Preparing the IT Environment for Forensic Investigation

Paul Jackson

Agenda

- The Need
- The Design
- The Legalities
- The Issues
- The Future

The Need

- Digital forensics can be broadly divided in two areas:
  a) Incident Response (malware, intrusion, IT policy breach etc)
  b) Forensic Investigation (user behaviour and activity – normally associated with a crime/breach of internal regulations)
- Each area has a unique skillset

The Need – Incident Response

- Is IT Security alone enough?
  - Constant cycle of incident → fix/patch → restore without 'investigate'
  - Ah but….why bother?
- IR provides IT security people with a better understanding of the threats
- Responsible citizens?

The Need – Forensic Investigation

- Under what circumstances might you need this capability?
  - Data leakages?
  - Harassment?
  - Policy violations?
  - Reputation protection?
  - Criminal activity?
- Only you know your needs!

The Design

- Necessary Components:
  - Forensic Workstations
  - Evidence Storage
  - Forensic Software (X-Ways vs. FTK Vs. EnCase Vs. ‘free’)
  - Write Blockers
  - As many cables & screwdrivers etc as possible!
  - A methodology!

The Design

- Possible Components
  - Forensic Server (Forensic image storage / hashset storage / virtualisation)
  - Live network forensic connectors (proprietary vs. vendor-neutral)
  - Niche Forensic tools (ie Netanalysis, Intella, Blade, PRTK, etc)
  - Data Wiping Tools / degaussers
  - Hardware cloners
  - Network taps & sniffers
  - Chain of custody forms and secure evidence bags
  - Dongle Server (USB over Internet)
  - Portable turnout kit

The Legalities

- Do the users know that they may be subject to forensics? Reserve your right to analyse your systems
- Forensics is ‘all-seeing’ – where do you draw the line?
- Multi-user systems – how to focus just on the target alone?

The Issues

- Who does the forensics? IT Security guy?
- Where to get training/experience?
- How to assess standards?
- TRUST!! Who watches the watcher?
- Privacy & freedom Vs. Oversight
- Cost!!!!

The Future

- Cloud based Virtual Machines – single session builds:
  - Does this render forensic investigations redundant?
- E-Discovery – vast data/no time? Do we just make sense of the obvious data?
- Obligation to enhance security by understanding what went wrong (root cause analysis rather than rebuilding) – in the financial world this is now a must (regulatory requirements)

A Final Thought

- Universities are ideal locations for setting up a Forensic Incident Response Centre
- Techniques are always evolving – a blend of investigators and students in an IR team could contribute to this development
- Involve local LE – Many experienced officers would be glad to share their knowledge and experience
- Global education partnerships – 2centre.org
- Community – Great place to start is 'Forensic Focus'

Paul Jackson – paul@htcia.org.hk