OBE December 2021

Date and time of Exam :- 15th Dec. 2021, 9:00AM

Examination Roll Number :- 19234757006

Name of Program :- Master of Computer Application

Semester :- V

Unique Paper Code (UPC) :- 223402501

Title of Paper :- Cyber Security

Name of the Dept. :- Dept. of Computer Science

Email-ID :- anubhav.mca19.du@gmail.com

Mobile No. :- 9044490197

No. of Pages used :- 3

192347570006

(5). (b). o let's assume we have 'Lab01-01.exe and Lab01-01.dll' files, to analyse we will use "www.totalVirus.com". As .dlls can't be run on their own, potentially Lab01-01.exe is used to run Lab01-01.dll.

o When a file is packed, it is more difficult to analyse as it is typically obfuscated and Compressed. Key Indicators that a program is packed, is a Lack of visble 'Strings' or information, or including certain functions such as 'LoadLibrary' or 'GetProcAdress' - used for additional functions. A packed executable has a wrapper - Program which decompresses and runs the file, and when statically analysing a packed program, only the wrapper program is examined.

• PEiD can be used to identify whether a file is packed, as it shows which packer or compiler was used to build the program.

o Investigating the 'imports' is useful in identifying what the malware might do. Imports are function used by a program, but are actually stored in a different program, such as common libraries. Tools like VirusTotal, PEiD or PE Explorer can be used to identify the imports.

- Along with Lab01-01.exe and Lab01-01.dll, there are other ways to identify malicious activity on ifected Systems. Disassembling Lab01-01.exe in PE-Explorer shows us a set of 'Strings' around Kernel32.dll which is supposed to be Kernal32.dll (not kernal23.dll).

- Further investigating the 'strings', however for Lab01-01.dll, it is apparent that there is an IP-address of 127.26.152.13, which could be acting as network-based indicator of malicous activity. (also it is not possible to provide any host or network-based indicator using static analysis without unpacking the files).

(a). - Reverse engineering technique is based on software engineering technique of malware analysis.

It is a process that hackers uses to figure out a program's component and functionalities in order to find vulnerabilities in the program. This process has evolved, as malware has become more sophisticated and detection tools have improved.

- Reverse Engineering Tools :-

1 → Disassembler : A disassembler will take apart an application to produce assembly code. eg - IDA Pro.

19234757006

2 → Debuggers : Reversers uses debuggers to manipulate the execution of a program in order to gain insight into what it is doing when it is running. eg:- x64dbg, WinDbg, GDB

3 → Network Analyzers : They tell an engineer how a program is interacting with other machines including what connections the program is making and what data it is attempting to send.
eg:- Wireshark.

- Advantages and dis-advantages wrt other approaches :-

1. Reverse engineering is an appropriate technique for use in analyzing malware.
2. Static and dynamic analysis methods each have advantages in the process of analyzing malware, then by combining the two methods will be able to provide more accurate results.
3. Each type of malware has its own way of working and threats, therefore malware analysis is an important thing to do in order to find the rigth methods to overcome it.

- The Reverse Engineering process in Software can be implemented with the following steps :-

1. Assembly
2. Dis-assembly
3. Debugging
4. X86 Architecture
5. Instruction
6. Hashing
7. String Analysis