Printed Page:- 04

Subject Code:- ACSCY0501

Roll. No:

NOIDA INSTITUTE OF ENGINEERING AND TECHNOLOGY, GREATER NOIDA

(An Autonomous Institute Affiliated to AKTU, Lucknow)

B.Tech

SEM: V - THEORY EXAMINATION (2024 - 2025)

Subject: Cyber Security Essentails

Time: 3 Hours

Max. Marks: 100

General Instructions:

IMP: *Verify that you have received the question paper with the correct course, code, branch etc.*

1. This Question paper comprises of three Sections -A, B, & C. It consists of Multiple Choice Questions (MCQ's) & Subjective type questions.

2. Maximum marks for each question are indicated on right -hand side of each question.

3. Illustrate your answers with neat sketches wherever necessary.

4. Assume suitable data if necessary.

5. Preferably, write the answers in sequential order.

6. No sheet should be left blank. Any written material after a blank sheet will not be evaluated/checked.

REG.JULY_DEC-2024

SECTION-A 20

1. Attempt all parts:-

1-a. What does two-factor authentication (2FA) enhance? (CO1,K1) 1

(a) Encryption strength

(b) Data Backup Processes

(c) User authentication security

(d) Firewall Efficiency

1-b. Which attack method is commonly used to compromise routers? (CO1,K1) 1

(a) DNS hijacking

(b) SQL Injection

(c) Credential stuffing

(d) Code obfuscation

1-c. Algorithm encrypting data for secure VPN communication. (CO2,K1) 1

(a) RSA

(b) MD5

(c) SHA-1

(d) AES

1-d. VPN type offering secure connections for remote users. (CO2,K1) 1

(a) Remote Access VPN

(b) Site-to-Site VPN

(c) Personal VPN

(d) Local Area Network VPN

1-e. Analysis process for determining an attack's origin in a network (CO3,K2) 1

(a) Security assessment
(b) Forensic analysis
(c) Risk management
(d) Network configuration

1-f. Encryption standard used for wireless networks (CO3,K1) 1

(a) AES
(b) SHA
(c) MD5
(d) DES

1-g. Tool used in Kali Linux for network penetration testing is:(CO4,K2) 1

(a) Nmap
(b) Metasploit
(c) Aircrack-ng
(d) Nessus

1-h. Network security technique where an encrypted tunnel is created over an insecure network is:(CO4,K1) 1

(a) ACLs
(b) VLANs
(c) VPN
(d) SSL/TLS

1-i. In a dictionary attack, which method is used?(CO5,K1) 1

(a) Trying words from a list
(b) Guessing by brute force
(c) Using complex algorithms
(d) Analyzing password hashes

1-j. Which of these is a common sign of password theft?(CO5,K2) 1

(a) Changing password regularly
(b) Unauthorized account access
(c) Changing security settings
(d) Using encrypted passwords

2. Attempt all parts:-

2.a. What are the common vulnerabilities exploited by attackers in social engineering attacks?(CO1,K1) 2

2.b. Mention two advantages of using OpenVPN compared to traditional VPNs.(CO2,K2) 2

2.c. Differentiate between TCP and UDP traffic in protocol analysis.(CO3,K1) 2

REG:JULY_DEC-2024

2.d.	State the function of Access Control Lists (ACLs) at the network layer.(CO4,K1)	2
2.e.	Why is password reuse a bad practice?(CO5,K2)	2

SECTION-B 30

3. Answer any five of the following:-

3-a.	How do spear phishing attacks differ from regular phishing?(CO1,K2)	6
3-b.	Describe common attacks targeting smartphones and how to mitigate them.(CO1,K1)	6
3-c.	How does OpenVPN utilize both symmetric and asymmetric encryption for secure communication?(CO2,K2)	6
3-d.	What are the security challenges associated with VPNs, and how does OpenVPN address them?(CO2,K1)	6
3.e.	Discuss the process of automating Wireshark scripts for incident response.(CO3,K3)	6
3.f.	Explain how firewalls contribute to network security at the network layer.(CO4,K2)	6
3.g.	Discuss the limitations of John the Ripper in cracking complex passwords.(CO5,K2)	6

SECTION-C 50

4. Answer any one of the following:-

4-a.	What are the emerging threats in cybersecurity post-pandemic?(CO1,K2)	10
4-b.	Differentiate between IoT attacks and cloud based attacks.(CO1,K1)	10

5. Answer any one of the following:-

5-a.	Explain the different types of VPNs and their applications in detail.(CO2,K1)	10
5-b.	Describe the tunneling process in VPNs and its importance for data protection.(CO2,K2)	10

6. Answer any one of the following:-

6-a.	Explore the tools and techniques used in preserving and analyzing digital evidence in an incident.(CO3,K2)	10
6-b.	Design a Wireshark script for detecting specific types of network anomalies in real-time.(CO3,K3)	10

7. Answer any one of the following:-

7-a.	Examine how Access Control Lists (ACLs) control traffic flow and enhance security at the Network layer.(CO4,K2)	10
7-b.	Discuss how encryption standards such as SSL/TLS provide end-to-end security for online transactions.(CO4,K3)	10

8. Answer any one of the following:-

8-a.	Explain the significance of salting in password hashing with examples. Describe how it prevents specific types of attacks.(CO5,K2)	10
8-b.	Compare and contrast brute-force, dictionary, and hybrid password cracking	10

REG:JULY_DEC:2024

techniques. Highlight their effectiveness and countermeasures.(CO5,K2)

REG:JULY_DEC-2024