Forensic Network Analysis Tools

Strengths, Weaknesses, and Future Needs

Eoghan Casey
- Author, *Digital Evidence and Computer Crime*
- Editor, *Handbook of Computer Crime Investigation*
- Technical Director, *Knowledge Solutions*
- eco@corpus-delicti.com
The Basics

- Hardware and configuration
- Read-only
- Security
- Integrity
  - Existing tools do not calculate MD5
    - Do it yourself after collection
- Documenting losses
  - Existing tools to not log all losses
- Document system status & performance
- Logging examiner actions
  - Not currently => rely examiner’s notes
Hardware

- CatOS Switched Port Analyzer (SPAN)
  - Only copies valid Ethernet packets
  - Not all error information duplicated
  - Low priority of SPAN may increase losses

- Physical tap
  - Copy signals without removing layers
  - May split Tx and Rx (reassembly required)

- Platform
  - Testing but no published data
  - < 200 Mb/sec => Linux
  - > 200 Mb/sec => FreeBSD
  - Kernel customization
HW (Vendor v Homemade)

- Commercial
  - More costly but uniform expertise
  - Vendor can testify about HW & OS config
  - Vendor responsible for problems

- Homemade
  - Less expensive but variable expertise
  - You can testify about HW & OS config
  - You are responsible for problems
Read Only

- No network response
  - Including ARP replies
- No network queries
  - Use internal DNS resolution
- No downloads from Internet
  - Don’t insert content from the Web when reconstructing Web pages
Security

- Secure OS configuration
  - Patches
  - Do not overuse root/Administrator account
- Secure remote access
  - SSH
  - SSL
- Secure programming
  - Prevent buffer overflows
  - Prevent crashes (and resulting data loss)
Data Loss

**NIC:**

% /sbin/ifconfig
eth0 Link encap:Ethernet HWaddr 00:B0:D0:F3:CB:B5
inet addr:128.36.232.10 Bcast:128.36.232.255
Mask:255.255.255.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:19877480 errors:0 dropped:0 **overruns:128** frame:0
TX packets:7327676 errors:0 dropped:0 overruns:0 carrier:1
collisions:442837 txqueuelen:100
Interrupt:23 Base address:0xec80

**Kernel:**

```
# tcpdump -X host 192.168.12.5
tcpdump: listening on xl0
.....[data displayed on screen]...
^C
29451 packets received by filter
4227 packets dropped by kernel
```

- Losses at the switch
  - show inter
- Bug or misrepresentation in application

Figure from Eoghan Casey’s “Error, Uncertainty, and Loss” article in International Journal of Digital Evidence (Vol. 1, Iss. 2)
Overview of Tools

- Tcpdump (www.tcpdump.org)
  - de facto standard file format (.dmp)
- Ethereal (www.ethereal.com)
- Review (www.net.ohio-state.edu/software/)
- IRIS (www.eye.com)
- InfiniStream (www.networkassociates.com)
- NetIntercept (www.sandstorm.net)
- NetDetector (www.niksun.com)
- NFR Security (www.nfrsecurity.com)
- NetWitness (www.forensicexplorers.com)
- SilentRunner (www.silentrunner.com)
- DCS1000 w/ CoolMiner/Packeteer (FBI)
Overview of Tool Features

- **Tcpdump** (multiple platforms, free)
  - Limited examination capabilities
- **Ethereal** (multiple platforms, free)
  - Basic examination capabilities
- **IRIS** (Windows, $)
  - Basic examination capabilities
- **NetWitness** (Windows, IIS, MSSQL, $)
  - Basic examination capabilities
  - Security concerns relating to ISS and MSSQL
- **InfiniStream** (Linux collector, Win console, $)
  - Tcpdump import but not export (.cap export)
  - Good examination capabilities (Sniffer-based)
Overview of Tool Features

- **Review** (Unix, free)
  - Good examination capabilities

- **NetIntercept** (FreeBSD, $)
  - Designed with evidentiary issues in mind
  - Excellent examination capabilities
    - Feature rich but still user-friendly
    - Decrypt SSH and SSL if key are available
  - Basic analysis capabilities

- **NetDetector** (FreeBSD, $)
  - Excellent examination capabilities
  - Graphic analysis features (Xpert)
  - Integrated IDS capabilities (Snort)
Overview of Tool Features

