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

RHINO SECURITY LABS

(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

RHINO SECURITY LABS

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

RHINO SECURITY LABS

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

RHINO SECURITY LABS

Offensive Forensics - Disk/Registry (1)

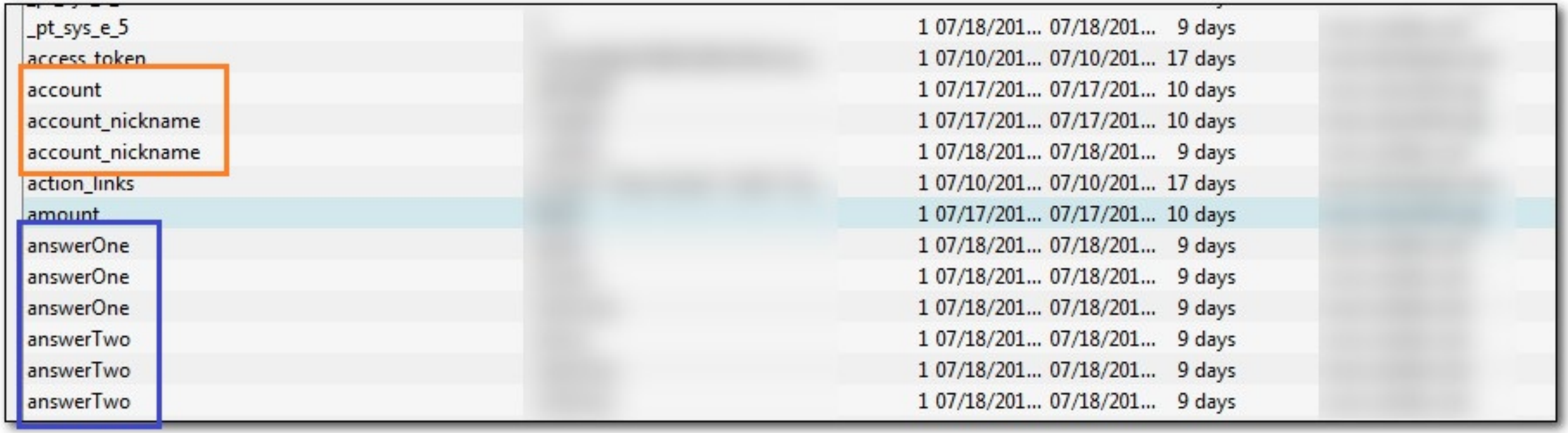
1. Browser Files - Watering Hole attacks, Locate intranet sites, Misc Sensitive
   - Firefox
     - **key3.db & signons.sqlite** (Passwords)
     - **places.sqlite** (Bookmarks and History)
     - **Cookies.sqlite** (Cookies)
     - **Formhistory.sqlite** (Saved form data)
     - **Downloads.sqlite** (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)

RHINO SECURITY LABS

Browser Form History – Credit Card Info

attendee_236329415_job_title	1	07/10/201...	07/10/201...	17 days
attendee_236329415_last_name	1	07/10/201...	07/10/201...	17 days
billTo_city	1	07/18/201...	07/18/201...	9 days
billTo_email	1	07/18/201...	07/18/201...	9 days
billTo_firstName	1	07/18/201...	07/18/201...	9 days
billTo_firstName	1	07/18/201...	07/18/201...	9 days
billTo_lastName	1	07/18/201...	07/18/201...	9 days
billTo_phoneNumber	1	07/18/201...	07/18/201...	9 days
billTo_postalCode	1	07/18/201...	07/18/201...	9 days
billTo_state	1	07/18/201...	07/18/201...	9 days
billTo_street1	1	07/18/201...	07/18/201...	9 days
billing_info[address1]	1	07/18/201...	07/18/201...	9 days
billing_info[address2]	1	07/18/201...	07/18/201...	9 days
billing_info[city]	1	07/18/201...	07/18/201...	9 days
billing_info[state]	1	07/18/201...	07/18/201...	9 days
billing_info[zip]	1	07/18/201...	07/18/201...	9 days
blogTextBox	1	07/18/201...	07/18/201...	9 days
card_cvNumber	1	07/18/201...	07/18/201...	9 days
card_expirationMonth	1	07/18/201...	07/18/201...	9 days
card_expirationYear	1	07/18/201...	07/18/201...	9 days
cf_field_3	1	07/18/201...	07/18/201...	9 days
cf_field_4	1	07/18/201...	07/18/201...	9 days
cf_field_5	1	07/18/201...	07/18/201...	9 days
cf_field_7	1	07/18/201...	07/18/201...	9 days
cforms_captcha	1	07/18/201...	07/18/201...	9 days
cforms_captcha	1	07/18/201...	07/18/201...	9 days

Browser Form History – Account Compromise



_pt_sys_e_5	1	07/18/201...	07/18/201...	9 days
access_token	1	07/10/201...	07/10/201...	17 days
account	1	07/17/201...	07/17/201...	10 days
account_nickname	1	07/17/201...	07/17/201...	10 days
account_nickname	1	07/18/201...	07/18/201...	9 days
action_links	1	07/10/201...	07/10/201...	17 days
amount	1	07/17/201...	07/17/201...	10 days
answerOne	1	07/18/201...	07/18/201...	9 days
answerOne	1	07/18/201...	07/18/201...	9 days
answerOne	1	07/18/201...	07/18/201...	9 days
answerTwo	1	07/18/201...	07/18/201...	9 days
answerTwo	1	07/18/201...	07/18/201...	9 days
answerTwo	1	07/18/201...	07/18/201...	9 days

RHINO SECURITY LABS

Offensive Forensics - Disk/Registry (2)

2. Most Recently Used (MRU) - What has the user been looking at?

3. Prefetch Files – What has the user been runnir

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)

RHINO SECURITY LABS

Offensive Forensics - Disk/Registry (3)

6. Crash dumps – (theoretically) same potential as live memory
   - Live systems can't access page/hiberfil directly, but dumps may be available

7. Calendars, Address book, Smartphone backups, print spools, misc.
   - Implicitly Sensitive (spearphishing, watering holes, password cracking, etc.)

