Digital Forensics Research Workshop Challenge 2009

Wouter van Dongen, Alain van Hoof
Research Project 2
1 July 2009
• Introduction
  • Challenge details
  • Research questions

• Method

• Time zones and Linux time stamps

• SSH traces

• Recovery of deleted files

• The big picture

• Questions
Challenge details

- Connecting from an IP address in New Orleans
- Advanced knowledge of Linux and digital forensics

Captured: March 11, 2009

NSSAL (Suspect)

- Thumb drive
  - FAT16
  - 512 MB
- PS3
  - Linux Ubuntu 8.10
  - EXT3 10 GB
- Physical Mem
  - 240 MB
- PCAP 1
- PCAP 2

- PCAP 1
- PS3
  - Linux Ubuntu 8.10
  - EXT3 10 GB

- Baltimore

Make illicit Mardi Gras images available to other ps3 users

JHU-ISI (John Hopkins University)
1. What relevant user activity can be reconstructed from the available forensic data and what does it show?

2. Is there evidence of inappropriate or suspicious activity on the system?

3. Is there evidence of collaboration with an outside party? If so, what can be determined about the identity of the outside party? How was any collaboration conducted?

4. Is there evidence that illicit data (specifically, Mardi Gras images) was exchanged? If so, what can be determined about that data and the manner of transfer?

5. What data (if any) was provided by the Johns Hopkins PS3?

6. The suspect claims that he was not responsible for any transfer of data. What evidence do you have to show that remote, unauthorized access to the system might have occurred, and does this evidence exonerate the suspect?
• Standard Linux commands on read-only mounted images

• Additional Linux utilities

• Restored images on Playstation 3 to observe and test behaviour

• Aftertime to parse and export 100,000 log entries of both systems

• Excel to quickly filter and search

• Created timeline
• 1 hour time difference

• Summertime: 8th of March

• Aftertime

<table>
<thead>
<tr>
<th>Disk Image</th>
<th>Physical Location</th>
<th>/etc/timezone</th>
<th>Code</th>
<th>UTC Offset Summertime (DST)</th>
<th>UTC Offset Wintertime</th>
</tr>
</thead>
<tbody>
<tr>
<td>nssal-linux-fs</td>
<td>New Orleans</td>
<td>America/Chicago</td>
<td>CDT</td>
<td>-5</td>
<td>-6</td>
</tr>
<tr>
<td>jhuis-linux-fs</td>
<td>Baltimore</td>
<td>US/Eastern</td>
<td>EST</td>
<td>-4</td>
<td>-5</td>
</tr>
</tbody>
</table>
• Modified, Access and Change time stamps, crucial for investigation.
• Mount options affect behaviour, not mentioned in literature!
  • relatime
  • noatime
  • nodiratime
• /etc/fstab

<table>
<thead>
<tr>
<th>Action</th>
<th>Updated time stamp(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creation</td>
<td>Access</td>
</tr>
<tr>
<td>Read</td>
<td>Access*</td>
</tr>
<tr>
<td>Modify Content</td>
<td>Access</td>
</tr>
<tr>
<td>Copy (source)</td>
<td>Access*</td>
</tr>
<tr>
<td>Copy (target does not exist)</td>
<td>Access</td>
</tr>
<tr>
<td>Copy (target does exist)</td>
<td>**</td>
</tr>
<tr>
<td>Move (target does not exist)</td>
<td></td>
</tr>
<tr>
<td>Move (target does exist)</td>
<td></td>
</tr>
</tbody>
</table>
Determining the mount options using time stamps

- **relatime**
  - Access > Change
  - Access = Change
  - Access < Change
  - Access > Modify
  - Access = Modify
  - Access < Modify

- **atime**
  - Access > Change
  - Access = Change
  - Access < Change
  - Access > Modify
  - Access = Modify
  - Access < Modify
Determining the mount options using time stamps
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>auth.log nssal-linux-side-fs.dd</td>
</tr>
<tr>
<td>3</td>
<td>ConsoleKit/history nssal-linux-side-fs.dd</td>
</tr>
<tr>
<td>4</td>
<td>wtmp nssal-linux-side-fs.dd</td>
</tr>
</tbody>
</table>
• ext3 zeros out block pointer on deletion
• Journaling: inode (entire block!) update is first recorded in journal
Carving is not always possible → journal based recovery

- Search for deleted files and their inode address in directory entries

505479  (16) Recipes  503339  (16) .lesshst
503412  (2688) memdump-powerpc.tar  <505465> (2660) .ICEauthority-n
<505482> (20) andromachi  <505483> (2604) bateman's
<505484> (20) stanley's  <505485> (2564) stoughton's

- Find inode copies in journal
No directory entries?

- Search journal for old entries (e.g. with ‘ext3grep –search’)
- Read all results (ext3grep --ls --block):

<table>
<thead>
<tr>
<th>Index</th>
<th>Next</th>
<th>Inode</th>
<th>Deletion Time</th>
<th>Mode</th>
<th>File Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>d</td>
<td>502947</td>
<td></td>
<td>drwxr-xr-x</td>
<td>.</td>
</tr>
<tr>
<td>1</td>
<td>d</td>
<td>502945</td>
<td></td>
<td>drwxr-xr-x</td>
<td>.profile</td>
</tr>
<tr>
<td>2</td>
<td>r</td>
<td>502948</td>
<td></td>
<td>rrw-r--r--</td>
<td>.profile</td>
</tr>
<tr>
<td>3</td>
<td>l</td>
<td>502949</td>
<td></td>
<td>lrwxrwxrwx</td>
<td>Examples -&gt; /u</td>
</tr>
<tr>
<td>4</td>
<td>r</td>
<td>502950</td>
<td></td>
<td>rrw-r--r--</td>
<td>.bash_logout</td>
</tr>
<tr>
<td>5</td>
<td>r</td>
<td>502951</td>
<td></td>
<td>rrw-r--r--</td>
<td>.bashrc</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>&lt;SNIP&gt;</td>
</tr>
<tr>
<td>34</td>
<td>d</td>
<td>503073</td>
<td></td>
<td>drwx-------</td>
<td>.update-notifi</td>
</tr>
<tr>
<td>35</td>
<td>d</td>
<td>505446</td>
<td></td>
<td>drwxr-xr-x</td>
<td>kmem</td>
</tr>
<tr>
<td>36</td>
<td>r</td>
<td>503092</td>
<td></td>
<td>rrw-t--r--</td>
<td>sudo_as_admin</td>
</tr>
<tr>
<td>37</td>
<td>r</td>
<td>503148</td>
<td>1236805424 Wed Mar 11 16:03:44 2009</td>
<td>rrw------</td>
<td>.bash_history</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>&lt;SNIP&gt;</td>
</tr>
<tr>
<td>46</td>
<td>r</td>
<td>503434</td>
<td>1236805688 Wed Mar 11 16:08:08 2009</td>
<td>rrw-r--r--</td>
<td>mem.find.pics</td>
</tr>
</tbody>
</table>

- Try restoring the inode
File still not recovered?

- Calculate block group data range and export the block (e.g. with `dd`) and try searching.

Recovered:

- Bash history
- Drug recipes
- Backdoor software

```bash
exit
pwd
lstsudo ./%backd00r &
gf
exit
adduser
adduser --help
ls /home
adduser --home /home/jhuisi jhuisi
passwd jhuisi
passwd jhuisi
ssh goatboy@ps3.isi.jhu.edu
ifconfig
```
Questions?