- **NFR Security ($)**
  - Custom analysis using N-code
  - OpenBSD collector, Windows admin console, Solaris/Linux mgmt server & Oracle database

- **SilentRunner (Windows, $)**
  - Powerful visual & analysis capabilities

- **DCS1000 (Windows, available to LE)**
  - Unique filtering with law enforcement in mind (e.g., RADIUS, e-mail pen register)
  - Not clear how robust (complexity of RADIUS and capturing content in e-mail header)
Examples

Key points

- Collection: capture all content versus filtering
- Documentation: poor across the board
- Examination: recover, classify, decode, reduce, search
- Analysis: individualize, evaluate source, advanced recovery, reconstruct, visualize, present
Collection

- Tcpdump
  - 68 byte default
- Ethereal
  - 65535 bytes default snap length
- Others
  - 68 < snap length < 65535 bytes
### NetDetector: Audit Log

#### Activities Log

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>Origin IP Address</th>
<th>User Name</th>
<th>Activity Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mon Jul 14 23:01 EDT 2003</td>
<td>10.70.0.2</td>
<td>admin</td>
<td>logged in</td>
</tr>
<tr>
<td>Mon Jul 14 23:03 EDT 2003</td>
<td>10.70.0.2</td>
<td>admin</td>
<td>Added/Edited alarm 1</td>
</tr>
<tr>
<td>Tue Jul 15 12:13 EDT 2003</td>
<td>10.70.0.2</td>
<td>admin</td>
<td>Reconstructed data at 08/19/2003 2:10 AM</td>
</tr>
<tr>
<td>Tue Jul 15 21:56 EDT 2003</td>
<td>10.70.0.2</td>
<td>admin</td>
<td>Added/Edited alarm 2</td>
</tr>
<tr>
<td>Tue Jul 15 02:02 EDT 2003</td>
<td>10.70.0.2</td>
<td>admin</td>
<td>Added/Edited alarm 3</td>
</tr>
<tr>
<td>Tue Jul 15 16:55 EDT 2003</td>
<td>10.70.0.2</td>
<td>admin</td>
<td>Logged out</td>
</tr>
<tr>
<td>Tue Jul 15 20:35 EDT 2003</td>
<td>10.70.0.2</td>
<td>admin</td>
<td>Logged in</td>
</tr>
<tr>
<td>Tue Jul 15 10:00 EDT 2003</td>
<td>10.70.0.2</td>
<td>admin</td>
<td>Log in</td>
</tr>
<tr>
<td>Tue Jul 15 10:05 EDT 2003</td>
<td>10.70.0.2</td>
<td>admin</td>
<td>Log in</td>
</tr>
<tr>
<td>Tue Jul 15 21:00 EDT 2003</td>
<td>10.70.0.2</td>
<td>admin</td>
<td>Log in</td>
</tr>
<tr>
<td>Tue Jul 15 21:40 EDT 2003</td>
<td>10.70.0.2</td>
<td>admin</td>
<td>Data Imported from alera.mj.nlausum.com in voip001pm-JB-1-and</td>
</tr>
<tr>
<td>Tue Jul 15 10:10 EDT 2003</td>
<td>10.70.0.2</td>
<td>admin</td>
<td>Data Imported from alera.mj.nlausum.com in voip001pm-JB-1-and</td>
</tr>
<tr>
<td>Tue Jul 15 10:40 EDT 2003</td>
<td>10.70.0.2</td>
<td>admin</td>
<td>Data Imported from alera.mj.nlausum.com in voip001pm-JB-1-and</td>
</tr>
<tr>
<td>Tue Jul 15 10:39 EDT 2003</td>
<td>10.70.0.103</td>
<td>admin</td>
<td>Data Imported from alera.mj.nlausum.com in voip001pm-JB-1-and</td>
</tr>
</tbody>
</table>
External MD5 Calculations

```
bash-2.04$ cd /usr/local/mercury/tmp
bash-2.04$ ls
export_data_stream
bash-2.04$ md5 export_data_stream > export_data_stream.md5
bash-2.04$ scp export_data_stream@vcr@18.0.0.20:/tmp
```

username@example.com
SNMP Recipient (host or ip)
Filtering During Collection

- BPF/Ethereal filtering syntax
  - IP address, port, etc.
- MAC address
- Custom NFR Security filters (using N-code)
- DCS1000
  - RADIUS
  - DHCP
- Filtering on protocol is risky
  - Pen register for e-mail (DCS1000)
  - If necessary, be very careful
  - Ideally use a specialized tool for this purpose
Examination: Protocol Decode

