SEMC-216

M.Sc. (IInd Semester) Examination, 2022

COMPUTER SCIENCE

Paper - FS-COMP-MSC-CS-CC-204

(Ethical Hacking)

Time : 1½ Hours]

[Maximum Marks : 40

Note :— The question paper contains three Sections.

Section-A (Marks : 1 × 10 = 10)

Note :— Answer all the *ten* questions (Answer limit 50 words). Each question carries 1 mark.

Section-B (Marks : 3 × 5 = 15)

Note :— Answer any *five* questions by selecting at least *one* question from each Unit (Answer limit 200 words). Each question carries 3 marks.

Section-C (Marks : 5 × 3 = 15)

Note :— Answer any *three* questions by selecting *one* question from each Unit (Answer limit 500 words). Each question carries 5 marks.

Section-A

1. (i) Define reconnaissance phase.

   (ii) Mention any *two* phases of hacking other than reconnaissance.

(iii)   What is the use of sbin ?

(iv)   What is the use of touch command ?

(v)   Define Man in the middle attack.

(vi)   What is the use of wireshark ?

(vii)   Define social engineering attack.

(viii)   Define DOS attack.

(ix)   What do you mean by session hijacking ?

(x)   What is the use of SQL MAP ?

Section–B

Unit–I

2.   Define the use of Kali Linux in hacking.

3.   Explain any two phases of hacking.

4.   Explain Trojans with a suitable example.

Unit–II

5.   What do you mean by privilege escalation ?

6.   Elaborate the use of metasploit tool usage in hacking.

7.   How do the wireshark capture the packets ?

Unit–III

8.   Explain the mechanism behind any DDOS attack.

9.   Define the various types of session hijacking.

10.   What is the utility of database hacking ? Explain.

BI–281

(2)

Section-C

Unit-I

11. Elaborate different phases of hacking with suitable softwares usage in each phase.

12. Differentiate the internal mechanism of virus and worms along with suitable example.

Unit-II

13. Explain the different steps following while handling metasploit for enumeration.

14. What are the different social engineering attacks ?

Unit-III

15. How web servers are attacked ? Elaborate the attacks.

16. Elaborate different types of password attacks.