COMP 2555 Principles of Computer Forensics

Lecture 12

Ramki Thurimella, PhD

Overview

- Midterm discussion
- Project 2 discussion
- Chapter 6 (Vacca) Evidence Collection & Data Seizure
- CERT Book, Module 4: Collecting Persistent Data 159-177

Chapter 6

- Challenges
  - Lack of permanence, in comparison to physical evidence
  - Difficult to form a cohesive argument
  - Each investigation is different
  - Expect the unexpected

Evidence Collection

- Collection process is
  - Expensive
  - Labor intensive
  - Affects availability
  - Difficult to analyze
- Why collect
  - To deter future attack
  - To predict future attacks
- Options during an attack
  - Pull the plug versus Monitor
    - + Mitigate the damage
    - + Don't become a launching pad for other attacks
    - - Might alert the attacker & might wipe out tracks
    - - Lose volatile data

Obstacles To Evidence Collection

- Recap of Forensics is So Yesterday
  - Who is the owner
    - The one who paid?
  - Who placed the evidence & Forensic ritual
    - Files make to the hard drive without user's consent
      - Cookies
      - Accidental visit to a web site
      - Spam with links to shady sites
      - Compromised computer
      - Freeware
  - Can evade – leave no trail
    - Don't write to disk
    - Tor
    - Encrypt

The 5 rules of electronic evidence

- Admissible
- Authentic
  - Evidence relates to the incident
- Complete
  - Present multiple views
    - Correlate command time line with IDS alarms
    - Separate previous attacks from current (protect the attacker from unrelated incidents)
    - Who else was logged in and why you think they didn't do it
- Reliable
  - Use sound collection methods & analysis procedures
- Believable
  - Understandable
  - Binary/log dumps are not accessible to common people

Do's and Don'ts

- Minimize handling
  - Preserve original access time and files
- Account for changes & keep detailed logs
  - Unavoidable alteration (e.g. removal of hardware)
- Follow security policy
  - Difficulties with the administration
  - admissibility
- Speed
  - Volatility
- Do not trust the compromised system,
  - Trojan commands/libraries
  - Take commands from read-only media

The 4 steps to collect & analyze

- Identify
  - Separate evidence from extraneous data
  - Be knowledgeable of where and how evidence is stored
- Preserve
  - Keep it safe so that it cannot be tampered
- Analyze (most exciting aspect of forensics—developing a theory and verifying it)
  - Extract relevant information
  - Correlate events
  - Recreate the chain of events
  - Motive
- Present
  - Be technically correct/credible
  - Easy to understand

Collecting & Logging

- Digitally sign and encrypt logs
- Store on a remote syslog server
- Attacker can synthesize fake entries into the logs
- Periodic auditing and accounting
- Monitor anomalous network activity
- Trace the attacker
- Monitor logs as they change
- Do not break laws while monitoring (e.g. do not look at packet content)
- Display a disclaimer about being watched

Collection

- Be circumspect as to who to notify and when
- Collect important data onto removable nonvolatile media
  - Be methodical (use a checklist)
  - Overcollect
  - Order of collection is important
- Take message digests
- Honeypots
- Sandboxing

Artificats

- Things left behind by the attacker
  - Code fragments
  - Trojaned programs
  - User accounts
  - Sniffer log files
  - Running processes
- Analysis of artifacts is important to analyze other attacks

Chain of custody

- Use verified duplicates
- Use isolated host machine
- Create a timeline
  - Clock drift
  - time zone & Day light saving time
  - Delayed reporting
  - Random network delays
  - 20% change in process execution based on how things are laid out
- Time stamp all forensic activity

Summary

- A lot of money is spent on
  - Hardening OSs
  - Installing firewalls
  - Monitoring network activity
  - Developing security policies and procedures
  - Rolling out security awareness programs
- This money is wasted if evidence is rendered inadmissible
- No evidence, no crime in the eyes of the law
- Common reasons for improper evidence collection
  - Poorly written policies
  - Lack of an established incident response plan
  - Lack of incident response training
  - Broken chain of custody