- Tcpdump has limited decode capabilities
- Ethereal
  - More decodes but assumes default behavior
  - “Decode As” feature
- InfiniStream/Sniffer
  - Several decodes including some VoIP
- NetDetector
  - Understands protocols including some VoIP
- NetIntercept
  - Understands protocols including some VoIP
  - More powerful stream reconstruction
  - Flags anomalies (like file sig mismatch)
  - Flags missing SEQ #’s in TCP session
Review: X Session Decode

Server

Client
Review: X Session Replay

- Step-by-step session replay
- Pauses before redrawing screen

Figure from Steve Romig's "Incident Response Tools" chapter in Handbook of Computer Crime Investigation
Examination: Data Reduction

- GUI versus command syntax
- Review: session summary & browsing
- NetIntercept: Forensics tab
Examination: Data Reduction

- SilentRunner: 3-D Visualization
- NFR Security: Query interface
Examination: Visualization

- Traffic charts
- Top Talkers
- Top Pairs
Examination: Visualization

- SilentRunner
  - 3-D display of traffic helps focus on interesting activities
- General purpose visualization tools
  - Clustering and other techniques for visually representing data to help examiners identify useful items in large datasets
Search and Recovery

- **Ethereal**
  - Miss keyword split between two packets
  - Export Web page & view in browser (bad)
  - File extraction requires expertise & tools

- **NetIntercept**
  - Performs search on reconstructed data
  - Sandbox for viewing Web pages
  - Does not execute code in Web pages
  - Automated file extraction

- **NetDetector**
  - GUI & regular expression on command line
  - Sandbox for viewing Web pages

- **NFR Security database query customization**

- **SilentRunner N-gram Analysis**
NetIntercept: Search
NetDetector: Search (GUI)
NetIntercept: Image Extraction
Ethereal: Web Page
NetIntercept: Web Page
NetIntercept: Search/Recover

Figure from Eoghan Casey’s “Digital Evidence and Computer Crime”, 2nd edition
Analysis

- Temporal views
  - Timelines
  - Histograms/charts
- Relational analysis
  - Thicker lines for higher traffic
  - N-gram analysis
- SilentRunner
  - 3-D visualization can be useful for analysis
  - Develop baseline of network activities for comparison
  - Visually represents anomalies and other noteworthy events
Analysis: NetIntercept
Analysis: NetDetector (Snort)

NetDetector Network Intrusion Recorder and Analyzer - Microsoft Internet Explorer provided by NIKSUN, Inc.

Configuration

Recorder
Interfaces
Alarms
Anomaly
Snort
User Management
Local User Accounts
External Server
Management Interface
Network Parameters
Firewall
Network Services
Logs & Jobs
Activities Log
Export Log
Job Queue

Alarms - Signature Configuration (Snort)

Snort Parameters

Status: Running

Options

Enable
Disable

Minimal Priority

Log All Snort Priorities

Monitoring Interface

niksun.com/msn_steve_tail

Monitoring interval

Continuous (Constant Monitoring starting from "now")

Last 1 Hour(s) (will be converted to absolute below)

Start/Stop

DEC 16 1.00PM 2002

Optional Log to Syslog Server

(syslog server name)

Optional Filter

View/Manage the current Snort signatures.
Visualization & Data mining

- Visualization techniques
  - Clustering and other techniques for visually representing data to help examiners identify noteworthy patterns and items in large datasets

- Data mining
  - Finding patterns, associations, links
  - Recognizing patterns of behavior
Reporting

- Bookmarks
- Default reports
  - Inventory hosts, accounts, nicknames, files, etc.
  - Top talkers
- Alerts

Figure from Steve Romig's "Incident Response Tools" chapter in Handbook of Computer Crime Investigation
### Web Pages

