****

**Case Project**

**CY5210 Information System Forensics**

**Instructor: Elton Booker**

**[Student Name]**

**EXECUTIVE SUMMARY**

[This section should be written last. This section should be one page, or less, or explain the case at a high level. I will often copy the first paragraph of the introduction, remove any technical jargon, and make sure it’s straightforward for non-technical folks. This will include the initial problem, the date you were notified, and how the detection was made (could be 1-2 paragraphs in the end).

I will include any relevant findings of the analysis section, but minimal detail. For example, I may summarize the USB and Shell Items sections to say – J. Smith connected two USB devices to his system. One device, a 32GB Kingston Data Traveler, was connected and four company proprietary documents were moved to the USB drive. I might also include the installation of malware and any attempt to perform anti-forensics using specific software or deleting outside of normal operation.

I will conclude this section with some items noted in the Conclusion section. For example – Analysis of J. Smith’s system identified indicators of data exfiltration via USB devices and personal e-mail. Evidence was clear that J. Smith was disgruntled and intended to leave the company with proprietary data to improve his reputation when he began employment with a competitor. J. Smith performed anti-forensic techniques in attempt to hide his activity. The personal USB devices should be requested and remediated so that proprietary data is not removed from the company, otherwise legal action may need to be initiated against J. Smith.]

**[Note:** This section needs to be less than one page.]

**[Report Notes:** Spell everyone’s name out the first time, but subsequent times their name should be abbreviated to F. LASTNAME. This includes your name as the Forensic Analyst/Investigator. Make sure you use the same tense throughout a paragraph. I attempt to use an active voice and past tense. I also use the “Justify” paragraph formatting, except bulleted points and section headings. If a new section begins at the end of a page, enter “Returns” so the section begins at the top of the next page. Finally, delete all template notes and sections with [] used as a guide before submitting the report.]

**[The Executive Summary should be page 2, but the Intro needs to begin on page 3 even if the Executive Summary is only ½ page.]**

**INTRODUCTION**

[Explain the date you were notified of an incident, why the activity is a concern (policy violation, illegal act, data exfiltration), what alert may have been received, and the department or person who first notified you or your team. Here you will include any authority you have received, the dates and completion of the chain of custody document (refer to the Appendix number for the document), and when you retrieved any devices (and imaged them) and the devices themselves.]

[You should also include a screenshot (Figure 1) of the hash verification here and identify whether the hashes verified or not, and why this is the case if they don’t match.]

**[This section is also one-half to a full page only]**

**ANALYSIS**

**[There is no particular order for the analysis you do, or the artifacts listed, but sections that will have 1-2 paragraphs, or more, should have their own heading. You can omit or add headings here as necessary. When you’re looking to hold a use responsible for an action, identify when that account was logged on and logged off to place the user “at the keyboard.”]**

**REGISTRY ANALYSIS**

[Identify the specific information required from registry analysis. These items are listed in the Week 13 slides and include user/group information, system information, and user activity. You may present this information in paragraph form, a bulleted list divided into sections, and this is more free form than other sections since analysts will add different information.]

**Example:** The Windows registry for [hostname] was analyzed for specific system configurations and settings, user specific settings, and user activity using Windows Registry Ripper v2.8. The SAM, SYSTEM, SOFTWARE and user hives (NTUSER.DAT and USRCLASS.DAT) were reviewed for relevant information pertinent to this investigation. The Windows registry identifies current system configuration and settings that may be useful to show the current state of the system and the actions performed by all users on a system.

Include sections similar to those below. You may use paragraph form (which is what I do if bulleted items are moved to the registry) or bulleted points, which law enforcement often does in the report. The Executive Summary should not have bullet points.

**USER/GROUP INFORMATION**

* **Users:** 
  + List the usernames here, their SIDs, and last login date [one per bullet point]
* **Groups:**
  + Note any groups of interest and any SIDs under that group name
  + What Administrator accounts exist? Who is allowed to RDP to the system?
  + What are the password settings for accounts of interest?

