Why not to “stay in your lane" as a digital forensic examiner

Alissa Torres
KEYW Corporation
Offensive Security Topics

- Operating Systems Internals
- Hacking/Pentesting
- Anti-Forensics Techniques
- Malware Reversing & Analysis
Benefits of Adding to your Technical Arsenal

1. Improve the Incident Responder Methodology
2. Increase Detection Capability
3. Enhance Forensic Kung Fu
Benefit # 1
Improve the Incident Responder Methodology
Benefit #1
Improve IR Methodology

- Temporal Recordkeeping Discipline
- Preventing Further Compromise
Keeping a Clean Timeline

- Attackers often use admin tools on compromised systems.
- Responders must maintain records of when they run their IR tools on a target system.
Out-of-Band Communications

- Attackers are on the network; therefore we must assume they can monitor communications.
- Encrypt email & chat sessions.
- Incident-related research must be done via non-attributable Internet resources behind anonymizing proxies.
- When compromised by a sophisticated adversary, the IR process should be moved off the network entirely.
Due to domain credential caching by Windows, it is possible to divulge further credentials to the attacker while responding to a compromised system.

Mike Pilkington

“Protecting Privileged Domain Accounts: Safeguarding Password Hashes”

http://computer-forensics.sans.org/blog/2012/02/21/protecting-privileged-domain-account-safeguarding-password-hashes
meterpreter > migrate 3296
[*] Migrating to 3296...
[*] Migration completed successfully.
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > background
msf  post(cachedump) > run

[*] Executing module against BATTLECADE
[*] Cached Credentials Setting: 10 - (Max is 50 and 0 disables, and 10 is default)
[*] Obtaining boot key...
[*] Obtaining Lsa key...
[*] Trying 'Vista' style...
[*] Vista compatible client
[*] Obtaining LK$KM...
[*] Dumping cached credentials...

[*] John the Ripper format: rblume:12cf2c7f7d71f34141f07db86ff6730c:CRAZYCHINCHILLA.COM:CRAZYCHINCHILLA
[*] Hash are in MSCACHE_VISTA format. (mscash2)
[*] Post module execution completed
msf  post(cachedump) >
PSExec Used by Responder w/Domain Creds

C:\>psexc \battl\ecade -u crazychinchilla\administrator -p EvilAnimal cmd.exe

PsExec v1.98 - Execute processes remotely
Copyright (C) 2001-2010 Mark Russinovich
Sysinternals - www.sysinternals.com

Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>netstat

Active Connections

<table>
<thead>
<tr>
<th>Proto</th>
<th>Local Address</th>
<th>Foreign Address</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>172.16.100.154:445</td>
<td>user-1b78sf:4963</td>
<td>ESTABLISHED</td>
</tr>
<tr>
<td>TCP</td>
<td>172.16.100.154:50193</td>
<td>184.17.251.43:3689</td>
<td>ESTABLISHED</td>
</tr>
<tr>
<td>TCP</td>
<td>172.16.100.154:50242</td>
<td>184.17.251.43:4444</td>
<td>CLOSE_WAIT</td>
</tr>
<tr>
<td>TCP</td>
<td>172.16.100.154:50250</td>
<td>184.17.251.43:4444</td>
<td>ESTABLISHED</td>
</tr>
<tr>
<td>TCP</td>
<td>170.16.432.454:50260</td>
<td>184.17.251.43:4444</td>
<td>ESTABLISHED</td>
</tr>
</tbody>
</table>
Cachedump (After)

```
msf post(cachedump) > run

[*] Executing module against BATTLECADE
[*] Cached Credentials Setting: 10 - (Max is 50 and 0 disables, and 10 is default)
[*] Obtaining boot key...
[*] Obtaining Lsa key...
[*] Trying 'Vista' style...
[*] Vista compatible client
[*] Obtaining LK$KM...
[*] Dumping cached credentials...
[*] John the Ripper format:
    rblume:12cf2c7f7d71f34141f07db86ff6730c:CRAZYPHENCHILLA.COM:CRAZYPHENCHILLA
    administrator:c319ffcbd0d70629b98d5269e2d08f3b:CRAZYPHENCHILLA.COM:CRAZYPHENCHILLA
[*] Hash are in MSCACHE_VISTA format. (mscash2)
[*] Post module execution completed
```
Benefit # 2
Increase Detection Capability
Benefit #2
Increase Detection Capability

