Correct Answers

STEP 01 – Basics

1. **Unzip the given .zip file.**
   - Given value is 32 byte long (64 characters in hex format) and based on following link https://en.wikipedia.org/wiki/List_of_hash_functions it could be GOST, BLAKE-256 or SHA-256. You can try them all and by comparing the hash values, you will find out that the SHA-256 was used (command *shasum256*).
   - Unzip the file with the command *unzip* and count unziped files. The .zip file contains 21 files.
   - By the extensions (.E0*) you can guess that it is EWF or Expert Witness Format.
   - Since this is an expert witness format, we can use the *ewfinfo* command to find out information about the analyst, the time of acquiring the image and the case number. (**Joe Taylor, 2021-04-26 12:42, 110**)
   - Do not forget command *ewfverify* to verify the disk image.
2. **Mounting the image and file system analysis.**
   - *ewfmount case_110.E* /mnt/ewf*
   - *mmls /mnt/ewf/ewf1* – There are overall 3 partitions allocated 2x NTFS/exFAT and 1x Unknown Type. If we want the size of partitions in bytes, we will have convert the Length value (e.g. second partition Length == 61 767 508, Size of partition == 61 767 508 * 512 == 31 624 964 096 bytes == 30 GB).
   - *kpartx –av /mnt/ewf/ewf1* – Create loop device/s (based on number of partitions).
   - *fsstat /dev/mapper/loop19p2* **–** Identify the file system type, OEM Name, Version. We will mainly deal with the second partition, as it is the most extensive and contains the most information (NOTE – in your own interest you can also analyze other partitions, but it is unnecessary for this exercise). **(NTFS, NTFS, Windows XP)**
   - *mount.ntfs –o ro,noexec,show_sys_files,streams_interface=windows /dev/mapper/loop19p2 /mnt/windows_mount* – Mounting the image on mount-point /mnt/windows_mount
   - Used commands - *ewfmount, kpartx, mount.ntfs*
   - Command *ls /mnt/windows_mount/Users* and count them, there is only one. (**unit2**)
3. **Extract hive files from the disk image.**
   - SYSTEM, SAM, SECURITY, SOFTWARE at /Windows/System32/config/
   - AMCACHE at /Windows/appcompat/Programs
   - NTUSER.DAT at /Users/unit2
   - USERCLASS.DAT /Users/unit2/AppData/Local/Microsoft/Windows
   - Command *cp* (copy) should be used to extract hive files (e.g. cp /mnt/windows_mnout/Windows/System32/config/SAM /destination/path/).
   - Number of hive files == 7.
   - Use sha256sum and calculate hash values of each extracted hive file. List of the sha256 values can be found on the following link (https://github.com/57972887/LaboratoryExerciseWR/blob/master/Documents/Hash%20Values.md).
4. **With the help of RegRipper create output files for every hive file you extracted.**
   - Example - *rip.pl –r SYSTEM –a > outputSYSTEM.txt* (same for other hive files) or you can use some fancy for-each statement.

STEP 02 - Basic analysis of the subject

1. **Extract specific data about operating system listed below.**
   - Computer name == DESKTOP-ATTCK-2 (SYSTEM)
   - Information about time zone == GMT STANDARD TIME. (SYSTEM)
   - Last Shutdown time == 2021-04-26 12:18. (SYSTEM)
   - Information about environment. Processor architecture == AMD64, Number of processors == 4. (SYSTEM)
   - Product Name == Windows 10 Home
   - Time == 17:03 date == 2021-04-11
   - registered owner == unit278865@gmail.com
   - Release ID = 2009. (SOFTWARE)
2. **Find information about user.**
   - Username == unit2
   - RID == 1001
   - SID == S-1-5-21-356729664-2683980348-2657983267-1001 (SAM, SOFTWARE)
   - No password hint. (SAM)
   - The account was created 2021-04-11, 17:10. (SAM)
3. **Identify right keys/values that contain information about processes and network.**
   - Timestamp == 2020-11-18 23:31, Name of the program == MicrosoftEdgeUpdate.exe (SYSTEM)
   - At system start-up - Run == firefox.exe, OneDrive.exe, SecurityHealthSystray.exe, VBoxTray.exe (NTUSER.DAT, SOFTWARE)
   - Card == Intel(R) PRO/1000 MT Desktop Adapter Timestamp == 2021-04-11 18:00 (SOFTWARE)
   - MAC == 52-54-00-12-35-02 type == wired (SOFTWARE)
   - DHCP server IP address == 10.0.2.2 (SYSTEM)
   - DNS IP address== 8.8.8.8 (SYSTEM)
4. **Analyze all mounted devices, which were attached to the system.**
   - Description == DISK&VEN_&PROD_USB_DISK_2.0&REV_PMAP, Name == USB_JS (SOFTWARE)
   - Search for MountedDevices and find the similarity. Drive letter == E. (SYSTEM)
   - Search for USB_JS (2021-04-24 17:29, 2021-04-24 18:36, 2021-04-24 18:47) (SYSTEM)

