Total No. of Questions : 8] *[Total No. of Printed Pages : 2*

Roll No .....

MTCF-301(C)

M.E./M.Tech. III Semester

Examination, June 2016

Malware Analysis and Reverse Engineering

Time : Three Hours

Maximum Marks : 70

Note : i) Attempt any five questions.
ii) All questions carry equal marks.

1. a) Explain the fundamentals of Malware Analysis.
   b) Discuss Reverse Engineering Malware (REM) methodology.

2. a) Discuss the various key Malware Analysis tools and techniques.
   b) Differentiate between Behavioural analysis and Code Analysis.

3. Explain following terms in detail
   a) Malware Threats
   b) Malware Indicators
   c) Malware Analysis Sandboxes

4. Explain following terms in detail
   a) Internet simulation using INetSim.
   b) Using Deep Freeze to Preserve physical systems
   c) Using MySQL database to Automate FOG Tasks

5. a) What is mean by Malware Forensics? Explain Malware and Kernel Debugging.
   b) Discuss configuration of JIT Debugger for Shellcode Analysis.

6. a) Discuss various WinDbg commands and controls in short.
   b) What do you mean by Reverse IP search, discuss in detail.

7. a) What is Memory Forensics? List out the steps of memory Forensics.
   b) Explain investigating process in Memory Dumps.

8. Write short notes on any two:
   a) Static maps and Interactive Maps
   b) Malware Lab Integrity
   c) Introduction to Python

******