

Lecture 25: The Insider, *con't*; Computer Forensics

Date: November 25, 2013

Homework Due: Dec. 6 at 5:00pm

1. Human solutions: detection and prevention
 - a. Policies: languages and hierarchies
 - b. Monitoring
 - c. Forensics
2. Human solutions: predictive
 - a. Taxonomies and their uses
 - b. Attack-related symptoms and behaviors
 - c. Semantic analysis
 - d. Motivational analysis
3. Legal considerations
4. Response
5. What is computer forensics?
 - a. Definitions
 - b. Issues and uncertainties
6. Laws and Courts
7. What to examine
 - a. Disk Forensics
 - b. Host Forensics
 - c. Mobile/Embedded Device Forensics
 - d. Network Forensics