CSI Maui: Forensics in the Case of the Attacked Browser
Share Session Orlando Session 9273

Laura Knapp
WW Business Consultant
Laurak@aesclever.com
Background

Incident Evaluation

Trace Evaluation
What is Computer Forensics

• Computer forensics involves the preservation, identification, extraction, documentation, and interpretation of computer media for evidentiary and/or root cause analysis.

• Network or TCP/IP forensics involves the preservation, extraction, documentation and interpretation of TCP/IP data for evidentiary and/or root cause analysis.

• Doesn’t prevent computer crime.

• After the fact investigation.

• Forensics experts follow clear, well-defined mythologies and procedures.
What is Network Forensics

- Network forensics entails monitoring network traffic and determining if there is an attack and if so, determine the nature of the attack.
- Key tasks include traffic capture, analysis and visualization.
- Network forensics systems can be one of two kinds:
  - "Catch-it-as-you-can" systems, in which all packets passing through a certain traffic point are captured and written to storage with analysis being done subsequently in batch mode.
  - "Stop, look and listen" systems, in which each packet is analyzed in a rudimentary way in memory and only certain information saved for future analysis.
Employee Trust

• Construction Company

• Senior IT person also in charge of security
• Used cost issue to convince upper management to let him store data at his home rather than pay for external off-site storage
• Conflict arose between the Employee and Employer
• Employee sent email’s to clients of the construction company indicating he had personal information
• Took 6 months to shut down the rogue employee after the employee used the internet to threatened people at which time the FBI became involved
• Construction company was fundamentally out of business

http://www.cio.com/article/454614/IT_Security_Pros_Share_Horror_Stories
Process Vulnerability

• Security administrator asked to shut off web security monitoring system as it was interfering with marketing’s ability to access the corporate web site for creation and editing.
• Director said ‘switch off’ not….. find a work around….find a fix….just ‘switch it off’
• Users quickly found that out that all web controls were no longer active
• A report surfaced that a user had used a desktop to access porn
• Due to the use of generic accounts tracking activity to a user was not possible
• Took 3 months, CCTV, internal and external police to finally catch the culprit
• To make matters worse the company dropped any further work on a security framework and made the security positions obsolete
• RSA conference 2007
• Over half the computers lacked proper protection
  • Many configured to automatically log on to WiFi networks like ‘Linksys’ ‘T-Mobile’
• Five rogue networks mimicked common hotspot names
  • These could easily insert man in the middle routines and capture data
• The RSA conference had a SAFE WIFI network but it was toooooo complex to use and the help desk line was long and slow
SPOOFCARD
THE NEXT GENERATION OF PHONE SPOOFING

SPOOFCARD calling cards offers you the ability to change what someone sees on their caller ID display when they receive a phone call.

Key Benefits: Make calls truly private, Ability to record calls, Change your voice, Fun and inexpensive, Easy to use and fast to set up! Instant Access!

SPOOFCARD FEATURES:

- Caller ID Spoofing
- Voice Changer
- Call Recording
- Web Control Panel

No computer needed: Simply dial the toll free number from the calling card you purchase.

1. Enter your pin number.
2. Enter Destination number.
3. Enter Any Caller ID Number you wish to display.
4. Choose the voice you would like to use.
5. Your call is connected using the specified Caller ID Number.

Control Panel Login

BUY INSTANT CALLING MINUTES
ADD MONEY TO EXISTING CARD
FREQUENTLY ASKED QUESTIONS
INTERNATIONAL RATES
CUSTOMER SERVICE
PRIVACY POLICY

Purchase $10 Calling Card

© Applied Expert Systems, Inc. 2010
2009 Litigation Highlights

**Starwood v. Hilton (2009)** - Complaint alleging that 2 former Starwood execs looted >100k Starwood computer files.

**U.S. v. Chung (2009)** – Boeing employee convicted at trial for passing trade secrets to Chinese government for 30 years. Co-defendant convicted and jailed for 24 years; Chung, 74 years old, received 15 years in prison.


**US v. Lee (2009)** – Former technical director of paint and coating company quit 2 weeks after return from business trip to China; discovered downloaded trade secrets, deleted files, one way ticket from Chicago to Shanghai.

