Hall Ticket No | | | | | | | | | | |

Question Paper Code: ACCC09

INSTITUTE OF AERONAUTICAL ENGINEERING

(Autonomous)
Dundigal-500043, Hyderabad

B.Tech VI SEMESTER END EXAMINATIONS (REGULAR) - JULY 2023
Regulation: UG-20
PENETRATION TESTING AND CYBER OPERATIONS

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) Discuss the process, techniques, and tools involved in effectively gathering OSINT for enhancing security measures with examples. [BL: Understand| CO: 1|Marks: 7]

   (b) Company ABC, a medium-sized organization, decides to enhance its cyber security strategy by implementing Nessus policies for vulnerability assessment and management. Write the steps taken by company ABC to configure and utilize Nessus policies, and discuss the benefits and outcomes of incorporating Nessus in their vulnerability management process. [BL: Apply| CO: 1|Marks: 7]

MODULE – II

2. (a) Explain the concept of Metasploit payloads and explain how they can be utilized to exploit open phpMyAdmin instances and provide some examples. [BL: Understand| CO: 2|Marks: 7]

   (b) In the context of cybersecurity, explore the case study of bypassing antivirus applications, examining the techniques employed by attackers to evade detection and the countermeasures that can be implemented to strengthen defenses. Discuss the concept of polymorphic malware, encrypted payloads, and fileless malware as methods used to bypass antivirus applications. [BL: Apply| CO: 2|Marks: 7]

MODULE – III

3. (a) Compare and contrast the privacy protocols employed in wired and wireless networks in terms of their effectiveness, vulnerabilities, and implications for data security. Provide real world example to justify your answer. [BL: Understand| CO: 3|Marks: 7]

   (b) Examine a case study on the implementation of wireless privacy protocols in a corporate environment to ensure secure and private wireless communications. Analyze the organization's requirements, challenges, and considerations for selecting and implementing wireless privacy protocols. [BL: Apply| CO: 3|Marks: 7]

4. (a) Describe the tools and techniques employed for cracking wireless passwords, including packet sniffing, brute force attacks and dictionary attacks. [BL: Understand| CO: 4|Marks: 7]

(b) Investigate a case study on wireless Denial-of-Service (DoS) attacks and their impact on network availability and security. Analyze the vulnerabilities and techniques used in wireless DoS attacks, such as deauthentication attacks, jamming, and beacon flooding. Discuss the consequences of these attacks on wireless network performance, user experience, and business operations

[BL: Apply| CO: 4|Marks: 7]

MODULE – IV

5. (a) Evaluate the mechanisms and techniques employed to enhance the security of SMTP, such as Transport Layer Security (TLS) encryption, Sender Policy Framework (SPF), and DomainKeys Identified Mail (DKIM). [BL: Understand| CO: 5|Marks: 7]

   (b) Explore a case study on the implementation of the Trivial File Transfer Protocol (TFTP) in a multinational technology firm, Company XYZ, for network file transfer. Analyze the applications of TFTP in firmware updates, bootstrapping network devices, and transferring configuration files.

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

6. (a) Discuss the consequences of ICMP SMURF attacks on network infrastructure, such as network congestion, resource exhaustion, and potential service disruptions with a suitable example.

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

   (b) Highlight the importance of vigilance and the implementation of robust security measures by organizations across various sectors, including e-commerce, finance, and government, to effectively mitigate the risks associated with PING-SYN attacks. [BL: Apply| CO: 5|Marks: 7]

MODULE – V

7. (a) Mention the features and functionalities of NeoTrace, including its ability to perform IP address and domain name lookups, trace network routes, and provide detailed network performance information. Analyze the benefits of using NeoTrace in identifying network issues, such as latency, packet loss, or routing problems, and its role in optimizing network performance.

   [BL: Understand| CO: 6|Marks: 7]

   (b) Investigate packet loss detection and troubleshooting network outages where trace route analysis has been utilized to pinpoint network problems and improve network performance.

   [BL: Apply| CO: 6|Marks: 7]

8. (a) Summarize the importance of inference control in preventing unauthorized disclosure of sensitive information through indirect or inferred means. Analyze the risks associated with inference attacks, where an adversary can deduce confidential information by combining seemingly innocuous data. [BL: Understand| CO: 6|Marks: 7]

   (b) Analyze the defense organization on multilevel database security and its significance in safeguarding sensitive information across different security levels. Analyze the challenges and requirements of implementing multilevel security in a database environment, where data with different classifications or security levels coexist. [BL: Apply| CO: 6|Marks: 7]