• Anticipating Adversary’s Tactics & Techniques
• Recognizing Rogue Processes/Services
• Detecting Anomalous Behavior
5 Phases of Remote Exploitation

- **Information Gathering** – Identify access vectors
- **Scanning & Enumeration** – Map attack surface
- **Gaining Access** – Breach the network
- **Expanding Access** – Identify and own key terrain
- **Sustaining Access** – Reduce footprint and consolidate collection
Gaining Access Methodology

- Upon Gaining Access to a remote system, the attacker will conduct a risk assessment.

- Enumerating:
  - Running Processes
  - Running Services
  - Software/Drivers Installed
  - Audit Policy Settings
  - Mapped Drives
  - User Profiles
  - Network Connections/Caches
  - Scheduled Jobs
Operating System Internals

• Like Attackers, Forensics Examiners must know what *normal* looks like
  o Standard Processes and their run paths
  o Parent Processes
  o Common options/switches for processes
  o Services that are native to their network
Common Processes

- Session Manager Subsystem (*smss.exe*)
- Client/Server Runtime Server Subsystem (*csrss.exe*)
- Windows Logon (*winlogon.exe*)
- Service Control Manager (*services.exe*)
- Local Security Authority Subsystem (*lsass.exe*)
- Service Host (*svchost.exe*)
- Explorer (*explorer.exe*)
Process Explorer v.15.2
by SysInternals (Mark Russinovich & Bryce Cogwell)