The Impact of a Digital Crime

• Disruption to organizational routines and processes
• Direct financial losses through information theft and fraud
• Decrease in shareholder value
• Loss of privacy
• Reputational damage causing brand devaluation
• Loss of confidence in IT
• Expenditure on information security assets and data damaged, stolen, corrupted or lost in incidents
• Loss of competitive advantage
• Reduced profitability
• Impaired growth due to inflexible infrastructure/system/application environments
• Injury or loss of life if safety-critical systems fail

• Theft of trade secrets exceeded $1 trillion in 2008 and continues to escalate
• Over 40% of U.S. businesses have reported intellectual property losses in 2008
Background

Incident Evaluation

Trace Evaluation
Incident Reporting

Law Enforcement report?
Regulatory agency report?
Insurance claim?
Disciplinary action?
Dismissal action?
Vendor report?
Update disaster recovery plan?
Update software to new versions?
Update employee training?
Public Affairs report?
CEO report to employees?
Business Service Management for Performance

Incident Response Process

- Define Roles
- Establish Policies
- Identify Tools
- Network Preparation

Complete IR Checklist
- Who/What/Where/When
- Incident Description
- Hardware/Software
- Personnel Involved
- Network

Incident Preparation

Incident Detection

Activate IR Team

Initial Response

Completed IR Checklist.

Is it really an Incident?

- Firewall Logs
- IDS Logs
- Suspicious User
- System Administrator

- Verify Incident
- Affected Systems
- Users Involved
- Business Impact
Incident Response Process Response

Response Strategy

Management Approval
- Dollar Loss
  - Downtime
  - Legal Liability
  - Publicity
  - Intellectual Property

Accumulate Evidence & Secure System

- Best Evidence Rule
- Chain of custody
- Data Volatility

- System Criticality
- Information Sensitivity
- Perpetrators
- Publicity
- Skill of Attacker
- System Downtime
- Dollar Loss

Forensic Duplication
Incident Response Process Improvements

- New Procedures
- Reinstall files
- Reinstall from CD-Rom
- Secure System
  - Turn off unneeded services
  - Apply patches
- Strong Passwords
- Strong Administration

Recovery

- Document everything as it occurs

Documentation

- Support both criminal and civil prosecution
  - Produce the final report
  - Process improvement
Background

Incident Evaluation

Trace Evaluation
Elements of Digital Forensics

- Business Applications
- Application Servers
- Database/Data Privacy
- HW Platform, OS, Storage
- LAN/WAN Network Access
- Facility/Infrastructure

- Applications Management Services (Remote/Smart Center)
- Managed Hosting Services
- Managed Network Services
- Colocation Services
- Managed Security Services
- Identity Services
- Application Security Services
- Data Privacy services

IT Services
 Risk/Compliance
 Security
Network Forensics Elements

Security has to be applied within a business context and fused into the fabric of the business.

- Crime is committed
- Secure the scene and/or network components involved
- Acquire details without changing or altering
- Authenticate that details have not been altered
- Analyze the details without alteration
- Gather detailed environmental background information
- Governance (Organization)
Forensic Tools

• IDS (Intrusion Detection System) attempts to detect activity that violates an organization’s security policy
• Firewall allows or disallows traffic to or from specific networks, machine addresses and port numbers
• Network Forensic Analysis Tools (NFAT) synergizes with IDSs and Firewalls.
  • Preserves long term record of network traffic
  • Allows quick analysis of trouble spots identified by IDSs and Firewalls
    • NFATs must do the following:
      • Capture network traffic
      • Analyze network traffic according to user needs
      • Allow system users discover useful and interesting things about the analyzed traffic
### NFAT Tasks

- **Traffic Capture**
  - What is the policy?
  - What is the traffic of interest?
  - Internal/External?
  - Collect packets
- **Traffic Analysis**
- **Organize traffic by session**
- **Protocol Parsing and analysis**
  - Check for strings, use expert systems for analysis
- **Interacting with NFAT**
  - Appropriate user interfaces, reports, examine large quantities of information and make it manageable

