Proactive & Reactive Forensics

Forensics, Antiforensics & Automation

Jess García
Security Instructor – The SANS Institute
Consultant – Jessland Enterprise Security Services

http://www.jessland.net

Agenda

- IR & Forensics
- Antiforensics
- Forensics Readiness
- Automated Forensics
What is Digital Forensics?
- Incident response
- Computer Forensic Investigations
- Forensic preparedness
- Secure Data Recovery

Incident Response

The 6-Step IR Process
- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Follow-up
The Forensics Process

- Seizure
- Preliminary Analysis
- Investigation
- Analysis

Evidence Types:
- Human Testimony
- Physical Evidence
- Network Evidence
- Host Evidence
  - Memory
  - Network Connections
  - Processes
  - Open Ports
  - Disks
  - Filesystems
  - External Devices
Real Life Problems

- Lack of training
- Poor Evidence
- Time consuming process
- Lack of logging & tracking capabilities
- Lack of containment capabilities
- Lack of appropriate Forensics environment

Antiforensics

Antiforensics is the “art” of reducing the Quantity and Quality of Forensics Data

- Perspectives
  - Unintentional
    - Quality of evidence deteriorates quickly
    - The Human Factor
      - The User
      - The Investigator
  - Malicious
Antiforensics

- Forensics' Analysts Issues
  - Short on time
  - Short on Technical Skills
  - Slave to their Tools

- Tools Issues
  - Filesystem's Restrictions and Bugs
  - Vulnerabilities

- Data Issues
  - Encryption
  - Proprietary Formats

Antiforensics

- Strategies
  - Data Destruction or Manipulation
    - Data itself
    - Meta-data
  - Data Hiding
    - Inserting Data where it does not belong
  - Data Contraception
    - In memory Execution
    - Small Footprint tools
Forensics Readiness

Forensics Readiness is the “art” of Maximizing an Environment’s Ability to Collect Credible Digital Evidence

No system or network is secure enough

Preparing IR Capabilities

- Building your IR Capabilities
  - The Lab
    - Isolated Network
    - Isolated Systems
    - Forensics Servers
    - Disk Servers
    - Short and Long Term Secure Storage
  - The Jump Bag
    - Blank Media
    - Disk Duplicators
    - Networking Gear
    - ... !!! ...
  - The Tools
    - Forensics Software Processes
Forensics Readiness
Preparing the IR Team

- The IR Team
  - Processes
    - Crime Scene Procedures
    - Chain of Custody
    - Legalities
  - Forensics Tools Training
    - Commercial Tools
    - Free Tools
    - Operating Systems & Applications
    - Hardware and Physical Devices
  - Real-Life Cases Training
    - Honeynets
    - Honeynet Project’s Softm
    - Reto Forense RedRIS / UNAM

Forensics Readiness
Preparing Systems & Networks

- Traffic Capturing Devices
  Rotation time >= Response time

- Workstations
- Servers
- External Services
- Honeynet
- ID Network
- VA / Forensics/ FW Manager
- Log Server / SEM
Preparing Systems & Networks:
- Use Turn on & Maximize logging capabilities
- Enable Remote Logging
- Enable Kernel & Filesystem Accounting
- Good Practices for Filesystems Separation
- Host-based Firewalls
- NIDS & HIDS
- Profiling
- Periodical Auditing
- Forensics-friendly Filesystems
- Analysis of the Impact of Forensics Tools

Preparing for Containment
- The Network
  - Good Practices for Network Design
  - Choke Points
- The Systems
  - Host-based Firewalls
- The People
  - Restricted Investigative Team
**The Forensics Process (Revisited)**

- Seizure
- Preliminary Analysis
- Investigation
- Analysis
- VERY Time consuming

**Forensics Response**

**What Type of IR/Forensics do you want/need?**

**What type of incidents do you expect?**

**Traditional**
- Slow
- Manual
- More accurate (if done properly)
- More Forensically Sound
- Older evidence

**Reactive**
- Faster
- Manual / Automated
- Risk of False Positives / Negatives
- Less Forensically Sound (?)
- Fresher evidence
Automated Response

1. Identify Attack
2. Trigger Automated Incident Response
3. Verify Incident
4. Trigger Automated Forensics Collection
5. Pre-analyze data
6. Trigger alert

Automated Forensics

- What is automated forensics?
  - Automate the most typical steps of the Forensics Analysis
- Perspectives:
  - Automated Forensics Tools
  - Automated Forensics Process
  - Live Forensics:
    - IDS / IPS Tool
    - Procedural Tool
  - Dead Forensics
Automated Forensics

- **Objectives:**
  - Help identify actual intrusions
  - Collect more evidence
  - Collect better evidence
  - Reduce Analysis Time
  - Forensically Sound
  - Help stop attack
  - Helps with difficult to handle scenarios:
    - Encryption
    - Strange hardware (e.g. RAID arrays)

Automated Forensics

- **The Process:**
  - Automated IR Analysis
    - Memory
    - Network Connections
    - Processes
    - Open Ports
    - Disks
    - Filesystems
    - External Devices
  - Automated Disk & Filesystem Seizure
  - Automated Memory Seizure
  - Automated Integrity/Rootkit Checks
Automated Forensics

The Process:
- Automated Profiling and Auditing
- Automated Traffic Analysis
- Automated Filesystem Analysis
  - Mactimes
  - Deleted Files Identification
  - Data Recovery
  - Artifacts Recovery
- Automated Memory Analysis
  - Processes Recovery
  - Artifacts Recovery
- Automated Artifacts Analysis

Risks & Limitations of Automated Forensics

Benefits
- Fast
  - Possibility of Early Detection
  - If nothing else, better than no response
- Earlier Evidence
- Optimizes Analysis Time
- Allows for more In-Depth Analysis

Requirements:
- Preserve Evidence
  - Avoid using local binaries and libraries: push statically compiled binaries
  - In memory execution (ftrans, userland exec)
Risks & Limitations of Automated Forensics

- Risks & Limitations
  - False Sense of Security
  - Assymetry:
    - Positive Results -> Probable break-in
    - Negative results do not mean unsuccessful break-in
  - False Positives & False Negatives
  - May not stand in Court