WINDOWS LIVE INCIDENT RESPONSE

SOFIA SACKETT CFRS 660 SPRING 2020

I. BEFORE YOU BEGIN

1. Prepare removable media
   a. Download cmd.exe and the en-US folder from C:\Windows\System32
   b. Download FTK Imager from https://accessdata.com/product-download/ftk-imager-version-4-2-1 and follow instructions
   c. Create a folder for all imaging and data collection (such as Cases > 001 > Collection)
   d. On the suspect device, insert removable media and determine which drive letter Windows has assigned to your device. We will assume drive K: for this tutorial.

2. Launch a trusted command shell from the Windows Start Menu by typing “cmd.exe” and either clicking “Run as administrator” on the rightmost pane or right-clicking on cmd.exe and choosing “Run as administrator”.

II. SYSTEM INFORMATION

3. Record the system date and time as well as actual date and time.
   a. From command line, record the system date with the command **date > k:\Cases\001\Collection\datetime.txt**
   b. Record system time by appending the datetime.txt file with the command **time >> k:\Cases\001\Collection\datetime.txt**
   c. Also, record the system time zone with **tzutil /g >> k:\Cases\001\Collection\datetime.txt**
   d. Finally, record the actual date, time, and timezone using a watch

4. Determine who is currently logged on and other system information.
   a. Record the username of the current user with **echo %username% > k:\Cases\001\Collection\userinfo.txt**
   b. Show all users on the system with **net users >> k:\Cases\001\Collection\userinfo.txt**
   c. Then, find more information about each user (user1 for example) by executing **net users user1 >> k:\Cases\001\Collection\userinfo.txt**
   d. Finally, collect general system information with **systeminfo > k:\Cases\001\Collection\sysinfo.txt**

III. DIR, PORTS, & IPCONFIG

5. Record the modified, created, and accessed times of all files on the suspect machine.
   a. To find the last modified time, execute **dir /t:w /a /s /o:d c:\ > k:\Cases\001\Collection\modifiedDirectory.txt** (If the directory is located in a different drive, replace c:\ with the letter of the correct drive)
   b. To find the created time, execute **dir /t:c /a /s /o:d c:\ > k:\Cases\001\Collection\modifiedDirectory.txt**
   c. To find the last accessed time, execute **dir /t:a /a /s /o:d c:\ > k:\Cases\001\Collection\modDirectory.txt**

6. Determine which ports are open and listening.
   a. Execute **netstat -anob > k:\Cases\001\Collection\open_ports.txt** to find all open ports and their associated apps
   b. Display the routing table in numerical form with **netstat -rn > k:\Cases\001\Collection\routing.txt**

7. Determine IP configuration and the DNS Resolver Cache.
   a. To show full IP configuration information, execute **ipconfig /all > k:\Cases\001\Collection\ipconfig.txt**
   b. Save the DNS Resolver Cache with **ipconfig /displaydns > k:\Cases\001\Collection\dns.txt**

IV. PROCESSES & FILES

8. Record a list of running processes.
   a. Output services being hosted for each running process, run **tasklist /svc >> k:\Cases\001\Collection\service.txt**
   b. To show verbose task information, execute **tasklist /v >> k:\Cases\001\Collection\tasklist_verbose.txt**

9. Output the processes and services to a table using the Windows Management Instrumentation Command Line.
   a. Execute **wmic**
   b. Run **/output:"k:\Cases\001\Collection\proc.html" process list full /FORMAT :htable** to output processes
   c. To save a table of currently running services, run **/output:"k:\Cases\001\Collection\service.html" service list full /FORMAT :htable**

10. Press **Ctrl-C** to exit wmic. Execute the following command to list all open files: **net file > k:\Cases\001\Collection\file.txt**

V. SYSTEM INFORMATION

11. Output the ARP cache and the netBIOS connections
   a. Display the arp cache with **arp -a > k:\Cases\001\Collection\arpcache.txt**
   b. Save netBIOS connections with **nbtstat -cns > k:\Cases\001\Collection\netBIOS.txt**

12. Collect scheduled tasks and started Windows services.
   a. Execute **schtasks /Query /fo list /v > k:\Cases\001\Collection\schtasks.txt** to display all scheduled tasks
   b. Use **net start > k:\Cases\001\Collection\start.txt** to show Windows services