- Shows tree-like structure of Processes
- Handles & DLLs
<table>
<thead>
<tr>
<th>Offset(V)</th>
<th>Name</th>
<th>PID</th>
<th>PPID</th>
<th>Thds</th>
<th>Hnds</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x84828020</td>
<td>System</td>
<td>4</td>
<td>0</td>
<td>107</td>
<td>547</td>
<td>2012-04-09 13:57:35</td>
</tr>
<tr>
<td>0x861e22c0</td>
<td>smss.exe</td>
<td>324</td>
<td>4</td>
<td>4</td>
<td>33</td>
<td>2012-04-09 13:57:35</td>
</tr>
<tr>
<td>0x8610a970</td>
<td>csrss.exe</td>
<td>420</td>
<td>396</td>
<td>9</td>
<td>543</td>
<td>2012-04-09 13:57:39</td>
</tr>
<tr>
<td>0x8614a2b8</td>
<td>wininit.exe</td>
<td>460</td>
<td>396</td>
<td>3</td>
<td>82</td>
<td>2012-04-09 13:57:39</td>
</tr>
<tr>
<td>0x86aad960</td>
<td>services.exe</td>
<td>528</td>
<td>460</td>
<td>5</td>
<td>238</td>
<td>2012-04-09 13:57:39</td>
</tr>
<tr>
<td>0x869f6b18</td>
<td>lsass.exe</td>
<td>572</td>
<td>460</td>
<td>8</td>
<td>765</td>
<td>2012-04-09 13:57:39</td>
</tr>
<tr>
<td>0x86adc030</td>
<td>lsm.exe</td>
<td>580</td>
<td>460</td>
<td>10</td>
<td>148</td>
<td>2012-04-09 13:57:39</td>
</tr>
<tr>
<td>0x86437920</td>
<td>svchost.exe</td>
<td>696</td>
<td>528</td>
<td>10</td>
<td>434</td>
<td>2012-04-09 13:57:40</td>
</tr>
<tr>
<td>0x86d7fd40</td>
<td>svchost.exe</td>
<td>776</td>
<td>528</td>
<td>7</td>
<td>270</td>
<td>2012-04-09 13:57:41</td>
</tr>
<tr>
<td>0x86dcad40</td>
<td>MsMpEng.exe</td>
<td>860</td>
<td>528</td>
<td>31</td>
<td>444</td>
<td>2012-04-09 13:57:41</td>
</tr>
<tr>
<td>0x87030460</td>
<td>svchost.exe</td>
<td>932</td>
<td>528</td>
<td>17</td>
<td>490</td>
<td>2012-04-09 13:57:42</td>
</tr>
<tr>
<td>0x87056030</td>
<td>svchost.exe</td>
<td>976</td>
<td>528</td>
<td>29</td>
<td>770</td>
<td>2012-04-09 13:57:42</td>
</tr>
<tr>
<td>0x8705b8b0</td>
<td>svchost.exe</td>
<td>1004</td>
<td>528</td>
<td>32</td>
<td>1216</td>
<td>2012-04-09 13:57:42</td>
</tr>
<tr>
<td>0x87155030</td>
<td>svchost.exe</td>
<td>1140</td>
<td>528</td>
<td>18</td>
<td>466</td>
<td>2012-04-09 13:57:44</td>
</tr>
<tr>
<td>0x871a8518</td>
<td>svchost.exe</td>
<td>1276</td>
<td>528</td>
<td>16</td>
<td>446</td>
<td>2012-04-09 13:57:44</td>
</tr>
<tr>
<td>0x87276530</td>
<td>spoolsv.exe</td>
<td>1548</td>
<td>528</td>
<td>12</td>
<td>293</td>
<td>2012-04-09 13:57:48</td>
</tr>
<tr>
<td>0x872e8a28</td>
<td>svchost.exe</td>
<td>1592</td>
<td>528</td>
<td>16</td>
<td>318</td>
<td>2012-04-09 13:57:48</td>
</tr>
<tr>
<td>0x87407c28</td>
<td>armsvc.exe</td>
<td>1696</td>
<td>528</td>
<td>4</td>
<td>67</td>
<td>2012-04-09 13:57:50</td>
</tr>
<tr>
<td>0x871e4030</td>
<td>NisSrv.exe</td>
<td>116</td>
<td>528</td>
<td>6</td>
<td>260</td>
<td>2012-04-09 13:57:52</td>
</tr>
<tr>
<td>0x874ab030</td>
<td>WUDFHost.exe</td>
<td>760</td>
<td>976</td>
<td>8</td>
<td>248</td>
<td>2012-04-09 13:57:52</td>
</tr>
<tr>
<td>0x87384d18</td>
<td>svchost.exe</td>
<td>2936</td>
<td>528</td>
<td>10</td>
<td>164</td>
<td>2012-04-09 13:52:25</td>
</tr>
<tr>
<td>0x86b37d40</td>
<td>SearchIndexer.exe</td>
<td>3100</td>
<td>528</td>
<td>15</td>
<td>827</td>
<td>2012-04-09 13:52:28</td>
</tr>
<tr>
<td>0x84934d40</td>
<td>OSPPSVC.EXE</td>
<td>3724</td>
<td>528</td>
<td>3</td>
<td>144</td>
<td>2012-04-09 13:52:54</td>
</tr>
<tr>
<td>0x849bbd40</td>
<td>spnsvc.exe</td>
<td>1124</td>
<td>528</td>
<td>4</td>
<td>172</td>
<td>2012-04-09 13:53:21</td>
</tr>
</tbody>
</table>
Detecting Anomalous Behavior

- Event log clearing/flooding
- Unusual Login Activity
- Changes to local security policies
**Event Log Clearing/Flooding**

<table>
<thead>
<tr>
<th>Level</th>
<th>Date and Time</th>
<th>Source</th>
<th>Event ID</th>
<th>Task Category</th>
<th>User</th>
</tr>
</thead>
</table>

*OR*

- Event ID 517: Successful Clearing of Event Log
Unusual Login Activity

- Attackers steal credentials and reuse them to move laterally across the network
- This lateral movement is not often detect due to the use of legitimate credentials
- Detecting outliers to the user account’s normal patterns aids in this activity’s detection
Presence of Hacking Tools

• Recognizing Offensive Tools
  o Hashsets of common offensive tools
    (keyloggers, packet sniffers, backdoors, pwdump)
  o Hashsets of common admin tools
    (psexec, xcmd.exe, etc)

