COMP 2555 Principles of Computer Forensics

Lecture 5
Ramki Thurimella, PhD
Overview

- Review of Lecture 4
- Exercises from Chapters 2 & 3 (Vacca)
- Material from Chapter 3 of Vacca
  - Types of Computer Forensic Systems
- Key Points from pp. 85—102, Module 3 of CERT Book
- Project 1 posted (due next week)
- Conclusion
Exercises, Chapters 2 & 3 (Vacca)

- Review Questions pp. 77—79
- Review Questions pp. 148—149
Collecting Volatile Data

- Once shutdown, the volatile data disappears
- Most tools focus on retrieving data from persistent data
- Volatile data (that is lost when a PC is powered down)
  - Registers
  - Cache
  - RAM
- Role of a first responder
  - Determine severity
  - Collect as much information as possible about the incident
  - Document all finding
  - Share this information to get to the root cause
Order of Volatility

- Registers and Cache
- Routing table, ARP cache, process table, kernel stats, connections
- Temp files
- Hard disk, flash drives, cdrom
- Remote or off-site logging (limited storage for video monitoring for ex.)
- Physical configuration & network topology
- Archival media, e.g. tapes, disks, etc.
First responder steps

- Gain initial insight
  - Obtain RAM to look at users currently logged on, running processes, open connections etc.
- Verify whether the alert is valid or a false positive
- If a rogue process is running on a critical asset
  - Remove remotely and determine if malicious
- View the suspicious computer as completely unreliable
- Common mistakes to avoid
  - Shutting off
  - Using native commands may trigger Trojans or other malware
- You get only one chance at collecting volatile data
Methodology

- Approach for performing activities in a Coherent, consistent, accountable and repeatable manner

- Six part methodology
  1. Incident response preparation: keep first responders toolkit, a team, and forensic policies
  2. Documentation: incident profile including how detected, when, who reported, hardware/software involved, logbook containing who is performing, history of tools/commands, generated output, etc
  3. Policy verification: don’t violate user’s rights, check consent
Methodology (cont.)

4. **Collection strategy:** types of volatile information to collect, tool & techniques that facilitate, where to save output

5. **Data Collection Setup:**
   a) Establish a trusted command shell
   b) Method to transmit/store collected data
   c) Ensure integrity and admissibility (MD5)

6. **Collection Process**
   a) Collect uptime, date, time, and history
   b) Separately collect history of commands used by the first responder
   c) Collect all types of volatile system and network information
Announcements

- Project 1: A simple data carving exercise
- To see your grades on the class website, submit a four-character code and
- For emailing announcements, give your preferred email