---

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>TCP</td>
<td>192.168.1.100</td>
<td>192.168.1.101</td>
<td>TCP</td>
<td>12345</td>
<td>67890</td>
<td>123456789</td>
<td>123456789</td>
<td>TCP</td>
<td>192.168.1.100</td>
<td>192.168.1.101</td>
<td>TCP</td>
<td>12345</td>
<td>67890</td>
<td>123456789</td>
<td>123456789</td>
</tr>
<tr>
<td>2</td>
<td>UDP</td>
<td>192.168.1.102</td>
<td>192.168.1.103</td>
<td>UDP</td>
<td>23456</td>
<td>67890</td>
<td>123456789</td>
<td>123456789</td>
<td>UDP</td>
<td>192.168.1.102</td>
<td>192.168.1.103</td>
<td>UDP</td>
<td>23456</td>
<td>67890</td>
<td>123456789</td>
<td>123456789</td>
</tr>
<tr>
<td>4</td>
<td>HTTP</td>
<td>192.168.1.106</td>
<td>192.168.1.107</td>
<td>HTTP</td>
<td>80</td>
<td>80</td>
<td>123456789</td>
<td>123456789</td>
<td>HTTP</td>
<td>192.168.1.106</td>
<td>192.168.1.107</td>
<td>HTTP</td>
<td>80</td>
<td>80</td>
<td>123456789</td>
<td>123456789</td>
</tr>
</tbody>
</table>

---

PCAP Attack Situation*

A malware attack is suspected and you need to identify the malicious web pages.

* Excerpts from the HONEYPOT PROJECT 2010 Forensic Challenge
What Can You Learn from the Trace?

- List the protocols found in the capture. What protocol do you think the attack is based on?
- List IPs, host names/domain names. What can you discern based on this information? Do you think it is a real situation?
- List all the visited web pages? Which ones might contain malicious javascript and who is connecting to them? Describe the nature of the malicious web pages.
- What are the overall actions performed by the attacker?
- What steps slow the analysis down?
- What Operating Systems, software, and vulnerabilities were involved?
What Can You Learn from the Trace?

List the protocols found in the capture. What protocol do you think the attack is based on?  

Tools used: CleverView for cTrace Analysis

- ARP
- DNS
- DHCP
- HTTP
- NetBIOS

Use Query Builder function to view protocols in trace.
How to Determine Protocols Running in Trace?

Query Builder allows viewing only specific common protocols/applications or ports.
What Can You Learn from this Trace? ARP