• Behavior Analysis of Toolsets
  o Sandbox Behavior Analysis
  o Active Monitoring (ARM, Regshot)
File Manipulation

Timestomping – technique used to obfuscate an attacker’s tools/code (files uploaded to system)

• Tool to detect – AnalyzeMFT.py

```
meterpreter > timestompp spammimic.txt -f desktop.lnk
[*] Setting MACE attributes on spammimic.txt from desktop.lnk
```

• Changing compile time/datestamp in PE Header to defeat malware analysis
Benefit # 3
Improve Forensics
Kung Fu
Benefit #3
Enhance Forensic Kung Fu

- Recognize the Rogue Internal User
- Find Registry settings/Service changes
  - Turning off Prefetch
  - Turning off System Protection (VSCs)
  - Clearing Shellbags
Profile of the Rogue User

- Obfuscation Tools (Browser add-ons, proxies)
- Signs of File Hiding
- Indications of secure delete tool usage
- Presence of hacking tools, ssh clients, programming language libraries (ruby, perl, python)
- Presence and use of Virtualization software (specialized pentesting/hacker distros)
<table>
<thead>
<tr>
<th>Addon Name</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cookies Manager+</td>
<td>1.5.1</td>
</tr>
<tr>
<td>Firebug</td>
<td>1.9.2</td>
</tr>
<tr>
<td>FoxyProxy Standard</td>
<td>3.6.2</td>
</tr>
<tr>
<td>Tamper Data</td>
<td>11.0.1</td>
</tr>
<tr>
<td>User Agent Switcher</td>
<td>0.7.3</td>
</tr>
</tbody>
</table>

Cookies Manager+: A cookies manager that allows view, edit, and create cookies as well as edit multiple cookies at once and backup/restore them.

Firebug: Web Development Evolved.

FoxyProxy Standard: FoxyProxy - Premier proxy management for Firefox.

Tamper Data: View and modify HTTP/HTTPS headers etc. Track and time requests.

User Agent Switcher: Adds a menu and a toolbar button to switch the user agent of a browser.
Indications of secure delete tool usage

• Secure delete/cleaner tools have grown more sophisticated over the years
• Still leave behind indications that they have been run
  o Log files
  o Job history files
  o Deleted temp files
  o Prefetch files
  o .LNK files
• Physical drive analysis
  o Consistent pattern of overwritten bytes
Detecting System Registry Changes

• Turning off Prefetch Files
• Turning off System Protection (VSCs)
• Clearing Shellbags
Turning off Prefetch

HKLM\System\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters

meterpreter > reg queryval -k "HKLM\system\currentcontrolset\control\session manager\memory management\Prefetchparameters" -v EnablePrefetcher
Key: HKLM\system\currentcontrolset\control\session manager\memory management\Prefetchparameters
Name: EnablePrefetcher
Type: REG_DWORD
Data: 3

0 = Disabled
1 = Application Launch Prefetch
2 = Boot Prefetch
3 = Prefetch All
Turning off Prefetch via the Registry

Registry value set to 0: prefetch file creation stopped

Registry value set to 3: prefetch file creation restarted, no effect on existing prefetch folder
Turning off Prefetch Service

Superfetch service stopped: System Event log entry
Superfetch service restarted: Prefetch folder cleared
Turning off VSCs

HKLM\Software\Microsoft\Windows NT\CurrentVersion\System Restore

0 = Disabled
1 = Enabled
Turning off VSCs

• Turning off VSCs via the GUI or the Registry, the Event log activity was the same
• Event 7036: The Volume Shadow Copy Service entered the stopped state.
• Event 7036: The MS Software Shadow Copy Provider Service entered the stopped state.
• Current VSCs in System Information Volume were deleted.
Summary

- Multiple benefits to crosstraining as forensic examiners/incident responders
- Training can consist of “on-the-job”, classroom, self-study, meetup groups, skills challenges
- Benefits maximized if the team/cell can train together
- Scenario-based team training events deliver realistic experience & provide a true measure of IR capabilities within an organization