**SYSTEM INFORMATION**

* **Microsoft OS Version:**
* **Service Pack Level:**
* **Current Control Set:**
* **OS Install Date:**
* **Computer Name:**
* **Time Zone:**
* **Network Interfaces with Last Connection Time:**
* **Autostart Programs:**
* **Last Shutdown Time:**

**USER ACTIVITY**

**[This may be easier in paragraph form, but this is up to your own discretion. You could also explain the findings of each item in 2-3 sentences in a bullet point.]**

* **Windows Search History:** Analysis identified that J. Smith searched for specific files or applications in the Windows Explorer bar which included, “CCleaner, proprietary document, stolen password file.”
* **Typed Paths:** J. Smith has not appeared to have searched for specific paths on the system according to the lack of evidence identified under the registry key NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths.
* **RecentDocs:** Identify recent documents opened by the user or note this will be covered in a separate section if this list is long.
* **Last Executed Commands:** This may not be populated if commands were not run from the START -> RUN box.
* **UserAssist:** Identify any programs executed by the user. If this is explained under application analysis – skip this.

**USB DEVICE ANALYSIS**

[Detail any relevant findings and note any devices connected by users of interest in a specific timeframe. Include the Friendly Name or type of device, the user that connected the device, serial number, first time connected, and last time connected. In the narrative, explain why devices are of interest. You can omit devices unrelated to your investigation or suspect, or leave them in, but explain why they’re unrelated. Identify any volume letters that may have been assigned to the device by the operating system.]

[Table 1 will identify the five characteristics required for USB device analysis (some cells may be blank due to a failure to recover them because they may not exist or need to be manually identified. Make sure the table is formatted in some way.]

**Note:** Slide 16 will identify exactly what is expected to be included here.

**Table 1 – USB Devices Connected to [Hostname]**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Device Name** | **Serial Number** | **User Account** | **First Time** | **Last Time** |
| Vendor/Make/Model | 123456789ABCD | johnsmith | 4/3/18 | 4/6/18 |

[Note: I typically remove timestamps for policy violations, but for legal and malware cases these are may be important. The idea is to keep the tables clean and report the relevant information for sanctions or appropriate action. This table can be used for shell items and prefetch as well. The amount of columns and their titles will clearly change.]

**APPLICATION ANALYSIS**

[Note what applications were downloaded, installed, and executed if they are relevant to a malware investigation or the policy violation being investigated. Were any applications uninstalled from the system in attempt to remove evidence?]

**PREFETCH ANALYSIS**

[Identify any programs executed, the number of times, the first time and last time of execution. Include a table that shows ONLY the rows that are important to your investigation. If there are more than 10 rows, this table must be moved to an appendix. Make sure the table is labeled and formatted, similar to the USB device table above.

**Table X – Prefetch Analysis for [System Name]**

|  |  |  |  |
| --- | --- | --- | --- |
| **Application Name** | **Times Ran** | **First Time** | **Last Time** |
|  |  |  |  |

**[Here you may also include the userassist and shimcache analysis results in a table or a figure. Explain any important findings in the narrative and these sections should have their own heading, similar to the PREFETCH heading.]**

**USERASSIST**

Identify any programs executed by each user. If this is explained under application analysis – skip this.

|  |  |  |  |
| --- | --- | --- | --- |
| **User Account** | **Application File** | **Times Ran** | **Last Time** |
|  |  |  |  |

**SHELL ITEM ANALYSIS**

[Here you want a table to shellbags, LNK files, and jump lists that are relevant to your case. If there are items unrelated to the policy violation or crime, remove them entirely or add the full list as an Appendix if there are more than 10. Identify for each files that were accessed, the first and last access or open dates, the filenames of interest and where these files are located.]

**Table X – Shellbag Analysis for [Hostname]**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Filename** | **Location** | **User Account** | **Created Time** | **Modified Time** |
|  |  |  |  |  |

**Table X – Jump List Analysis for [Hostname]**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Filename** | **MRU** | **AppId** | **User**  **Account** | **Source**  **Created (First)** | **Source**  **Modified (Last)** |
|  |  |  |  |  |  |

**Table X – LNK File Analysis for [Hostname]**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Filename** | **Location** | **User Account** | **Source Created (First)** | **Source Modified (Last)** |
|  |  |  |  |  |

[These tables can be made yourself or be formatted after being output from a tool, which is easier.]

