**EXPERIMENT NO. 5**

|  |
| --- |
| **Student Name and Roll Number: Harshit Parashar /18CSU081** |
| **Semester /Section:5TH SEMESTER /CS-V-CSA** |
| **Link to Code:** |
| **Date: 17/9/2020** |
| **Faculty Signature:** |
| **Marks:** |

|  |
| --- |
| **Objective:** Performing the static investigation of any Windows executable binary |
| **Outcome:** Students will learn how to extract static features of a Windows executable binary using a single tool |
| **Problem Statement:** Extract and analyse static features of a Windows executable binary |
| **Background Study:** PeStudio is a free tool performing the static investigation of any Windows executable binary. A file being analyzed with PeStudio is never launched. It supports both 32-bit and 64-bit EXE files. Therefore you can evaluate unknown executable and even malware with no risk. PeStudio runs on any Windows Platform and is fully portable, no installation is required. PeStudio does not change the system or leaves anything behind. Link to download: https://www.winitor.com/ |
| **Algorithm/Flowchart:** |
| **Code(Solution):** |
| **Sample Outputs:**  **Open the PEStudio and drag and drop the window binary,since we are studying malware analysis , we will analyse a malware file**     * **After opening file here in the tool,we saw th e hash has already there and virustotal recognizes this file as malicious**   **It says that 60 out of 71 antivirus recognizes it as a malware**      **Next we saw DOS header**    **Next we saw dos stub**    **Next we saw import dll that has been imported by the malware file,it is containg some important dll such as loadlibrary and getproc address,this symbolises that malware is trying to interact with the system core functionality**    **In libraries section ,it has blacklisted dll as well that means they are harmful**    **PEStudio has indicators also** |
| **Question Bank:**  **Q1. What are different features offered by PEStudio?**  Answer: **PEStudio** is used by many Computer Emergency Response Teams (CERT) worldwide in order to perform:   * Virus Detection * Showing Libraries, Imports and Exports * Resources used by the malware to host payload * Can run as a GUI Tool or a CLI Tool. * Report file documentation * Indicators * Compute entropy * To compute blacklist and whitelist strings * Virustotal score of file * Blacklist signature of resources * Shows first byte of entrypoint   Q2. **State the difference between CFF Explorer and PEStudio.**  Answer : CFF Explorer provides features like file identification, address conversion, dependency scanning, and the ability to add imported functions to a Portable Executable. It is an open source tool while PEStudio determines if a file is malicious based on certain indicators it generates. It offers functionality like hash which is recognized by virustotal.  Q3. **What is the importance of TLS\_callbacks feature to a malware developer?**  Answer: TLS callback functions allow malware developers to execute malicious code before the debugger has a chance to pause at the traditional Entry Point. This allows malware to infect the system or disable the debugger before the analyst has a chance to look at the malware sample's code  Q4**. How significant is TLS\_callbacks feature to a malware analyst?**  Answer: Analysts often examine the malicious program's code by starting with the instructions located at the Entry Point of the executable. The Entry Point is a field in the PE header that stores the address of the "first" instruction in the program that Windows is supposed to execute; debuggers typically take us to that instruction after loading the executable. To bypass the TLS callback defense to debug the program starting from its true beginning of the TLS callback function, configure the debugger to pause on the system entry point, instead of the traditional program entry point. |