Reg No.:_____

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

EIGHTH SEMESTER B.TECH DEGREE (HONS.) EXAMINATION, MAY 2019

Course Code: EC466

Course Name: CYBER SECURITY

Max. Marks: 100 Duration: 3 Hours

PART A

Answer any two full questions, each carries 15 marks. Marks

1 a) Explain the architecture of OpenVAS. (10)

b) Describe how Metasploit can be used as an effective vulnerability scanning tool. (5)

2 a) Explain the concept of Network Reconnaissance and describe any tool that supports it. (10)

b) Explain False Positives and False Negatives. What is Zero-day Vulnerability? (5)

3 a) What can you infer from the term "Banner/Version Check"? (5)

b) Explain the working of WinRelay. (5)

c) List the features of NETCAT and SOCAT (5)

PART B

Answer any two full questions, each carries 15 marks.

4 a) What do you understand by HTTP Utilities? Write a description on OpenSSL and Curl (3)

b) Explain the concept of Virtual Private Network (12)

5 a) What do you mean by Brute-Force Attack? Explain L0htcrack tool that assist in Brute-Force Attacks (5)

b) Write a brief note on Application Inspection tools (5)

c) What are the different versions of Stunnel? Explain the purpose of Stunnel while redirecting the traffic from HTTPS to HTTP? (5)

6 a) Explain the features of JOHN THE RIPPER password cracking tool (7)

b) Describe the Packet characteristics that need to be followed by Packet Filters and Firewall? (8)

PART C

Answer any two full questions, each carries 20 marks.

7 a) Explain the architecture of Firewall. What are the various characteristics of Firewall? (8)

b) What is password cracking? List four guidelines that need to be followed to avoid password cracking. (8)

c) What do you understand by the term "STEGANOGRAPHY"? (4)

8 a) What is Incident Response? What are the different phases associated with Incident Response. (10)

b) What is Cyber Crime? How is it classified? What are the different types of cyber crimes towards an individual? (10)

9 a) Explain the ethical aspects of Digital Forensics. (10)

b) Write a short note on: (10)

1. DDOS attack
2. SQL injection
3. Buffer overflow

****