Offensive Forensics: CSI for Bad Guys

Benjamin Caudill
Principal Consultant, Rhino Security Labs
Introductions

• Benjamin Caudill
  • Principal Consultant with Rhino Security Labs
    • Pentesting, Social Engineering, Webapp

• ~4 Years in Security, 8+ Years in IT
  • Aerospace/Defense
    • Incident response, forensics (APT-centric)
  • Finance Industry
    • Webapp assessments
  • Consulting
    • Pentesting, Social Engineering

• Number of certifications, but who cares?
Overview

- Traditional Forensics
  - Brief background

- Offensive Forensics
  - Introduction/Basics
  - Memory
    - Potential, Problems
  - Disk/Registry
    - Potential, Problems

- New Metasploit Module
  - Usage
  - Quick demo
(Traditional) Digital Forensics

“...the recovery and investigation of material found in digital devices”

- Related tools and concepts used for investigations (criminal/civil/corporate/etc)

- Objective: Solve a “crime”

- As a result, few ‘forensics’ tools for pentesters
Offensive Forensics

“The use of forensics techniques for offensive purposes”
(Often for improved social engineering, password cracking)

• Why?
  • When traditional post-exploit techniques are insufficient for next steps
  • Pentesting has a time limit (can’t wait all day keylogging…)

• Objective- Access to additional sensitive information
  • Explicit vs Implicit
Forensic Comparison
(Live/Dead Analysis)

Traditional Forensics
• Live Analysis –
  • Can grab memory, but things are changing (scary)
  • Legal concerns, chain of custody…

• Dead Analysis –
  • System off
  • Stable – nothing is changing
  • Grab disk image

Offensive Forensics
• Live Analysis –
  • Access remotely and can grab memory, but permission prevent access to files
    • Hiberfil.sys, page.sys, other OS files, etc…

• Dead Analysis -
  • All files accessible (through disk image)
  • Loss of potential from user interaction/live RAM
Offensive Forensics - Memory

• Windows Clipboard
  • Password Managers – copy/paste

• Command-line History
  (“doskey /history”)
  • Adding users, FTP/Telnet sessions, etc

• Passwords, Key Files, Encryption Keys
  (‘process_memdump’ in post MSF modules)
  • Password/Key cache (ie: Truecrypt)
  • Older software (ie: PuTTY)

