**Studio: Basic Static Analysis (Windows)**

**Overview**

The purpose of this assignment is to practice the skills taught in Chapter 1 of the Sikorski/Honig textbook. In order to simulate realistic malware analysis, you will be given little or no information about the program you are analyzing. The malware and most of the questions in this exercise are taken from Sikorski/Honig.

This document outlines the major steps you will take, and you will fill in answers to the questions asked. There are no restrictions on resources that can be used to complete the assignment. This includes consulting with other students and the instructor. We only ask that you will not share your report with others (outside your group -- you may collaborate on generating the report).

Please use this document as the template of your report, and remember to submit it in .pdf form by the deadline. The assignment will be graded on best effort rather than strict correctness.

**Part 1: Download code samples (potential malware)**

1. Download the sample files from Canvas. These files are taken from the “Practical Malware Analysis” book mentioned above. Please remember to make it a habit not to run any binary even in your local environment when practicing static analysis. Instead, move the files to your safe Windows VM environment (via shared Kali folder and python http server). The password is “infected”. 7-zip is a program for extracting files on Windows if you are in need of one. The recommended workflow is to download the .7z file on your host machine, transfer it to your Windows VM, and extract it in a new folder (importantly, NOT a shared folder, as this will cause permissions/access issues on the files). To extract the file, right-click it and select 7zip->Extract, then provide the password (“infected”) when prompted.

-----------------------------------------------

Answer:

No answer needed for this question.

-----------------------------------------------

2. Prepare to use the following tools to analyze the malware, which should be on your Windows VM as a part of the Flare-VM installation.

(1) A PE viewer tool. The book uses PEview; PE-bear is on the VM and preferred by many. Make sure you can run your selected PE Viewer on your Windows VM. Based on the slides and/or other resources, what does this tool do?

-----------------------------------------------

Answer:

-----------------------------------------------

(2) A packing-detection tool. The book uses PEiD; Detect It Easy (DIE) is on the VM and preferred by many..

Based on the slides and/or other resources, what does this tool do?

-----------------------------------------------

Answer:

-----------------------------------------------

(3) A dependency-analysis tool. The book uses Dependency Walker and this is installed in Flare-VM also; PE-Bear provides some of the same functionality, though not in as much depth.

Based on the slides and/or other resources, what does this tool do?

-----------------------------------------------

Answer:

-----------------------------------------------

**Part 2 – Textbook Lab 1-1**

1. Upload “Lab01-01.exe and Lab01-01.dll” to https://www.VirusTotal.com/ and view the reports.

*Note: you will need network access for your machine to complete this step! For this step, set the “Network” setting of the VM to use a mode that allows network access (first choice: “Nat network” in VirtualBox), and reset the networking preferences inside the Windows VM to use Dynamic IP allocation and DNS services, rather than the static 10.0.0.3 IP address we set up for our malware analysis toolbench. Go ahead and upload all three files from the assignment’s 7zip archive to VirusTotal while you have the network open. Afterwards, remember to switch the network configuration of the machine back to using a local network with static IP addressing, so that the Windows VM cannot access the Internet directly. You may repeat this procedure anytime you wish to upload a sample to VirusTotal from the Windows VM.*

*Alternatively, you can upload the file to VirusTotal from your host machine or Kali, though be VERY careful not to accidentally run any potential malware sample on your host!*

Does one of the files match existing antivirus signatures? Add a screenshot and provide an explanation below:

-----------------------------------------------

Answer:

-----------------------------------------------

2. When was ‘lab01-01.exe’ compiled?

Use the space below to explain where you found this info, and report the compile time.

-----------------------------------------------

Answer:

-----------------------------------------------

3. Use PEiD to determine what tool was used to build the program. What is it? Are there any indications that either of these files is packed or obfuscated? If so, what are these indicators?

-----------------------------------------------

Answer:

-----------------------------------------------

4. Use Dependency Walker to look at the imports and exports in ‘lab01-01.exe’. Do any imports hint at what this program does? If so, which imports are they?

-----------------------------------------------

Answer:

-----------------------------------------------

5. Use Dependency Walker or another tool to look at the imports and exports in ‘Lab01-01.dll’. Does it import the same functions from kernel32.dll? What can you learn from this?

-----------------------------------------------

Answer:

-----------------------------------------------

6. Are there any other files or host-based indicators that you could look for on infected systems?

-----------------------------------------------

Answer:

-----------------------------------------------

7. What network-based indicators could be used to find this malware on infected machines?

-----------------------------------------------

Answer:

-----------------------------------------------

8. When considering all your findings, can you make an educated guess about the purpose of these two files (.exe and .dll)?

-----------------------------------------------

Answer:

-----------------------------------------------

**Part 3 – Textbook Lab 1-2**

In this section, we will analyze Lab01-02.exe.

1. Upload the Lab01-02.exe file to https://www.VirusTotal.com/. Does it match any existing antivirus definitions?

-----------------------------------------------

Answer:

-----------------------------------------------

2. Are there any indications that this file is packed or obfuscated? If so, what are these indicators? If the file is packed, unpack it if possible.

-----------------------------------------------

Answer:

-----------------------------------------------

3. Do any imports hint at this program’s functionality? If so, which imports are they and what do they tell you?

-----------------------------------------------

Answer:

-----------------------------------------------

4. What host- or network-based indicators could be used to identify this malware on infected machines?

-----------------------------------------------

Answer:

-----------------------------------------------