13. Save event logs and driver configuration information.
   a. To save the event logs, run **wevtutil el > k:\Cases\001\Collection\eventlogs.txt**
   b. To collect all driver information, execute **driverquery /FO csv /si > k:\Cases\001\Collection\drivers.txt**

14. Record the system and actual date and time (Ref. Step 3).

15. Record all commands used with **doskey /history > k:\Cases\001\Collection\history.txt**

16. Capture memory with Access Data’s FTK Imager.
   a. Open FTK Imager from the trusted removable media
   b. Click “File” → “Capture Memory”
   c. Next to the Destination Path field, click “Browse” and save the image to k:\Cases\001\Collection
   d. Choose a relevant filename, such as Win10x64.mem
   e. Click “Capture Memory”

LINUX LIVE INCIDENT RESPONSE

SOFIA SACKETT CFRS 660 SPRING 2020

I. BEFORE YOU BEGIN

1. Launch a trusted command shell and enter command **sudo su** to gain administrator privileges.
2. If Linux does not mount your removable media (complete with all forensic tools) automatically, execute **mount** followed by your device and mount point, such **mount /dev/cdrom /mnt/cdrom**
   a. **cd** into the mounted device root directory
   a. Create a folder for all data collection with the command **mkdir /hda1/Case001**, where hda1 is the name of the removable media

II. SYSTEM INFORMATION

3. Record the system date and time as well as actual date and time.
   a. From command line, record the system date, time, and timezone with the command ./**date > /hda1/Case001/datetime.txt**
   b. Finally, record the actual date, time, and timezone using a watch
4. Record the username of the current user with ./**w > /hda1/Case001/user.txt**
5. Collect OS information with ./**uname –a > /hda1/Case001/os.txt**

III. FORENSIC INFO

6. Record all recent connections with **./ip route list > /hda1/Case001/connections.txt**
7. Collect arp cache information by executing command **arp –a > /hda1/Case001/arp.txt**
8. Find all scheduled tasks with the command **crontab -1 > /hda1/Case001/tasks.txt**
9. Display all successful logins with the command **./last > /hda1/Case001/successful_login.txt**
10. Display bad logins with **./lastb > /hda1/Case001/bad_login.txt**
11. Record open ports and the name of application with process ID using **./netstat –anp > /hda1/Case001/open_ports.txt**
12. Collect Kernel Loaded Modules with **./lsmod > /hda1/Case001/connections.txt**
13. Collect all running processes with **./ps –ef > /hda1/Case001/proc.txt**
14. List all of the mounted file systems with **./mount > /hda1/Case001/mounted.txt**
15. Record all IP configuration information with **./ifconfig –a > /hda1/Case001/ifconfig.txt**

IV. MAC TIMES AND LOGS

16. Record modification and access times of all files
    a. From the root directory, list access time with **./ls –alRu / > /hda1/Case001/accesstime.txt**
    b. Next, list the inode modification time of all files in the root directory with the command **./ls –alRc > /hda1/Case001/inode_mod.txt.**
    c. Finally, record the last modified time of all files with the command **./ls –alR / > modified.txt**
17. List and output all log files
    a. First, **cd /var/log**
    b. Execute **ls > /hda1/Case001/logs.txt**

V. WRAP-UP

18. **cd** back into the root folder and check if any files are in promiscuous mode with the command **netstat -i**. Any 'P's in the Flg column could be indicative of network sniffers. Take note!
19. Record the date and time once again with **date >> /hda1/Case001/datetime.txt** and the help of a watch
20. Record all commands used with **./history > /hda1/Case001/history.txt**

VI. MEMORY

21. Download LiME from https://github.com/504ensicsLabs/LiME onto your forensic workstation
22. Build LiME according to the suspect computer's kernel version using command **uname -a** on the suspect computer
23. Unzip the LiME zip file you downloaded and change the directory to LiME-master/src with **make -C /lib/modules/3.13.04-34-generic/build M=$PWD**, replacing 3.13.04-34-generic with the name of your kernel version. Now you should have a lime.ko file in the src directory
24. Copy the kernel module (lime.ko file) to your external drive and plug it into the suspect machine. The drive should be mounted automatically.
25. **cd** into your external drive (in this case, hda1)
26. Create a memory image with **insmod lime-3.13.04-34-generic.ko "path=/media/hda1/Case001/memory.lime format=lime"**, replacing lime-3.13.04-34-generic.ko with the name of your kernel module.