Reg.No. \_\_\_\_\_\_\_\_\_\_\_\_

G:\logo and QP Template\logo 3 Feb 2018 final.tif

**End Semester Examination – Nov/Dec – 2018**

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
| **Code :** | **17CS3076** | **Duration :** | **3hrs** |
| **Sub. Name :** | **BINARY AND MALWARE ANALYSIS** | **Max. marks :** | **100** |

**ANSWER ALL QUESTIONS (5 x 20 = 100 Marks)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Q. No.** | **Sub Div.** | **Questions** | **Course**  **Outcome** | **Marks** |
| 1. | a. | Differentiate the key features of static analysis and dynamic analysis. | CO1 | 10 |
| b. | Examine the format of PE Files with PEview program tool. | CO1 | 10 |
| (OR) | | | | |
| 2. |  | Recognize the C code to construct a assembly code for the following loops and analyze graphically its function using IDA Pro   1. IF statement 2. For statement 3. While statement | CO2 | 20 |
|  |  |  |  |  |
| 3. |  | Illustrate the handling of user-mode calls by the kernel debugging with VMware using WinDbg. | CO2 | 20 |
| (OR) | | | | |
| 4. | a. | Enumerate the two types of disassembler algorithms for linear and flow-oriented. | CO3 | 10 |
| b. | Explain the anti-debugging technique for the instructions:CALL and JMP. | CO3 | 10 |
|  |  |  |  |  |
| 5. |  | Discuss execution of a ‘HELLO WORLD’ code snippet if it is virtual or nonvirtual.  class SimpleClass  {  public:  int x;  void HelloWorld()  {  printf("Hello World\n");  }  };  int \_tmain(intargc, \_TCHAR\* argv[])  {  SimpleClassmyObject;  myObject.HelloWorld();  } | CO4 | 20 |
| (OR) | | | | |
| 6. |  | Demonstrate the usage of (p0f) a passive operating system identification tool.  Inidentify the architecture of the remote system (e.g.,Windows, Linux), version (e.g., 2000, XP, Vista), service pack, and link type of the systemsprobing the honeypot. | CO5 | 20 |
|  |  |  |  |  |
| 7. |  | In November 2006, the authors wrote a research paper on one of the first Zeus variants seen in the wild. During the reverse engineering phase, they loaded the Zeus binary in IDAPro and named as many functions as possible based on their behavior. Zeus stole information from victim computers, compressed it, encrypted it, and sent it over the network to the attackers. Based on the algorithm they saw in the Zeus binary, they wrote a decryption tool to recover the stolen data. However, after a while, the tool stopped working. Clearly,the Zeus authors had updated the code in some way that prevented their old decryption algorithm from working, and they needed to figure out how to fix it. Discuss how to use BinDiff to quickly locate the decryption function and determine exactly how it changed. | CO5 | 20 |
| (OR) | | | | |
| 8. |  | Investigate the development of the C/C++, includes API functions to facilitate in getting your DLL into the memory of the target process, and generate a lot of source code examples forcreating your own programs. How to build an API monitor with Detoursand Microsoft Visual Studio. | CO6 | 20 |
|  | |  |  |  |
|  | | **Compulsory**: |  |  |
| 9. |  | Interpret the reversing of XOR Algorithms in Python that has been obfuscated with XOR for the following the Basic XOR Calculations.   |  |  |  | | --- | --- | --- | | **X** | Y | X^Y | | 0 | 0 | 0 | | 0 | 1 | 1 | | 1 | 0 | 1 | | 1 | 1 | 0 | | CO6 | 20 |