<table>
<thead>
<tr>
<th>ID</th>
<th>Timestamp</th>
<th>Datagram Size</th>
<th>Local IP</th>
<th>Rmt. IP</th>
<th>Protocol</th>
<th>Messages</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>14:00:29:6694</td>
<td>60</td>
<td>10.0.2.15</td>
<td>10.0.2.15</td>
<td>ARP</td>
<td>ARP Request from 10.0.2.15: Who Has 10.0.2.15</td>
</tr>
<tr>
<td>6</td>
<td>14:00:29:9753</td>
<td>60</td>
<td>10.0.2.15</td>
<td>10.0.2.15</td>
<td>ARP</td>
<td>ARP Request from 10.0.2.15: Who Has 10.0.2.15</td>
</tr>
<tr>
<td>7</td>
<td>14:00:30:9711</td>
<td>60</td>
<td>10.0.2.15</td>
<td>10.0.2.15</td>
<td>ARP</td>
<td>ARP Request from 10.0.2.15: Who Has 10.0.2.15</td>
</tr>
<tr>
<td>20</td>
<td>14:00:37:9882</td>
<td>60</td>
<td>10.0.2.15</td>
<td>10.0.2.2</td>
<td>ARP</td>
<td>ARP Request from 10.0.2.15: Who Has 10.0.2.2</td>
</tr>
<tr>
<td>21</td>
<td>14:00:37:9883</td>
<td>60</td>
<td>10.0.2.2</td>
<td>10.0.2.15</td>
<td>ARP</td>
<td>ARP Reply from 10.0.2.15: Answering 10.0.2.2</td>
</tr>
<tr>
<td>106</td>
<td>14:00:59:6378</td>
<td>60</td>
<td>10.0.3.15</td>
<td>10.0.3.15</td>
<td>ARP</td>
<td>ARP Request from 10.0.3.15: Who Has 10.0.3.15</td>
</tr>
<tr>
<td>107</td>
<td>14:01:00:1585</td>
<td>60</td>
<td>10.0.3.15</td>
<td>10.0.3.15</td>
<td>ARP</td>
<td>ARP Request from 10.0.3.15: Who Has 10.0.3.15</td>
</tr>
<tr>
<td>108</td>
<td>14:01:01:1602</td>
<td>60</td>
<td>10.0.3.15</td>
<td>10.0.3.15</td>
<td>ARP</td>
<td>ARP Request from 10.0.3.15: Who Has 10.0.3.15</td>
</tr>
<tr>
<td>123</td>
<td>14:01:08:5411</td>
<td>60</td>
<td>10.0.3.15</td>
<td>10.0.3.2</td>
<td>ARP</td>
<td>ARP Request from 10.0.3.15: Answering 10.0.3.2</td>
</tr>
<tr>
<td>124</td>
<td>14:01:08:5416</td>
<td>60</td>
<td>10.0.3.2</td>
<td>10.0.3.15</td>
<td>ARP</td>
<td>ARP Request from 10.0.3.15: Answering 10.0.3.2</td>
</tr>
<tr>
<td>380</td>
<td>14:01:54:7888</td>
<td>60</td>
<td>10.0.4.15</td>
<td>10.0.4.15</td>
<td>ARP</td>
<td>ARP Request from 10.0.4.15: Who Has 10.0.4.15</td>
</tr>
<tr>
<td>381</td>
<td>14:01:55:4530</td>
<td>60</td>
<td>10.0.4.15</td>
<td>10.0.4.15</td>
<td>ARP</td>
<td>ARP Request from 10.0.4.15: Who Has 10.0.4.15</td>
</tr>
<tr>
<td>382</td>
<td>14:01:56:4552</td>
<td>60</td>
<td>10.0.4.15</td>
<td>10.0.4.15</td>
<td>ARP</td>
<td>ARP Request from 10.0.4.15: Who Has 10.0.4.15</td>
</tr>
<tr>
<td>403</td>
<td>14:02:06:5130</td>
<td>60</td>
<td>10.0.4.15</td>
<td>10.0.4.2</td>
<td>ARP</td>
<td>ARP Request from 10.0.4.15: Who Has 10.0.4.2</td>
</tr>
<tr>
<td>404</td>
<td>14:02:06:9131</td>
<td>60</td>
<td>10.0.4.2</td>
<td>10.0.4.15</td>
<td>ARP</td>
<td>ARP Reply from 10.0.4.15: Answering 10.0.4.2</td>
</tr>
<tr>
<td>702</td>
<td>14:03:59:9930</td>
<td>60</td>
<td>10.0.5.15</td>
<td>10.0.5.15</td>
<td>ARP</td>
<td>ARP Request from 10.0.5.15: Who Has 10.0.5.15</td>
</tr>
<tr>
<td>703</td>
<td>14:04:00:0869</td>
<td>60</td>
<td>10.0.5.15</td>
<td>10.0.5.15</td>
<td>ARP</td>
<td>ARP Request from 10.0.5.15: Who Has 10.0.5.15</td>
</tr>
<tr>
<td>704</td>
<td>14:04:01:0888</td>
<td>60</td>
<td>10.0.5.15</td>
<td>10.0.5.15</td>
<td>ARP</td>
<td>ARP Request from 10.0.5.15: Who Has 10.0.5.15</td>
</tr>
<tr>
<td>712</td>
<td>14:04:04:1816</td>
<td>60</td>
<td>10.0.5.15</td>
<td>10.0.5.2</td>
<td>ARP</td>
<td>ARP Request from 10.0.5.15: Who Has 10.0.5.2</td>
</tr>
<tr>
<td>713</td>
<td>14:04:04:1817</td>
<td>60</td>
<td>10.0.5.2</td>
<td>10.0.5.15</td>
<td>ARP</td>
<td>ARP Reply from 10.0.5.15: Answering 10.0.5.2</td>
</tr>
</tbody>
</table>

ARP was used once per client computer
DHCP was used once per client computer
DNS was used to resolve WEB Server Names
What Can You Learn from this Trace? ICMP

ICMP reported Transit TTL exceptions
What Can You Learn from this Trace? NetBios

NetBios Uses ports 137, 138, 139

NetBios announcement queries being sent from the clients but no responses.....
What Can You Learn from this Trace? HTTP

HTTP represents the majority of traffic in the trace.
List Key IP Addresses in this Trace - 192.168.56.52

Tools used: CleverView for cTrace Analysis, WHOIS

Clients:
10.0.2.15, 10.0.3.15, 10.0.4.15, 10.0.5.15…all use 8fd12edd2dc1462

Attacker:
192.168.56.52 (hostname: sploitme.com.cn)

Services:
10.0.2.2, 10.0.3.2, 10.0.4.2, 10.0.5.2 (DHCP servers and gateways)
192.168.1.1 (DNS)

Simulated hacked hosts:
192.168.56.51 (hostname: shop.honeynet.sg)
192.168.56.50 (hostname: rapidshare.com.eyu32.ru)

External hosts:

The clients are most likely VMs, as each has its own subnet, but they share an ethernet adapter, a DNS server (single MAC address, multiple IPs per subnet) and a DHCP server (on a different subnet).