**ACTIVITY TIMELINE**

[Here is where students imitate a forensic analysis case that includes a high-level bulleted list of events in chronological order that highlight case or system actions that are relevant for the investigator.]

[List at least 10-15 bullet points that highlight user actions that relate to the initial case questions and include dates and times wherever possible.]

* 12 November 2021 1400 malicious file <malicious.exe> was downloaded to host FOR12345
* 14 November 2021 1650 a word document sensitive.doc was opened on the system
* 17 November 2021 at 1717 a relevant case file was first created in the local Dropbox folder

**CLOUD FORENSIC ANALYSIS**

[For CS3 list the 7 cloud service folders using copy and paste functions or screenshots (5 cloud services; two have two different subfolders). Also list the table of case-specific software installed, including the versions of software installed. Take screenshots of the folders and their file content, label the screenshots, and complete a narrative that highlights important actions based on filenames and timestamps.]

**USER ACTIVITY**

[List the files that are specific for the case, including their relevance to the case, their created and modified timestamps and what they imply, and take screenshots of the file’s contents when the files apply to the case to show intent, premeditation, and supporting evidence that might help an investigator. Also include any related metadata when relevant. Make sure you include AT LEAST the 5 files covered during the session. This would include user files in the Recycle Bin, Documents, Downloads and Desktop folders]

**MALWARE ANALYSIS** (Not in CS3)

[This section is used to identify any malicious applications identified on the system and may have some data similar to the prefetch section above. This is where you follow the basic malware triage steps and is not required for the case project, but can be extra credit. If you run anti-virus against a mounted drive, or your local antivirus engine identifies malware, make sure you identify the source file as well as the virus name identified by the antivirus vendor.]

[Also note any hashes, screenshots, or tables of the malicious program. This program could be adware, spyware, or malware in general. Identify any open source information about the malware and its capabilities. Review the section headers using tools similar to PEiD. Perform any static analysis to quickly triage the malware and recommend that the system be wiped. You may perform dynamic analysis or reverse engineer the malware if you think this is appropriate for the case to create IOCs. This is not done for general crimeware or spyware often.]

**[INCLUDE OTHER SECTIONS AS NECESSARY OR DESIRED]**

[Examples include deleted files, items in the Recycle.Bin, items that were downloaded to the system and if they were executed or malicious, they may be listed above. A list of specific documents or share access may also be highlighted. Somewhere in the report, e-mail addresses should be identified that could be avenues of misuse.]

**CONCLUSION**

[Here you will wrap up the case and draw conclusions. Did you verify there was a policy violation or law broken? Was there an infection or compromise caused by user action/interaction? Where is the largest risk of data loss or exfiltration?

Summarize the evidence you found. Where are the files of interest? What conclusions can you make about the evidence? Answer the initial questions asked of you by your manager, chief security officer, or legal counsel.

Finally, make recommendations. Note how the case be handled as a result of what was discovered during the exam? Should the user receive additional security training, a reprimand, or some form of administrative hearing? Should the suspect be charged civilly or criminally? Also, make sure you note any additional questions you believe the suspect should be asked by law enforcement or corporate investigators. Should we ask about the whereabouts for a specific device? Should we identify other systems or mobile devices, should we review corporate e-mail? This can be a bulleted list where you recommend actions be taken that may further your case and investigation.]

**TOOLS**

[Here I list the tools and version numbers used throughout the report. This allows other examiners to verify my work and determine what conclusions may have been drawn incorrectly due to the tool itself. This is a best practice to ensure the tool versions are at least in the body of the report.]

Access Data Forensic Toolkit (FTK) v6.4

Access Data FTK Imager v3.4.2.6

Registry Ripper v2.8

Autopsy v4.6.0

**Eric Zimmerman’s tools and version numbers**

**USBDeviceForensics v.X.X.X**