

**IMT CENTRE FOR DISTANCE LEARNING
GHAZIABAD**

Distance Learning Programme

IMT-96

Software Hacking

Notes:

- a. All set of assignments would be made in a single MS. Word file and would be sent together through e-mail to imt.ankitfadia@gmail.com with a cc to nidhimathur@imtc dl.ac.in & richa@imtc dl.ac.in
- b. Subject of the e-mail of assignment submission should be 'UNIT-6'.
- c. Students are required to clearly mention their name, roll no, and subject code in the first page of the word file.
- d. Write answers in your own words as far as possible and refrain from copying from the textbooks/handouts.

ASSIGNMENT QUESTIONS(Subjective) Total Marks = 20 Marks

Complete the following questions:

1. You are a developer at a reputed Internet Security company, your company is about to launch a product in Internet Safety for home users. Design a custom protection scheme that you prefer to be the best way to track piracy at the same time you have to keep your software customer friendly.
2. What are EFLAGS? Give examples. Which EFLAG is of the most use and has priority in assembly analysis of programs in a debugger?
3. How is a DWORD data type different from the BYTE data type in assembly programming?
4. In context to Virtual Memory Management, out of the 3 states of a process's virtual address, in which state is the page access, protected by memory protection option? And which API call is used to specify memory access permissions?
5. Explain the working of SoftICE. Decompilers are not reliable. Why?
6. While crackers are breaking time-based protections, what APIs they mostly look for in the program disassembly? And what are the preferred Countermeasures for it?
7. Among UPX, ASPACK and MoleBox (all in their latest versions), which one would you choose to pack your programs and its dependants (DLLs, OCXs etc.) and why?

8. A binary program has 50 45 00 00 in the signature field. Determine whether it's a PE, NE, LE or LX file. Mention reason.

9. What are descriptors, in context to Symbian mobile OS? How are they useful in mobile application reversing?