Attacker and hacked hosts reside in the same private subnet. (Not a real-world scenario.)

Hacked Site #1 is probably a ripoff of the well-known rapidshare.com. Hacked Site #2 is an e-commerce site, either innocent (but exploited to serve malicious JS) or malevolent.
List Key IP Addresses in this Trace – Devil in the Details

- Host Details
- MAC Address
List the WEB Sites involved and the Malicious Sites?

*Tools Used: CleverView for cTrace Analysis: Microsoft Security Bulletins*

<table>
<thead>
<tr>
<th>URL</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connected to by 10.0.2.15 and 10.0.3.15</td>
<td></td>
</tr>
<tr>
<td>Connected to by 10.0.2.15 and 10.0.3.15</td>
<td></td>
</tr>
<tr>
<td><a href="http://sploitme.com.cn/fg/show.php?s=3feb5a6b2f">http://sploitme.com.cn/fg/show.php?s=3feb5a6b2f</a></td>
<td>Contains a 404-disguising page with an encrypted javascript, also easily decoded by replacing eval() with alert(). The javascript doesn't contain any malicious behaviour, perhaps because the exploit pack doesn't contain an exploit for sent User-Agent (Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.3) Gecko/20090824 Firefox/3.5.3), which corresponds to Firefox v3.5.3</td>
</tr>
<tr>
<td>Connected to by 10.0.2.15 with User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.3) Gecko/20090824 Firefox/3.5.3</td>
<td></td>
</tr>
</tbody>
</table>

**List the WEB Sites involved and the Malicious Sites?**

*Tools Used: CleverView for cTrace Analysis: Microsoft Security Bulletins*

<table>
<thead>
<tr>
<th>URL</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://sploitme.com.cn/fg/show.php?s=3feb5a6b2f">http://sploitme.com.cn/fg/show.php?s=3feb5a6b2f</a></td>
<td>The decoded javascript contains an MDAC exploit (MS06-014) which has its effect (download&amp;execute a binary) on the browser. The version of the browser is Internet Explorer v6 accordingly to the User-Agent</td>
</tr>
<tr>
<td><a href="http://www.honeynet.org/">http://www.honeynet.org/</a></td>
<td>Contains no malicious content</td>
</tr>
<tr>
<td><a href="http://www.google.fr/">http://www.google.fr/</a></td>
<td>Although it contains a cryptic javascript, it's no malicious</td>
</tr>
<tr>
<td><a href="http://sploitme.com.cn/fg/show.php?s=3feb5a6b2f">http://sploitme.com.cn/fg/show.php?s=3feb5a6b2f</a></td>
<td>The 404-alike page now doesn't contain any javascript, probably because of an IP ban given by the exploit pack to prevent multiple infections of the same victim</td>
</tr>
</tbody>
</table>

First request by 10.0.3.15 with User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)

Second request by 10.0.3.15
List the WEB Sites involved and the Malicious Sites?

*Tools Used: CleverView for cTrace Analysis: Microsoft Security Bulletins*

<table>
<thead>
<tr>
<th>URL</th>
<th>Description</th>
</tr>
</thead>
</table>
| **http://shop.honeynet.sg/catalog/**     | Contains a differently encrypted and inserted iframe to http://sploitme.com.cn/?click=84c090bd86
| Requested by 10.0.4.15                   | Decryption: replace `document.write()` with `alert()`                                            |
| Requested by 10.0.4.15                   |                                                                                                 |
| **http://sploitme.com.cn/fg/show.php?s=84c090bd86** | Malicious javascript contains following exploits:                                              |
| Requested by 10.0.4.15                   | 1. MDAC exploit (MS06-014)                                                                       |
| User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) | 2. IWinAmpActiveX exploit (I think it’s not gonna work because of an incorrect “classid”)       |
|                                           | 3. DirectShow exploit (MS09-032)                                                                 |
|                                           | 4. MS Access Snapshot Viewer exploit (MS08-041)                                                 |
|                                           | 5. Msdds.dll COM exploit (MS05-052)                                                             |
|                                           | 6. Office Web Components exploit (MS09-043)                                                     |
|                                           | The exploits are being executed in a chain, one after another. All exploits are targeted to perform a download&exec of the same binary. |
| **http://sploitme.com.cn/fg/show.php**   | The page doesn’t contain malicious content for the same reason as                                |
| Requested by 10.0.5.15                   | http://sploitme.com.cn/fg/show.php?s=3feb5a6b2f by 10.0.2.15                                   |
| User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.6) Gecko/20040614 Firefox/0.8 | or because no ‘s’ variable is specified                                                        |
How did I get the Detailed Information on Web Sites?

