Forensics

TU856/TU857/TU858 Year 4 - Continuous Assessment 2 (20%)

Due Date: Sunday 1st May 2022 @ 23:59

Introduction

This assignment consists of two tasks in the following areas:

- Network Analysis
- Memory Analysis

Each task carries equal marks.

Task 1 – Network Analysis:

A computer on a company network is suspected of being targeted with a malware attack. The Systems Administrator (Thomas Anderson) has performed a network capture of all devices on the Sales subnetwork. Networks are facing threats more than virus, such as malware, denial of service, port scanning covert channels, and information theft. Detail the steps required to perform a network analysis using a protocol analyser (Wireshark).

Requirements:

You are required to **create a detailed document describing the process to follow in examining a network packet capture** to identify potential malware. Any techniques/methods used should describe their purpose and their use in the forensic investigation. In your answer describe how the different network parameters can be used with Wireshark to help trace network traffic to identify the malware and the host machine.

A packet capture example should be used to complement your answer. (There are a number of example packet captures that are available for practicing forensic skills etc, see Brightspace for more information)

Marking:

- Detailed description of process to follow (65%)
- Packet Capture Explanation (35%)

Task 2 –Memory Analysis:

Analyse the Windows memory image provided. The link to the image is available on Brightspace (~2GB).

Examine the image and answer the following questions. F1 to F6 list the details required for the memory analysis, see grading rubric below for marking details.

- **F1 -** How was the RAM profile identified? What version of the OS is this potentially?
- **F2 -** State how many processes were running at the time. Give the full OS process list.
- **F3 -** How many files were open at the time? How many jpeg files were open at the time?
- **F4 -** What searches appear in the Internet history? What browser was used in the search?
- **F5 -** A file called duck.gif was downloaded. When did this happen? What program do you think was used to open the file? Give reasons for your answer.
- **F6 -** Choose a likely process and dump its memory to a file. Examine the dump with strings. Search for ASCII strings and UTF16 strings. Find something and point it out.

Requirements:

You are required to **create a detailed document describing the process to follow in examining the memory capture**. Any techniques/methods used should describe their purpose and their use in the forensic investigation. In your answer describe how the different memory analysis parameters can be used to identify useful information and content from the image.

You must use screenshots of your terminal window / GUI to document the process followed and the commands/tasks performed.

Hint: The Volatility Framework version 2 would be a good option for this task (https://www.volatilityfoundation.org/)

Marking:

- Detailed description of process to follow for each task performed and its outputs

Grading Rubric:

