Web Forensics

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

http://www.jessland.net
**Agenda**

- Digital Forensics
- Evidence
- Web Forensics
- Network Forensics
- Operating System Forensics
- Client Side Forensics
- Server Side Forensics
- Demo
- Forensics Readiness
What is Digital Forensics?
- Incident response
- Computer Forensic Investigations
- Forensic preparedness
- Secure Data Recovery
Goal: Obtain Good Evidence

- Evidence
  - Human Testimony
  - Environmental
  - Network Traffic
  - Network Devices
  - Host
    - Operating Systems
    - Databases
    - Applications
  - Peripherals
  - External Storage
  - Mobile Devices
  - … ANYTHING !!!
Web Forensics

- Why Web Forensics?
  - Child Pornography
  - CC Fraud
  - Identity Theft
  - Industrial Espionage
  - Casual Hacks
  - ...

- Web Attacks:
  - Clients:
    - Perimeter Penetration
    - CC Fraud / Identity Theft
  - Web Servers:
    - Access critical information (e.g. customer databases)
    - Trojanize software
Players

- Common
  - Network Traffic
  - Operating Systems
- Client Side
  - Web Browsers
- Server Side
  - Web Servers
  - Application Servers
  - Database Servers
Network Forensics

- Phases
  - Deployment
    - May integrate with NIDS
  - Traffic Capture
  - Traffic Analysis

- Challenges:
  - Encryption (HTTPS)
  - High Traffic Load
Operating System Forensics

- Operating Systems
  - Windows, UNIX, ...

- Analysis
  - Files, Directories & Filesystems
    - Timestamps, permissions
    - Additions, changes, removals
  - Memory & Swap
  - Processes
  - Services
  - Network Connections
  - Logs
Dozens

- Lots of tools, both commercial and open source
- Open Source Favorite Suites (more UNIX-oriented)
  - Helix Bootable CD
- Commercial Favorite Suites (more Windows-oriented)
  - EnCase
  - FTK
- Check:
  http://www.jessland.net/Forensics/Software.php
Client Side Forensics

**Goals**
- Determine if a user has been involved in a crime
- Determine if a user has been victim of a crime

**How**
- Tie a person to a system at a particular point of the time

**Analysis**
- Operating System
- Web Browser
Client Side Forensics: The Web Browser

- Electronic Evidence
  - Email
  - Visited Pages
  - Internet Searches

- Web Browsers
  - Internet Explorer
  - Firefox/Mozilla/Netscape
  - Others:
    - Safari
    - Opera
    - Konqueror
    - Galeon
    - links/lynx
Web Browser Forensics:
Internet Explorer

■ Most commonly used Browser

■ Characteristics:
  - Stores user’s Internet activity under his Windows Profile
    ■ Cached Information
      - C:\Documents and Settings\john\Local Settings\Temporary Internet Files\Content.IE5\n    ■ History
      - C:\Documents and Settings\john\Local Settings\History\History.IE5\n    ■ Cookies
      - C:\Documents and Settings\john\Cookies\n    ■ File
      - Index.dat
Web Browser Forensics:

**Tools**

- **Pasco**
  - Parses IE index.dat files

- **Web Historian**
  - Allows to review user’s browsing history.

- **Cache View**
  - Allows to view user’s web cache.

- **IE History View**
  - Allows to review user’s browsing history.

- **FTK, Encase**
  - General Purpose Forensics Suites
Components:
- Web Servers
- Application Servers
- Database Servers
The Web & Application Servers
- Heavily based on log analysis
- Strategies
  - Increase verbosity of Logs
  - Log remotely
  - Log securely
- Log analysis tools for identification
- Keep your logs safe! Know your logs!

The Database Backend
- Transaction Log based.
- Challenges:
  - Database Rootkits
Other Player’s Forensics

- Other players:
  - Network Devices
  - Firewalls
  - IDSs
  - Proxies

- In the end:
  - Operating System Forensics
  - Log Analysis
  - Network Traffic Analysis
The Incident

I’VE BEEN HACKED !!!

Now What???
The Response

Seizure

Preliminary Analysis

Investigation

Analysis
A wider view: *Incident Response*

**The 6-Step IR Process**

- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Follow-up
Web Server Compromise

&

Forensics Analysis
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
Are you Ready?

No system or network is secure enough:

Plan for the Worst, Hope for the Best!!!

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

If You Have an Incident

Ask for Professional Help!!

Download this presentation:
http://www.jessland.net/Docs.php

More information:
http://www.jessland.net/KB/Forensics/

sm4rt Security Services - http://www.sm4rt.com