• Private Browsing/Sandboxing
  • Not quite so private after all…
    • (Coming soon!) Volatility plugin to detect Private Browsing Sessions
1. Browser Files - Watering Hole attacks, Locate intranet sites, Misc Sensitive
   • Firefox
     • key3.db & signons.sqlite (Passwords)
     • places.sqlite (Bookmarks and History)
     • Cookies.sqlite (Cookies)
     • Formhistory.sqlite (Saved form data)
     • Downloads.sqlite (Downloads)
     • Content-prefs.sqlite (Site-specific settings, such as local download locations)
     • Addons.sqlite (Browser Addons)
     • Sessionstore.js (Saved session for when Firefox re-opens)
<table>
<thead>
<tr>
<th>Column Name</th>
<th>Last Updated</th>
<th>First Updated</th>
<th>Days Ago</th>
</tr>
</thead>
<tbody>
<tr>
<td>attendee_236329415_job_title</td>
<td>07/10/201...</td>
<td>07/10/201...</td>
<td>17 days</td>
</tr>
<tr>
<td>attendee_236329415_last_name</td>
<td>07/18/201...</td>
<td>07/18/201...</td>
<td>9 days</td>
</tr>
<tr>
<td>billTo_city</td>
<td>07/18/201...</td>
<td>07/18/201...</td>
<td>9 days</td>
</tr>
<tr>
<td>billTo_email</td>
<td>07/18/201...</td>
<td>07/18/201...</td>
<td>9 days</td>
</tr>
<tr>
<td>billTo_firstName</td>
<td>07/18/201...</td>
<td>07/18/201...</td>
<td>9 days</td>
</tr>
<tr>
<td>billTo_firstName</td>
<td>07/18/201...</td>
<td>07/18/201...</td>
<td>9 days</td>
</tr>
<tr>
<td>billTo_lastName</td>
<td>07/18/201...</td>
<td>07/18/201...</td>
<td>9 days</td>
</tr>
<tr>
<td>billTo_phoneNumber</td>
<td>07/18/201...</td>
<td>07/18/201...</td>
<td>9 days</td>
</tr>
<tr>
<td>billTo_postalCode</td>
<td>07/18/201...</td>
<td>07/18/201...</td>
<td>9 days</td>
</tr>
<tr>
<td>billTo_state</td>
<td>07/18/201...</td>
<td>07/18/201...</td>
<td>9 days</td>
</tr>
<tr>
<td>billTo_street1</td>
<td>07/18/201...</td>
<td>07/18/201...</td>
<td>9 days</td>
</tr>
<tr>
<td>billing_info/address1</td>
<td>07/18/201...</td>
<td>07/18/201...</td>
<td>9 days</td>
</tr>
<tr>
<td>billing_info/address2</td>
<td>07/18/201...</td>
<td>07/18/201...</td>
<td>9 days</td>
</tr>
<tr>
<td>billing_info/city</td>
<td>07/18/201...</td>
<td>07/18/201...</td>
<td>9 days</td>
</tr>
<tr>
<td>billing_info/state</td>
<td>07/18/201...</td>
<td>07/18/201...</td>
<td>9 days</td>
</tr>
<tr>
<td>billing_info/zip</td>
<td>07/18/201...</td>
<td>07/18/201...</td>
<td>9 days</td>
</tr>
<tr>
<td>blogTextBox</td>
<td>07/18/201...</td>
<td>07/18/201...</td>
<td>9 days</td>
</tr>
<tr>
<td>card_cvNumber</td>
<td>07/18/201...</td>
<td>07/18/201...</td>
<td>9 days</td>
</tr>
<tr>
<td>card_expirationMonth</td>
<td>07/18/201...</td>
<td>07/18/201...</td>
<td>9 days</td>
</tr>
<tr>
<td>card_expirationYear</td>
<td>07/18/201...</td>
<td>07/18/201...</td>
<td>9 days</td>
</tr>
<tr>
<td>cf_field_3</td>
<td>07/18/201...</td>
<td>07/18/201...</td>
<td>9 days</td>
</tr>
<tr>
<td>cf_field_4</td>
<td>07/18/201...</td>
<td>07/18/201...</td>
<td>9 days</td>
</tr>
<tr>
<td>cf_field_5</td>
<td>07/18/201...</td>
<td>07/18/201...</td>
<td>9 days</td>
</tr>
<tr>
<td>cf_field_7</td>
<td>07/18/201...</td>
<td>07/18/201...</td>
<td>9 days</td>
</tr>
<tr>
<td>cforms_captcha</td>
<td>07/18/201...</td>
<td>07/18/201...</td>
<td>9 days</td>
</tr>
<tr>
<td>cforms_captcha</td>
<td>07/18/201...</td>
<td>07/18/201...</td>
<td>9 days</td>
</tr>
<tr>
<td>Column</td>
<td>Data 1</td>
<td>Data 2</td>
<td>Days</td>
</tr>
<tr>
<td>-----------------</td>
<td>--------</td>
<td>--------</td>
<td>-------</td>
</tr>
<tr>
<td>account</td>
<td>1 07/18/201... 07/18/201...</td>
<td>9 days</td>
<td></td>
</tr>
<tr>
<td>account_token</td>
<td>1 07/10/201... 07/10/201...</td>
<td>17 days</td>
<td></td>
</tr>
<tr>
<td>account_name</td>
<td>1 07/17/201... 07/17/201...</td>
<td>10 days</td>
<td></td>
</tr>
<tr>
<td>account_id</td>
<td>1 07/17/201... 07/17/201...</td>
<td>10 days</td>
<td></td>
</tr>
<tr>
<td>action_links</td>
<td>1 07/18/201... 07/18/201...</td>
<td>9 days</td>
<td></td>
</tr>
<tr>
<td>amount</td>
<td>1 07/17/201... 07/17/201...</td>
<td>10 days</td>
<td></td>
</tr>
<tr>
<td>answerOne</td>
<td>1 07/18/201... 07/18/201...</td>
<td>9 days</td>
<td></td>
</tr>
<tr>
<td>answerTwo</td>
<td>1 07/18/201... 07/18/201...</td>
<td>9 days</td>
<td></td>
</tr>
<tr>
<td>answerThree</td>
<td>1 07/18/201... 07/18/201...</td>
<td>9 days</td>
<td></td>
</tr>
<tr>
<td>answerFour</td>
<td>1 07/18/201... 07/18/201...</td>
<td>9 days</td>
<td></td>
</tr>
<tr>
<td>answerFive</td>
<td>1 07/18/201... 07/18/201...</td>
<td>9 days</td>
<td></td>
</tr>
<tr>
<td>answerSix</td>
<td>1 07/18/201... 07/18/201...</td>
<td>9 days</td>
<td></td>
</tr>
<tr>
<td>answerSeven</td>
<td>1 07/18/201... 07/18/201...</td>
<td>9 days</td>
<td></td>
</tr>
<tr>
<td>answerEight</td>
<td>1 07/18/201... 07/18/201...</td>
<td>9 days</td>
<td></td>
</tr>
</tbody>
</table>
2. Most Recently Used (MRU) - What has the user been looking at?

3. Prefetch Files – What has the user been running?

4. Deleted files/Slack Space - What had been on the disk?
   ('imager.rb', 'recover_files.rb' in post MSF modules)
   • Files are deleted for a reason
   • Still underutilized as it takes more time

5. Backups, Volume Shadow-Copy Service (VSS)
   ('vss_list.rb', related others in post MSF modules)
6. Crash dumps – (theoretically) same potential as live memory
   • Live systems can’t access page/hiberfil directly, but dumps may be available

   • Implicitly Sensitive (spearphishing, watering holes, password cracking, etc.)
Offensive Forensics - Disk/Registry

- Mo’ Data, Mo’ Problems!
  - Thousands of potential files/directories to search
  - Not all apply to every OS, application, version, etc.
Offensive Forensics - Disk/Registry

• ...And a Meterpreter script was born!

• **Forensic_Scraper**- Using OS identification, grabs and downloads:
  
  • All Major Browser Files (history, saved passwords, form data, etc)
  • Most Recently Used (MRU) list for Windows, MS Office
  • Prefetch data (exe’s, time-date stamps)
  • Windows Crash Dumps
  • Print Spools
  • Located Backups (Windows, iPhone, Blackberry, etc)
  • Much more...
Forensic_Scraper – Demo

- Simple – point and shoot
Forensic_Scraper – Demo
Offensive Forensics - Conclusion

Q/A:
Find me afterwards

‘Forensic_Scraper’ Download/Demo:
RhinoSecurityLabs.com/blog
(or from Defcon)

Contact:
Benjamin.Caudill@RhinoSecurityLabs.com
@RhinoSecurity