	70 +	69 – 60	59 – 50	49 – 40	39 - 0
Task 2 Network Analysis Description of the process to follow in examining a network packet capture (65%)	Excellent description of all network analysis techniques using Wireshark in the forensic analysis process. The approach taken and the appropriate network analysis tasks completed with Wireshark have been described in granular detail.	Very good description of all network analysis techniques using Wireshark in the forensic analysis process. The approach taken and the appropriate network analysis tasks completed with Wireshark have been described in good detail. Some minor omissions or more detail/discussion needed.	Good description of the network analysis techniques using Wireshark in the forensic analysis process. The approach taken and the appropriate network analysis tasks completed with Wireshark have been described in good detail. Some noted omissions or more detail/discussion needed.	Good description of the network analysis techniques using Wireshark in the forensic analysis process. The approach taken and the appropriate network analysis tasks completed with Wireshark have been described in good detail. Some noted omissions or more detail/discussion needed.	Major issues with the attempted example of the network analysis using Wireshark and/or the approach taken is acceptable. This could have been described in more detail.
Task 2 Network Analysis Packet capture example (**35%**)	Very detailed description of the network analysis of a pcap file and the process followed to source pertinent information relevant to the forensics investigation.	Detailed description of the network analysis of a pcap file and the process followed to source pertinent information relevant to the forensics investigation. Some minor omissions in the techniques used in this process.	Good description of the network analysis of a pcap file and the process followed to source pertinent information relevant to the forensics investigation. Some noted omissions in the techniques used in this process.	Good description of the network analysis of a pcap file and the process followed to source pertinent information relevant to the forensics investigation. Some noted omissions in the techniques used in this process. Some aspects could have been covered in more detail.	Major issues with the attempted network analysis of a pcap file and/or the techniques used in the assignment. More discussion and/or detail needed.
Task 3 Memory Analysis F1 RAM profile (**10%**)	The process followed to identify the RAM profile has been described in granular detail. The correct version of the OS has been obtained.	The process followed to identify the RAM profile has been described in good detail. The correct version of the OS has been obtained.	The process followed to identify the RAM profile has been described in good detail. The correct version of the OS has been obtained. Some minor issues with the description of the process followed and/or the OS version obtained.	The process followed to identify the RAM profile has been described in reasonable detail. The correct version of the OS has been obtained. Some issues with the description of the process followed and/or the OS version obtained.	Major issues with the attempted description of the techniques to identify the RAM profile. More discussion and/or detail needed.
Task 3 Memory Analysis F2 – OS Process list (**10%**)	The process followed to identify the process list has been described in granular detail.	The process followed to identify the process list has been described in good detail.	The process followed to identify the process list has been described in good detail. Some minor issues with the process followed and/or results obtained.	The process followed to identify the process list has been described in good detail. Some issues with the process followed and the results obtained.	Major issues with the attempted of listing of the process. More discussion and/or detail needed.
Task 3 Memory Analysis F3 – Open Files (**20%**)	The process followed to identify how many files/jpegs were open at the time has been described in granular detail.	The process followed to identify how many files/jpegs were open at the time has been described in good detail.	The process followed to identify how many files/jpegs were open at the time has been described in good detail. Some minor issues with the description of the process followed and/or the results obtained.	The process followed to identify how many files/jpegs were open at the time has been described in good detail. Some issues with the description of the process followed and the results obtained.	Major issues with the attempted description of the techniques to identify the open files / jpegs. More discussion and/or detail needed.
Task 3 Memory Analysis F4 – Searches and Internet browser (**20%**)	The process followed to identify the browser used and search history has been described in granular detail.	The process followed to identify the browser used and search history has been described in good detail.	The process followed to identify the browser used and search history has been described in good detail. Some minor issues with the description of the process followed and/or the results obtained.	The process followed to identify the browser used and search history has been described in good detail. Some issues with the description of the process followed and the results obtained.	Major issues with the attempted description of the techniques to identify the browser used and search history. More discussion and/or detail needed.
Task 3 Memory Analysis	The process followed to identify when duck.gif was downloaded and what this was opened with and has been	The process followed to when duck.gif was downloaded and what this was opened with and has been described in good detail.	The process followed to identify when duck.gif was downloaded and what this was opened with and has been described in good detail. Some minor issues	The process followed to identify when duck.gif was downloaded and what this was opened with and has been described in good detail. Some issues with	Major issues with the attempted description of the techniques to identify when duck.gif was downloaded and

F5 – Info on Duck.gif (**20%**)	described in granular detail.		with the description of the process followed and/or the results obtained.	the description of the process followed and the results obtained.	what this was opened with. More discussion and/or detail needed.
Task 3 Memory Analysis F6 – Process dump and string analysis (**20%**)	The process followed to dump an appropriately file and examine it's ASCII and UTF content has been described in granular detail.	The process followed to dump an appropriately file and examine it's ASCII and UTF content has been described in good detail.	The process followed to dump an appropriately file and examine it's ASCII and UTF content has been described in granular detail. Some minor issues with the description of the process followed and/or the results obtained.	The process followed to dump an appropriately file and examine it's ASCII and UTF content has been described in granular detail. Some issues with the description of the process followed and the results obtained.	Major issues with the attempted description of the techniques to dump an appropriately file and examine it's ASCII and UTF content. More discussion and/or detail needed.