Printed Page:- 04

Subject Code:- ACSCY0502

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: Ethical Hacking

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.

SECTION-A 20

1. Attempt all parts:-

1-a. Ethical hacking focuses on identifying vulnerabilities in systems to prevent cyberattacks.(CO1,K1) 1

(a) TRUE

(b) FALSE

(c) Sometimes

(d) None of these

1-b. Ethical hacking provides significant importance in safeguarding sensitive data.(CO1 K1) 1

(a) Decreasing costs

(b) Delaying breaches

(c) Increasing backups

(d) Enhancing security

1-c. Cuckoo Sandbox is primarily used for:(CO2,K1) 1

(a) Malware Analysis

(b) Network Scanning

(c) Penetration Testing

(d) System Monitoring

1-d. Cuckoo Sandbox can be integrated with which of the following tools for enhanced security operations?(CO2,K1) 1

(a) Nessus
(b) SIEM systems
(c) IDS
(d) Firewall

1-e. Attack that manipulates queries to a database?(CO3,K1) 1

(a) Cross-Site Scripting
(b) SQL Injection
(c) Directory Traversal
(d) File Inclusion

1-f. Scanning technique to identify open ports in a web application?(CO3,K1) 1

(a) Port Scanning
(b) OS Fingerprinting
(c) Code Scanning
(d) Protocol Analysis

1-g. Which port scanning technique is the most stealthy and difficult to detect?(CO4,K1) 1

(a) NULL scan
(b) UDP scan
(c) Connect scan
(d) SYN scan

1-h. What does the command nmap -sS perform?(CO4,K1) 1

(a) TCP Connect scan
(b) Stealth SYN scan
(c) UDP scan
(d) OS detection

1-i. Tool commonly used to crack WEP Wi-Fi passwords?(CO5,K1) 1

(a) Aircrack-ng
(b) Wireshark
(c) NetCat
(d) Nmap

1-j. Privilege escalation is used to gain access to what?(CO5,K1) 1

(a) A regular user account
(b) Administrative privileges
(c) Remote access
(d) Local network access

2. Attempt all parts:-

2.a. Name one famous hacker who became a White Hat after serving time in prison. 2

2.b. Define the term “footprinting” in the context of security. 2

2.c.	Define web application security.	2
2.d.	Identify a key feature of a TCP SYN scan.	2
2.e.	Name one tool commonly used for reverse engineering malware.	2

SECTION-B 30

3. Answer any five of the following:-

3-a.	Describe the concept of ethical hacking and its importance in cybersecurity.(CO1,K1)	6
3-b.	Discuss the role of an ethical hacker in securing sensitive data and systems.(CO1,K1)	6
3-c.	Explain the basic usage of Cuckoo Sandbox in analyzing malware.(CO2,K2)	6
3-d.	How does Cuckoo Sandbox simulate an environment to detect malware behavior?(CO2,K1)	6
3.e.	Define CSRF and explain its effect on web applications.(CO3,K1)	6
3.f.	Describe how Nmap performs version detection for services running on open ports.	6
3.g.	List and explain John the Ripper techniques.(CO5,K3)	6

SECTION-C 50

4. Answer any one of the following:-

4-a.	Describe the various types of ethical hackers (White Hat, Black Hat, and Grey Hat) and their roles in cybersecurity.(CO1,K1)	10
4-b.	Explain the scope of ethical hacking in today's cybersecurity landscape and its growing importance.(CO1,K1)	10

5. Answer any one of the following:-

5-a.	Describe the basic usage of Cuckoo Sandbox for malware analysis and how it processes a suspicious file.(CO2,K2)	10
5-b.	Discuss the key components of Cuckoo Sandbox and their functions in analyzing suspicious files.(CO2,K2)	10

6. Answer any one of the following:-

6-a.	Describe SQL injection, its working mechanism, and prevention techniques.(CO3,K2)	10
6-b.	Define Cross-Site Request Forgery (CSRF) and explain its mitigation techniques.(CO3.K2)	10

7. Answer any one of the following:-

7-a.	Explain how Vulnerability analysis can be process in scanning .(CO4,K3)	10
7-b.	Write the challenges associated with TCP port scanning.(CO4,K2)	10

8. Answer any one of the following:-

8-a.	Describe how privilege escalation works and provide examples of different methods used to achieve it in a system.(CO5,K2)	10

8-b. What is malware and how its analysis can be done ? Discuss its importance in Ethical Hacking.(CO5,K2) 10