STEP 03 – Recently opened documents.

1. Find the tree structure on Desktop ls */mnt/windows_mount/Users/unit2/Desktop/New Folder.* Files in the tree structure are in .txt format. Folder names contain only numbers.
2. Name of the last opened file == txtfile.txt. LastWrite time == 2021-04-26 12:18 (NTUSER.DAT)
3. Use the output file from Usrclass.dat and search for the LastWrite time. Identify the right Directory (*11/13*) and extract the information with command *cat /mnt/windows_mount/Users/unit2/Desktop/New Folder/11/13/txtfile.txt*
4. It seems like there are overall 4 clues**.**
5. The first clue == "The password is 30 characters long".

STEP 04 – Pictures

1. If you use RecentDocs there are few images to analyze (.jpg or .png) but without paths. The best way is to try key Applets, there is a whole list of pictures with the paths. (NTUSER.DAT)
2. Analyze those pictures with exiftool/xxd/strings, one of them is trying to hide something.
3. The second clue == "The password consists of 8 numbers, 15 capital letters, 5 lowercase letters and 2 commas"

STEP 05 – Paths that the user searched for

1. Keys TypedPaths, TypedURLs could contain such information. (NTUSER.DAT)
2. From TypedPaths we can get several paths, we have to find suspicious files at the end of each listed path. The file you have to search for is on the path *C:\Program Files (x86)\Common Files\Micro Services\New folder\Info.txt*
3. This file does not contain the clue, but it is hidden inside the ADS. Command *getfattr –n ntfs.streams.list Info.txt*. Get the stream name ("hidden"). Use *cat Info.txt:hidden* to extract third clue.
4. The third clue == "SHA-128 value of the password is F92AEE50CFD6392E1CFF81EEA7FE8E04AA8CE03A"

STEP 06 – Executable files

1. Use only plugin shimcache on the SYSTEM hive file (rip.pl –r SYSTEM –p shimcache). After that you should use command *grep* and filter out all the unnecessary data. There will be few .exe files at the end, but the one you should search for is on the path *C:\Users\unit2\Dekstop\Programs\RT009.exe.*
2. Luckily the source code is also here. Analyze the source code and find the right file. Path to the file is *C:\Program Files\Wallpapers\RT008\ktamem.dll*.
3. Name of the file suggests that it is .dll file, but if you look into the binary format, it is very suspicious. Use command *strings –n 1 ktamem.dll* and find the final clue.
4. The fourth clue == "Password is the Windows Registry, Hive file == SOFTWARE".

STEP 07 – Find the password

1. So, we know that the string values in Windows Registry are encoded in UTF-16. We also know all clues and before writing excellent grep command, we can try to use sha1sum. Something like this: *strings --encoding=l -n 30 SOFTWARE | grep ',' | while read line; do echo $line >> out.txt; echo -n $line | sha1sum >> out.txt; done* and after this one-liner just search for the SHA1 value. The password above is the right one.
2. The right password is **“**BFAWKHBRKW7165JWIPO,qemqa9973,”

STEP 08 – Analyze the .zip file

1. There were several files in this password-protected .zip file **-** building_plan.jpg, Plan.txt, Team.txt and Threat.txt
2. The real target is the military organization ARM.
3. Based on the Team.txt file, there could be 5 or more attackers. (Names – Jack, John, Mark, Eliot, Samantha)
4. After the attack the team wanted to flee to Argentina.