Computer and Network Forensics

Forensics Defined
Methods and techniques for gathering evidence that can be used in court

Viewpoints of Security
- Prevention
- Deterrence
- Detection
- Response
- Recovery

Before the fact

After the fact
Approaches to Security

- Policies
- Architectures
- Tools

A Comprehensive Security Program
- Prevention
- Deterrence
- Detection/monitoring
- Response
- Recovery

Tools for Attack/Intrusion Prevention
- Access Control
- Firewalls
- Cryptography
- Public Key Infrastructures
- Intrusion Detection and Response systems
Tools for Attack Response

- Access Control Systems
- Firewalls
- Intrusion Detection Systems
- Forensics tools

Policies for Deterrence

- Enhancing Forensic Capabilities

Goal of Forensics

- Gather data to:
  - Further the investigation
  - Use in court (this data is evidence)
Important Questions

- Who is the attacker?
- What actions have they taken?
- What is their objective?
- How much damage have they done?

Forensics Topics

- Forensic Preparation
- Evidence Collection
- Evidence Preservation
- Evidence Presentation

Forensic Preparation

- Surveillance
- Marking
- Mirroring
Evidence Collection

- Data Discovery
  - Logs
  - Caches
  - Tracing
  - Watermarking
- Data Recovery
- Privacy Considerations

Evidence Preservation

- Secure copying
- Tamper prevention
- Disaster recovery
- Chain of custody

Forensic Presentation

- The juror's view
- Successful prosecution: Case histories
- Using graphics to make the case
Computer and Network Forensics Positions

- CNF Technician
- CNF Professional
- CNF Policy Maker
- CNF Researcher

CNF Technician

- Technical Aspects of Gathering Evidence
  - CS-oriented (software)
  - CE-oriented (hardware)
  - Network-oriented

CNF Professional

- Multi-disciplinary Expertise of Gathering Computer Evidence
  - Complete set of technical knowledge
  - Criminology
  - Law
CNF Policy Maker

- Sees the big picture
  - Technically familiar
  - Multi-disciplinary understanding
  -Synthesizes above with business goals

CNF Researcher

- Undefined, as yet

Instruction by Position

- CNF Technician
  - Short course(s)
  - Professional certificate
  - Two year degree (AS)

- Professional
- Policy Maker
- Researcher
  - Four year degree
  - Masters
  - Doctoral
Goal and Objectives of Systems Administrators

- Get the system running
- Keep the system running efficiently and effectively
  - Optimization
  - Fault/failure prevention
- Restore the system after faults/failure

Relationship between Forensics and System Administration

- Both need past and present data about:
  - Users
  - Activity
  - Architecture

A Strategy for Establishing Policies for Enhancing Forensic Capabilities

1. Analyze Attack Strategies
2. Determine what data you will need
3. Identify the sources of that data
4. Decide what/when to monitor
5. Decide what data to keep & how long
Questions?