TB174700C **Reg. No: .....**

Name: .....

BCA DEGREE (C.B.C.S.S) EXAMINATION, MARCH 2019
(2017 Admissions Regular, 2016 AdmissionsImprovement/ Supplementary)
SEMESTER IV- CORE COURSE
(CLOUD TECHNOLOGY AND INFORMATION SECURITY MANAGEMENT)
CA4B05TB - ETHICAL HACKING FUNDAMENTALS

Time: Three Hours **Maximum Marks: 80**

PART A

I Answer all questions. Each question carries 1 mark.

1. Define security testing.
2. Define session hijacking.
3. Expand WEP and WPA.
4. Differentiate between NIDS and IDS
5. Write the different phases in report writing.
6. Define risk evaluation.

(6x1=6)

PART B

II Answer any seven questions. Each question carries 2 marks

7. Write steps in malicious hacking.
8. List any 6 scanning tools.
9. What are Ettercap, Hunt, Juggernaut, T-sight?
10. What are the symptoms of DoS attack?
11. Explain about sniffers and Denial of service?
12. Write the lifecycle of a virus.
13. What is stateful inspection firewalls?
14. Draw the diagram of methods of network penetration testing**.**
15. Define false positive and false negative and CVE.
16. Write the types of mitigation planning.

(7x2=14)

PART C

III Answer any five questions. Each question carries 6 marks

17. Write a short note on Trojan.
18. Explain Web server and web application attacks and countermeasures.
19. Write a short note on web application hacking.
20. Write a note on Linux hacking.
21. Explain SQL injection in detail.
22. Write a short note on phases in report writing.

23. Write a short note on vulnerability assessment report.
24. What is penetration testing? Explain network penetration testing report.

(5x6=30)

PART D

IV Answer any two questions. Each question carries 15 marks

25. Briefly explain SNMP and NetBIOS enumeration.
26. Write a note on
    (i) Hidden fields (3)
    (ii) Web-based authentication(5)
    (iii) Web-based password cracking(4)
    (iv) XSS(3)
27. Briefly explain wireless hacking in detail.
28. Briefly explain
    (i) Demonstration of vulnerabilities (7)
    (ii) Mitigation (8)

(2x15=30)