Reg. No……. Name…… **18U563**

B. B. A. DEGREE END SEMESTER EXAMINATION - OCTOBER/NOVEMBER 2018

SEMESTER –5: BACHELOR OF COMPUTER APPLICATION (BCA) (OPEN COURSE)

COURSE: 16U5OCBCA1: SECURITY THREATS AND TRENDS

(For Regular - 2016 admission)

Time: Three Hours Max. Marks: 75

SECTION A

Answer all the following (1 marks each)

1. List types of virus?
2. Name any two antivirus software?
3. Mention any new trend in cyber security?
4. What type of virus affect the boot sector of a floppy or hard disk?
5. …… malware run in the stealth mode or hidden mode.
6. DMZ is ……..
7. Honey net is ……..
8. What is IDS?
9. ……..is the main function of a RAT.
10. Who is responsible for fixing Zero day vulnerabilities in the system? (1 x 10 = 10)

SECTION B

Answer any 8 (2 marks each)

11. Checking every employee in the organization at the entrance and exit points is part of ……control.
12. A logical or physical discontinuity in a network to prevent unauthorized access to data or resources is known as ……
13. Explain the attack phase of virus?
14. What is an AIDS Trojan?
15. Differentiate between Trojans and viruses.
16. Write the main function of Trojan.
17. Why should procedural control against RATs include training of users?
18. What is detective control?
19. What are the techniques used in targeted attack?
20. Define discovery stage of APTs? (2 x 8 = 16)

SECTION C

Answer any 5 (5 marks each)

21. Differentiate between infection phase and attack phase of a virus?
22. Explain different methods for antivirus detection?
23. Draw the diagrammatic representation of Honey net.
24. Explain the working of DMZ.
25. Write a note on Security implications of Rootkits.
26. Explain information warfare?
27. Explain Discovery phase of APT attack? (5 x 5 = 25)

SECTION D

Answer any 2 (12 marks each)

28. Explain different methods used as countermeasures for viruses and worms?
29. Explain countermeasures for Botnet attacks and also about recent Botnet attack.
30. What are the countermeasures used against rootkits?
31. Briefly explain the different threats to system security? (12 x 2 = 24)