Practical laboratory exercise – Forensic analysis of Windows Registry

Instructions

In order to maintain the continuity of the laboratory exercise, it is advisable to follow the individual steps. However, this requirement is for guidance only. There are several tasks in each step, and you should answer all the questions or do all the subtasks that are part of these tasks to complete them. If you find some task difficult or unsolvable, you can look at the correct answer sheet that will be present with each task.

Correct answers can be found on the following link (https://github.com/57972887/LaboratoryExerciseWR/blob/master/Documents/Correct%20Answers/Correct_answers.md).

Assignment

In recent days, a threat has emerged on the Internet that a group of attackers will attack the international company Health Worldwide. The goal of this attack is to extract as much sensitive data as possible and later misuse it. Today, the team of the special unit managed to track down and arrest one of the potential attackers. When the special unit marched in, the attacker was behind his PC and as he saw them, he tried to escape, but unsuccessfully.

After the arrest, forensic technicians inspected the crime scene and extracted a disk image from the mentioned PC. In the initial analysis, they found that all information about the attack is probably in a password-protected .zip file. A brute-force attack was used to decipher the password, but since the password can be quite long and can consist of various characters, there is nothing left but to look at some hints or the password itself in the acquired disk image. Your forensic team asks you to try to look at the disk image and found the mentioned password (possibly extract and document all the findings from the image and also from the mentioned .zip file).

Now you are a crucial part of your forensic team, do not forget to use hash functions to preserve integrity, note everything (create output report file) and use chain of custody, if you find any evidence.

Hash function value calculated on the .zip file == a86ab54314fa4670563c6570f398a0a1a23c39b9f51b6acfe094b2f565f284d5.

STEP 01 – Basics

In this step, your task is to verify the disk image, find out information about the partition table, mount the disk image correctly, extract the hive files from the disk image and run program RegRipper against all the hives. Note all things along the way!

1. **Unzip the given .zip file.**
    - Based on the provided hash value, verify what kind of hash function it is and whether the hash value calculated by you matches the provided.
    - How many files does this .zip file contain?
    - In what format was the disk image taken?
    - Who took that disk image, when was the image taken, note also the case number?
2. **Mounting the image and file system analysis.**
    - What file system was the attacker using?
    - Find out information about Partition table (e.g. number of partitions, size of the individual partitions and any useful information for the next part).
    - What commands did you use to mount the given disk image?
    - How many created users does this disk image contain (do not count Administrator or Guest)?
    - Do not forget all the necessary options when mounting!!!
3. **Extract hive files from the disk image.**
    - Find the individual hives and extract them to your case directory.
    - How many hive files did you extract?
    - How to preserve the integrity of these hive files? Calculate what is necessary and create output file with those values.
4. **With the help of RegRipper create output files for every hive file you extracted.**
    - Create multiple output .txt files with findings from every extracted hive file. If you do not know how to use program RegRipper in SIFT workstation, see the following link (https://github.com/57972887/LaboratoryExerciseWR/blob/master/Documents/Manuals/Necessary%20Tools.md).

STEP 02 - Basic analysis of the subject

Your forensic team needs a basic analysis of the operating system. Use the output files from the previous step as the main source of your information.

For this STEP you can use vim and the search option. But you should know where to find required information.

1. **Extract specific data about operating system listed below.**
    - Computer name.
    - Information about time zone.
    - Last Shutdown time.

- Information about environment (Processor architecture, Number of processors).
- Product name, installation time and date, release ID.

2. **Find information about user.**
    - What username did the user used? What RID and SID is bound to this username?
    - When was the account created?
    - Is there any password hint?
3. **Identify right keys/values that contain information about processes and network.**
    - Identify the services that updated the browser Microsoft Edge, extract the timestamp and the name of the .exe file (create new file if necessary and use the appropriate plugin).
    - Are there any processes, which are executed at system start-up? List them all.
    - Identify the network cards and default gateway MAC address with timestamps.
    - Search for DHCP server and DNS IP addresses.
4. **Analyze all mounted devices, which were attached to the system.**
    - Look for Portable devices and analyze all devices under this key. Note the Device description and device name.
    - Now search for mounted devices. Can you find some similarity between the devices in this list according to the extracted device description. Which drive letter was assigned to this device?
    - Based on the name of the device, find the first installation date, last arrival date and last removal date.

After a basic analysis, the essential thing comes to mind. The detainee refuses to testify, even laughing at our unit and revealing that the password-protected .zip file should really contain information about their planned attack, but he himself is sure that we will not decrypt the file in time.

However, the interrogator noticed that the suspect often used the number 4, maybe it's just a coincidence, but if you can figure out what that number should represent, maybe the whole case would be easier for us to approach.

STEP 03 – Recently opened documents.

If you've already looked at the data on the mounted drive, you may have noticed that there is a huge tree structure on the desktop. Maybe this is where the attacker hid his password. Extract useful information from the output file that you obtained from the individual hive files.

1. **Navigate yourself to the tree structure. In what format are files in the tree structure? What type of characters do folder names contain?**
2. **What is the last opened .txt file? Note also the LastWrite time.**
3. **Based on the Last Write time, try to find directory with the help of ShellBags.**
4. **How many clues are hidden in the given disk image?**
5. **What is the first clue?**

STEP 04 – Pictures

We know it's not much, but a colleague from another forensic team advised us that one perpetrator hid a lot of information in the pictures. Try to analyze the last opened images/pictures, but beware that essential information may also be hidden in the image metadata.

1. **Analyze recently opened pictures. Maybe the user used some Windows based programs to open those pictures.**
2. **Use the right tools to extract extra information about each picture.**
3. **What is the second clue?**

STEP 05 – Paths that the user searched for

The next step would be to analyze the keys that the user activity created in the sense when e.g. he searched for something and entered input from the keyboard.

1. **What keys/values could contain such information?**
2. **Analyze suspicious files.**
3. **Did you find the third clue?**
4. **Where can it be?**
5. **What is the third clue?**

STEP 06 – Executable files

Looks like we are pretty close to finding the password, now try to analyze .exe files with the help of Shimcache. If necessary, create new output file with findings from just one plugin.

1. **According to the detected key, extract data from the appropriate hive file, which you can further investigate or filter.**
2. **Analyze the suspicious .exe file. Analyze the source code, is there any file that this program works with.**
3. **What format does this file have?**
4. **What is the fourth clue?**

STEP 07 – Find the password

Based on the indications provided, find out what the password of the .zip file is and try to use it.

1. **What is the password?**
2. **Did it work?**

STEP 08 – Analyze the .zip file

Hooray, you did it! You saved us a lot of time by finding that password. However, the work is not finished yet, please analyze the contents of the .zip file and determine, what is the target of these attackers.

1. **What did you find in this .zip file? List all files.**
2. **What is the real target of those attackers?**
3. **How many attackers were to take part in this attack? Note also names/nicknames.**
4. **To which country they wanted to flee after the attack.**