RHINO SECURITY LABS

Offensive Forensics - Disk/Registry

- **Mo' Data, Mo' Problems!**
  - Thousands of potential files/directories to search
  - Not all apply to every OS, application, version, etc.

RHINO SECURITY LABS

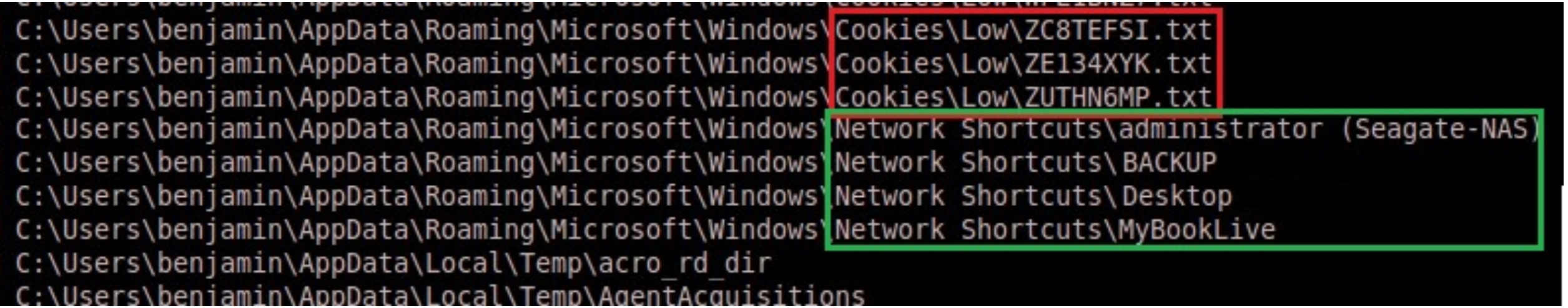
Offensive Forensics - Disk/Registry

- …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



RHINO SECURITY LABS

Forensic_Scraper – Demo

```
found C:\Users\benjamin\AppData\Local\Google\Chrome\User Data\Default\Archived History
found C:\Users\benjamin\AppData\Local\Google\Chrome\User Data\Default\Cookies
found C:\Users\benjamin\AppData\Local\Google\Chrome\User Data\Default\Current Tabs
found C:\Users\benjamin\AppData\Local\Google\Chrome\User Data\Default\Extension Cookies
found C:\Users\benjamin\AppData\Local\Google\Chrome\User Data\Default\History
found C:\Users\benjamin\AppData\Local\Google\Chrome\User Data\Default\Login Data
found C:\Users\benjamin\AppData\Local\Google\Chrome\User Data\Default\Visited Links
found C:\Users\benjamin\AppData\Local\Google\Chrome\User Data\Default\Web Data
found C:\Users\benjamin\AppData\Roaming\Mozilla\Firefox\Profiles\crixlgd7.default\addons.sqlite
found C:\Users\benjamin\AppData\Roaming\Mozilla\Firefox\Profiles\crixlgd7.default\content-prefs.sqlite
found C:\Users\benjamin\AppData\Roaming\Mozilla\Firefox\Profiles\crixlgd7.default\cookies.sqlite
found C:\Users\benjamin\AppData\Roaming\Mozilla\Firefox\Profiles\crixlgd7.default\cookies.sqlite-shm
found C:\Users\benjamin\AppData\Roaming\Mozilla\Firefox\Profiles\crixlgd7.default\cookies.sqlite-wal
found C:\Users\benjamin\AppData\Roaming\Mozilla\Firefox\Profiles\crixlgd7.default\downloads.sqlite
found C:\Users\benjamin\AppData\Roaming\Mozilla\Firefox\Profiles\crixlgd7.default\extensions.sqlite
found C:\Users\benjamin\AppData\Roaming\Mozilla\Firefox\Profiles\crixlgd7.default\formhistory.sqlite
found C:\Users\benjamin\AppData\Roaming\Mozilla\Firefox\Profiles\crixlgd7.default\key3.db
found C:\Users\benjamin\AppData\Roaming\Mozilla\Firefox\Profiles\crixlgd7.default\places.sqlite
found C:\Users\benjamin\AppData\Roaming\Mozilla\Firefox\Profiles\crixlgd7.default\places.sqlite-shm
found C:\Users\benjamin\AppData\Roaming\Mozilla\Firefox\Profiles\crixlgd7.default\places.sqlite-wal
found C:\Users\benjamin\AppData\Roaming\Mozilla\Firefox\Profiles\crixlgd7.default\sessionstore.js
found C:\Users\benjamin\AppData\Roaming\Mozilla\Firefox\Profiles\crixlgd7.default\signons.sqlite
```

Offensive Forensics - Conclusion

Q/A:

Find me afterwards

‘Forensic_Scraper’ Download/Demo:

RhinoSecurityLabs.com/blog
(or from Defcon)

Contact:

Benjamin.Caudill@RhinoSecurityLabs.com
@RhinoSecurity

RHINO SECURITY LABS