily. Recently, your company has received a security audit report highlighting several vulnerabilities in your web applications, database servers, and network infrastructure. The vulnerabilities include outdated software versions, improper access controls, unpatched security flaws, and misconfigurations that could potentially be exploited by attackers. List the System security tools, address them, and ensure that the company's systems are secure against potential threats.