CYBER SECURITY ASSIGNMENT QUESTION

DAY 80

1. Explain the process of database forensics and its importance in digital investigations. Discuss the techniques and tools used to retrieve and analyze data or metadata found in databases to uncover evidence of cybercrimes, data breaches, or insider threats.

2.Discuss the challenges and techniques of malware forensics in analyzing malicious code to identify and analyze viruses, ransomware, or Trojan horses. Explain how forensic analysts use static and dynamic analysis techniques, reverse engineering, and sandboxing to dissect malware samples and understand their behavior.

3.Explore the role of database forensics in investigating data breaches and insider threats. Discuss how forensic analysts use database logs, audit trails, and transaction histories to reconstruct digital events, trace data exfiltration attempts, and identify insider misuse or unauthorized access to sensitive data.

4. Discuss the process of malware forensics in analyzing ransomware attacks. Explain how forensic analysts can extract and analyze ransomware samples, identify encryption algorithms, and recover encrypted files to support incident response and recovery efforts.

5.Explore the applications of database forensics and malware forensics in incident response and digital forensics investigations. Discuss how these forensic techniques are used to gather digital evidence, reconstruct cyber incidents,

and support legal proceedings in criminal cases or civil litigation.