Used ‘Sequence of Execution’ to see the communication between the involved sites, then looked at the packet details.

Shows Login to rapidshare.com/ey u32.ru
What are the Overall Actions Performed by the Hacker?

1. Hacked sites are initialized with javascript code that adds a hidden iframe pointing to sploitme.com/cn?click=x using SQL injections or XSS techniques.
2. A client surfs to a hacked site and his browser requests sploitme.com.cn/?click=x which is redirected to sploitme.com.cn/fg/show.php?s=X.
3. A 404 page is displayed which is intended to confuse the client.
4. The browser executes the javascript which goes through a series of exploits to see if one is successful. (DirectShow is an example)
5. If an exploit is successful it executes a file at sploitme.com.cn/fg/load.php?e=X.
6. Some of the items performed by this malware:
   1. Client computer is a BOT for sending spa,
What Steps Slow Down the Analysis Process?

Iframe’s are difficult for human’s to understand

Malicious page is disguised to look like a 404 page

Javascript is coded using a polymorphic javascript

The sent exploit set depends on what browser the victim is using

Victim’s IP address is ‘banned’ by the exploit pack. In packet 366 the victim tries to access the show.php file again but gets a ‘clean’ 404 page
What Operating Systems, software, and Vulnerabilities were involved?

<table>
<thead>
<tr>
<th>Exploit</th>
<th>Vulnerable Component</th>
<th>Published</th>
<th>Reference</th>
<th>Remedy</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>MDAC RDS.Dataspace ActiveX control</td>
<td>Apr 2006</td>
<td>CVE-2006-0003</td>
<td>MSB-MS06-014</td>
</tr>
<tr>
<td>II</td>
<td>AOL IWinAmpActiveX control (AmpX.dll)</td>
<td>May 2009</td>
<td>OSVDB-54706</td>
<td>(none)</td>
</tr>
<tr>
<td>III</td>
<td>DirectShow ActiveX control (msvidctl.dll)</td>
<td>Jul 2009</td>
<td>CVE-2008-0015</td>
<td>MSB-MS09-032</td>
</tr>
<tr>
<td>IV</td>
<td>Office Snapshot Viewer ActiveX control</td>
<td>Jul 2008</td>
<td>CVE-2008-2463</td>
<td>MSB-MS08-041</td>
</tr>
<tr>
<td>V</td>
<td>COM Object Instantiation (msdds.dll)</td>
<td>Aug 2005</td>
<td>CVE-2005-2127</td>
<td>MSB-MS05-052</td>
</tr>
<tr>
<td>VI</td>
<td>Office Web Components ActiveX control</td>
<td>Jul 2009</td>
<td>CVE-2009-1136</td>
<td>MSB-MS09-043</td>
</tr>
</tbody>
</table>
Summary

- Forensic science is application of science to questions of interest to the legal profession.
- Several unique opportunities give computer forensics the ability to uncover evidence that would be extremely difficult to find using a manual process.
- Computer forensics also has a unique set of challenges that are not found in standard evidence gathering, including volume of electronic evidence, how it is scattered in numerous locations, and its dynamic content.
- Searching for digital evidence includes looking at “obvious” files and e-mail messages.
- Need for information security workers will continue to grow, especially in computer forensics.
- Skills needed in these areas include knowledge of TCP/IP, packets, firewalls, routers, IDS, and penetration testing.
AES Sessions at Share

Aug 8, 2011: 1:30-2:30  9288:  Keeping Your Network at Peak Performance as You Virtualize the Data Center
Aug 10, 2011: 8:00-9:00  9266:  IPv6 Basics
Aug 10, 2011: 4:30-5:30  9270:  Managing an IPv6 Network
Aug 11, 2011: 3:00-4:00  9273:  CSI Maui: Forensics in The Case of the Attacked Browsers
Aug 11, 2011: 11:00-12:00  9277:  Implementing IPv6 on Windows and Linux Desktop
Aug 11, 2011: 1:30-2:30  9290:  Network Problem Diagnosis with OSA Examples
Aug 12, 2011: 8:00-9:00  9308:  TCP/IP Performance Management in a Virtualized Environment
QUESTIONS?

laurak@aesclever.com
www.aesclever.com
650-617-2400