CYBER SECURITY ASSIGNMENT QUESTION

DAY 71

1. Explain the concept of live forensics and its importance in digital investigations. Discuss the challenges and techniques involved in conducting live forensics on a running system.

2. Discuss the significance of memory forensics in digital investigations. Explain how memory analysis techniques are used to extract valuable evidence from volatile memory (RAM) dumps.

3. Explain the role of live forensics in incident response and digital investigations. Discuss how live system analysis can help identify and mitigate security incidents in real-time.

4.Discuss the challenges and limitations of memory forensics in digital investigations. Explain how factors such as encryption, anti-forensic techniques, and system volatility can impact the effectiveness of memory analysis.

5.Explain the process of capturing and analyzing memory dumps in memory forensics. Discuss the steps involved in acquiring, extracting, and analyzing volatile memory contents to uncover evidence of malicious activities.