Day 10

Key Aspects of Cross-Layer Detection

1. Multiple Data Sources:
    - Network Layer: Monitors network traffic, connections, and patterns.
    - System Layer: Observes system calls, process behavior, and interactions between applications and the operating system.
    - File System Layer: Tracks file changes, access patterns, and modifications.
    - Application Layer: Analyzes application logs and behavior for anomalies.
2. Integration and Correlation:
    - Data Aggregation: Collects data from various layers to create a unified view.
    - Correlation Analysis: Cross-references information from different sources to identify suspicious or malicious patterns that might not be evident when analyzing a single layer in isolation.
3. Enhanced Threat Detection:
    - Behavioral Patterns: Identifies behaviors indicative of threats, such as rapid file encryption (often seen with ransomware) or unusual network activity.
    - Contextual Awareness: Provides context by combining data from multiple sources, improving the accuracy of threat detection and reducing false positives.
4. Improved Response:
    - Automated Actions: Enables automated responses based on correlated data, such as isolating affected systems or blocking malicious activities.
    - Incident Investigation: Offers a clearer understanding of the scope and nature of a threat, aiding in faster and more effective incident response.