COMP 2555 Principles of Computer Forensics

Lecture 7

Ramki Thurimella, PhD

Overview

- Review of Lectures 5 & 6
- Exercises from Chapters 3 (Vacca)
- Material from Chapter 4 of Vacca
  - Vendor and Computer Forensics Services
- Key Points from pp. 122—142, Module 3 of CERT Book
- Project 1 discussion
- Conclusion

Exercises, Chapters 3 (Vacca)

- IDSs perform all except
  a) Monitoring and analyzing of user & system activity
  b) Deleting tightly bound services
  c) Auditing of system configs & vulnerabilities
  d) Assessing the integrity of critical system and data files
  e) Recognition of activity patterns reflecting known attacks

Exercises, Chapters 3 (Vacca)

- Attacker Motives: Internet attacks come from three basic groups, except two:
  a) For challenge
  b) High-tech vandalism without any political or social agenda
  c) For investigative purposes, to avoid incurring legal action
  d) For investigative purposes, with a need to avoid legal action
  e) Corporate competitor or political adversary

Chapter 4
Vendor & Forensics Services

- 93% of fraud from employees
  - Of which 44% by management
- Internal breaches are easy to contain
  - Easier to know the motive
  - And the attacker
- External breaches are hard
  - But easy to prove unlawful access

Cyber Detectives

- Forensic investigators
  - Detect the extent of a breach
  - Recover lost data
  - Determine why breach happened
  - Possibly, identify the culprit
- Legal issues
  - Admissibility
  - Lag time between legislation & technology
  - Archaic and nonspecific laws to fit unusual circumstances
    - For e.g., *theft* must permanently deprive the victim of property
    - How does sharing of company's data violate this?

Fight back with risk management

- Create well-communicated IT & Staff policies
  - What an individual can or cannot do
  - Diminish the risk of internal attack
  - When attack does occur, clearly defines what constitutes a breach, making it easier to prosecute
- Apply effective detection tools
  - Anomaly detection
  - Signature matching
- Ensure procedures are in place to deal with incidents
  - Make sure the right people know about it
- Have a forensic response capability
  - Create a deterrent

Deterrents

- Fundamental element of defensive strategy
- Three causal variables of general deterrence theory
  - Certainty
  - Severity
  - Celerity (Swiftness of action or motion)
- Well developed deterrents exist for military/government, not for corporations
- Infragard
- Case Study on pp. 158
- IDS limitations
  - Can log, report, isolate, and reconfigure
  - No support for evidentiary or legal

Deterrents (cont.)

- Aircraft black box analogy
- Autos records speed (?)
- Similar history of commands stored in a tamper proof way
- Cyber hot pursuit
  - Need capability to distinguish friends from foes
- Trusted insider threat

Case History

- From pp. 181

Project 1

- Discussion

Announcements

- Quiz on Wednesday
  - Material: Relevant pages from Module 3 from CERT Book
  - Chapter 4 of the textbook