Assignment 3 Forensics By Kevin Harianto

In-Class Lab 8

Installed and validated Logstash and the compatible JVM.

Text

Description automatically generated

Graphical user interface, text, application, email

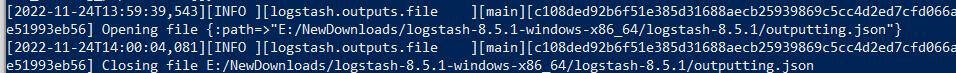
Description automatically generated

^created configuration file for logstash to run from which will inport the log file and export as a JSON file

Text

Description automatically generated with medium confidence

…



^running logstash and closing the JSON file

Text

Description automatically generated

^exported file as JSON.

(Script from splunk to read the json file created earlier to print the specified fields)

Text

Description automatically generated

^Setting and adding data displaying the fields included

Graphical user interface, text

Description automatically generated with medium confidence

^Searching through the parsed JSON data.

Graphical user interface, text, application, email

Description automatically generated

^note when expanded it shows the variables and its values

Lab 9

1.The PID of wc.exe is 364.

A picture containing text

Description automatically generated

Text

Description automatically generated

^Used the filter pslist as it would showcase all of the processes and their process ID.

2. the amount of DLL files is 24 in total.

Text

Description automatically generated

^used dllist to find the dll files and I counted the lines through piping to grep in which it started in the memory as so it would improve accuracy as all the dll files started with 0 representing the address.

3. the username of the non-default user account is callb

Text

Description automatically generated



^used the command envars to show where all the environments and variables are and this includes the username.

4. the machine’s IP address is 127.16.150.20

Text

Description automatically generated

^used connscan to scan the local address of the host pc to get the machine’s IP address.

5. the IP address of the web server that was connected to port 80 is 58.67.132.141

Text

Description automatically generated



^used connscan to scan the IP’s for anything that the machine has connected with to get to the web server, and found out that in port 80 the Machine has connected to the remote address of 58.64.132.141 representing the web server.

6. the URL in the current user’s clipboard is <http://58.64.132.8/download/Symantec-1.43-1.exe>

Text

Description automatically generated

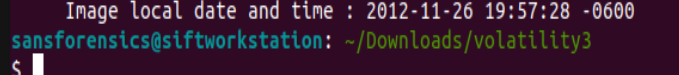


^used the command clipboard in order to look into what the user copied as well as what site that the user copied which the question asked for.

7. the clock says 7:57pm

Text

Description automatically generated



^I used the filter imageinfo to obtain the time in which the Machine’s image was taken

8. the windows domain that is the computer one is windows XP in system32.

Text

Description automatically generated



^I used imageinfo to take in what profile the host was on, as the suggested profile gives an insite to what the OS is that the machine was running on.

9. the cached domain authentication hashes available are 500:b7ae6225a35c376da8 …(in screenshot)

Text

Description automatically generated

^I used the filter hashdump in order to get the authentication hases

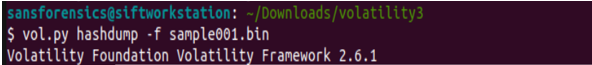
and

Text

Description automatically generated

^This includes the passwords for the domain authentications such as getting support as well as the backup password.

10. The Local password hashes for non-domain users is (in screenshot)





^Used Hashdump as it showcases the password hashes for guest accounts as well which are non-domain users.

11. the amount of open file handles pointing to files with three letter extensins are 103.

Text

Description automatically generated

^this is due to how processes always point to three letter extensions as they are executables and we just need to count the amount of executables. Handles also shows all the handles pointing to the files.

12. the two websites are windows explorer home, and Symantec’s download page.

Text

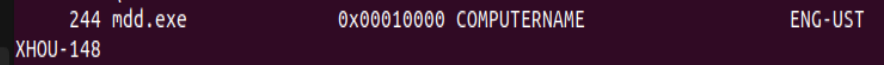
Description automatically generated

^timeliner shows the timeline of the machine’s activity as well as we are looking into the two websites so we set the type to the internet’s history.

13. the machine’s name is ENG-USTXHOU-148

Text

Description automatically generated



^Used the filter envars as the variables which includes the computer system and it’s name is included.

14. the amount of entries in the security event log is 0. Proof of why this is the case is shown in screenshot as it parsed through all security events

Text

Description automatically generated

^Used the filter evtlogs to extract all of the event logs, this includes the security event logs and saved to an output to read for any entries. This is done by counting the amount of lines extracted, thus providing proof that there were no entries in the security event logs.

15. The name of the most recently started scheduled task is lsass as it checks the security for authentication and other related means.

Calendar

Description automatically generated

^with how services.exe and lsass running right after showing how it was the most recently scheduled task set from the windows services utility. And the pslist showing the connected processes that occure sequentially.

16. mdd.exe was copied from windows explorer as the Parent process ID leads to there.

Text

Description automatically generated

Calendar

Description automatically generated

^using the filter pslist as we are able to backtrack through the processes that occurred to find where mdd.exe was obtained from through its connection with its parent process ID.

17. The year and month that Windows Update last run was at 2012 November the 3rd.

Text

Description automatically generated

Text

Description automatically generated

^utilized the filter printkey to open up what the current version is on the machine’s system.

Text

Description automatically generated

^paging file is already configured. This is shown in the imageinfo as it shows overall information on the image itself as well as whether or not the paging file was configured.

4)Creating a dump file

Graphical user interface, text, application

Description automatically generated

^Using notMyFault a tool learned in class to generate crash dump file.

Graphical user interface, application, table

Description automatically generated

^location of the dump file for extraction in SIFT VM

Text

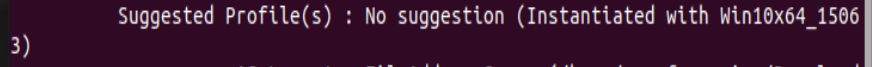
Description automatically generated

^shared the dump file for analysis

5)found the matching profile of windows VM as it is matching due to how the VM is a Windows 10 instance.

Text

Description automatically generated



6)extract list of all processes.

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

(SHOWCASEING TRIES AND THAT DESPITE CREATING A COMPLETE MEMORY DUMP FILE USING EASILY AVAILABLE TOOLS THE FOLLOWING PROCEDURES AND MULTIPLE DIFFERENT WAYS OF EXTRACTING THE PROCESSES COULD NOT BE COMPLETED)Despite using the proper tools for creating the memory dump file for analysis none of the processes could be extracted for analysis using volatility.

7. I am letting you know that I cant copy or move the pagefile.sys for analysis despite it being in a VM. this is because of how pagefile.sys is constantly being used and despite pausing and restarting the vm the .sys file is still in use and I cant copy it or analyze in volatility using the same mounted folder.

Graphical user interface, table

Description automatically generated

^This can be showcased with how despite sharing the folder directly connected to the sys file even after pausing and restarting the windows VM, the pagefile.sys is still being used and unable to be transported for analysis by the volatility utility.