<table>
<thead>
<tr>
<th>Connection Size</th>
<th>File Name</th>
<th>Host</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>/cgi-bin/linkdirector/signup?_lang=EN</td>
<td>help.msn.com</td>
</tr>
<tr>
<td>31</td>
<td>/en_us/frameset.asp?Topic=REGTy20Passport BrandID= Filter= H_VE</td>
<td></td>
</tr>
<tr>
<td>31</td>
<td>/en_us/helpwindow.asp?Topic=REG20Passport BrandID= Filter= H_VE</td>
<td></td>
</tr>
<tr>
<td>31</td>
<td>/en_ush_fbar.asp?UNIP=25.ini_html HITSFile=ppv25.its51 H_VER=1.5b1</td>
<td></td>
</tr>
<tr>
<td>32</td>
<td>/datase/enspdata/ppv25.its51%conten H_APP=Microsoft+%2ENET+Pass xml=xml=</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>/cgi-bin/login</td>
<td>loginnet.passport.com</td>
</tr>
<tr>
<td>184</td>
<td>/logoat.srf?_lang=EN lc=1033 id=2 r</td>
<td></td>
</tr>
</tbody>
</table>

### Alerts

<table>
<thead>
<tr>
<th>Message: Connection close not captured</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection ID</td>
</tr>
<tr>
<td>---------------</td>
</tr>
<tr>
<td>199</td>
</tr>
<tr>
<td>202</td>
</tr>
<tr>
<td>203</td>
</tr>
<tr>
<td>204</td>
</tr>
<tr>
<td>116</td>
</tr>
<tr>
<td>201</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Message: Media type 'image/gif' requested by GIF, but it didn't match and PlainTxt did</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection ID</td>
</tr>
<tr>
<td>---------------</td>
</tr>
<tr>
<td>141</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Message: Media type 'text/html' requested by HTML, but it didn't match and ASCII Type did</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection ID</td>
</tr>
<tr>
<td>---------------</td>
</tr>
<tr>
<td>187</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Message: Media type 'text/html' requested by HTML, but it didn't match and PlainTxt did</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection ID</td>
</tr>
<tr>
<td>---------------</td>
</tr>
<tr>
<td>190</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Message: Reset out of window</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection ID</td>
</tr>
<tr>
<td>---------------</td>
</tr>
<tr>
<td>14</td>
</tr>
<tr>
<td>35</td>
</tr>
<tr>
<td>193</td>
</tr>
<tr>
<td>195</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Message: Window ignored</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection ID</td>
</tr>
<tr>
<td>---------------</td>
</tr>
<tr>
<td>14</td>
</tr>
<tr>
<td>35</td>
</tr>
</tbody>
</table>
Comparison Summary

- **NetIntercept & NetDetector**
  - Best starting point for examination
  - Useful for most common analysis needs

- **NFR Security**
  - Advanced evidence processing using N-Code, GUI Queries & Perl Query Add-on

- **SilentRunner**
  - 3-D visualization useful in some cases

- **DCS1000**
  - Good effort to filter during collection (e.g., pen register, RADIUS, DHCP)
Summary of Future Needs

- Platform standards to minimize losses
  - Published performance testing
  - Consider security and stability
- Read-only
  - No network responses or queries during collection or examination
- Integrity
  - Not necessarily during collection (after)
- Validate security and data interpretation of tools
- Documentation
  - System status & performance (proper operation)
  - Record primary sources of losses
  - Audit trail of examiner actions
Future Needs (cont.)

- Support tcpdump format import and export
  - Collect using one tool, examine w/ other

- Filtering capabilities during collection
  - DHCP & RADIUS
  - May be safer to use specialize tool for protocol filtering & pen register needs

- Filtering during examination
  - Exclude known files (e.g., logo, safe content)
  - Flag suspicious files (e.g., encrypted files or intellectual property/hacker tools using MD5)
  - Drill down on top host/protocols (e.g., ntop.org)
  - More visualization of data to help filtering
Future Needs (cont.)

- Protocol identification and decode
  - Based on protocol v. variables chars
  - Flag protocol violations, missing SEQ #s
  - More decodes and step-by-step replay

- Text search capabilities
  - Keywords split between multiple packets
  - Grep syntax

- More file extraction capabilities
  - KaZaA fragments from multiple sources

- More analysis capabilities
  - Behavior pattern recognition
  - System profile violations