Hall Ticket No □□□□□□□□□□ Question Paper Code: ACCC03

INSTITUTE OF AERONAUTICAL ENGINEERING

(Autonomous)
Dundigal-500043, Hyderabad

B.Tech V SEMESTER END EXAMINATIONS (REGULAR/ SUPPLEMENTARY) - FEBRUARY 2024

Regulation: UG20

NETWORK SECURITY

Time: 3 Hours **CSE(CYBER SECURITY)** **Max Marks: 70**

Answer ALL questions in Module I and II
Answer ONE out of two questions in Modules III, IV and V
All Questions Carry Equal Marks
All parts of the question must be answered in one place only

MODULE – I

1. (a) Provide an overview of the border gateway protocol (BGP) and its critical role in internet routing. Identify and discuss three security challenges or vulnerabilities associated with BGP, emphasizing their potential impact on network stability and security. [BL: Understand| CO: 1|Marks: 7]

   (b) Write about virtual local area network (VLAN) and elucidate its purpose in a large organization's network architecture. Discuss three security considerations and best practices associated with the implementation of VLANs, highlighting their role in enhancing access control and segmentation. [BL: Apply| CO: 1|Marks: 7]

MODULE – II

2. (a) Interpret the implications of integrating security protocols at different layers, considering factors such as performance, scalability and interoperability. [BL: Understand| CO: 2|Marks: 7]

   (b) Demonstrate the association between an IKE header and the key exchange payload with the help of a diagram, detailing each field of both. [BL: Understand| CO: 2|Marks: 7]

MODULE – III

3. (a) Identify different types of attacks that leverage ICMP messages. Discuss the potential impact of these ICMP-based attacks on network availability and integrity. [BL: Understand| CO: 3|Marks: 7]

   (b) Elucidate the significance of OS fingerprinting in the context of cybersecurity and how it relates to ICMP messages. [BL: Understand| CO: 3|Marks: 7]

4. (a) Describe the purpose of ICMP route redirect messages in a network. Discuss a potential security implication associated with ICMP route redirect and propose a mitigation strategy. [BL: Understand| CO: 4|Marks: 7]

   (b) Differentiate between the authentication header (AH) and encapsulating security payload (ESP). [BL: Understand| CO: 4|Marks: 7]

MODULE – IV

5. (a) Write about pretty good privacy (PGP). Explain its primary purpose in securing communication. Identify and describe the essential services offered by PGP in ensuring the confidentiality and integrity of messages. [BL: Understand| CO: 5|Marks: 7]

(b) Explore how PGP integrates with other security measures in the communication project, such as network security and endpoint protection. Propose strategies to enhance the overall security synergy, ensuring a holistic and robust defense against potential threats.

[BL: Apply| CO: 5|Marks: 7].

6. (a) Develop step-by-step overview of the process involved in transmitting a PGP-encrypted message. Include key generation, encryption, and the use of digital signatures.

[BL: Understand| CO: 5|Marks: 7]

(b) Write the steps involved in receiving and decrypting a PGP-encrypted message. Discuss how the recipient verifies the authenticity of the message and sender. [BL: Understand| CO: 5|Marks: 7]

MODULE – V

7. (a) Explain how the SSL handshake protocols contribute to preventing man-in-the-middle attacks, a prevalent web threat. [BL: Understand| CO: 6|Marks: 7]

(b) Enumerate and categorize four distinct types of threats commonly encountered on the web. For each identified threat, elucidate the specific risks it poses to web security and potential impacts on users and organizations. [BL: Apply| CO: 6|Marks: 7]

8. (a) Provide a comprehensive overview of the architecture of the secure socket layer (SSL), emphasizing its core components and their functionalities. [BL: Understand| CO: 6|Marks: 7]

(b) Explore how changes or vulnerabilities in one component may impact the overall security posture of the SSL/TLS implementation? Apply strategies for maintaining a resilient and secure web communication environment. [BL: Apply| CO: 6|Marks: 7]

– ○ ○ ◯ ○ ○ –