.

Printed Page:-4 **Subject Code:- ACSCY0701**

Roll. No:

NOIDA INSTITUTE OF ENGINEERING AND TECHNOLOGY, GREATER NOIDA
(An Autonomous Institute Affiliated to AKTU, Lucknow)
B.Tech
SEM: VII - THEORY EXAMINATION (2025 - 2026)
Subject: Penetration Testing

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. _____ best defines penetration testing(CO1,K1). 1

(a) A method of debugging software
(b) A simulated cyberattack to find vulnerabilities
(c) A process to upgrade systems
(d) A firewall testing method

1-b. The first step in a penetration testing is _____ (CO1,K1) 1

(a) Exploitation
(b) Reporting
(c) Reconnaissance
(d) Maintaining Access

1-c. Passive reconnaissance involves: (CO2,K2) 1

(a) Using Nmap directly
(b) Gathering public information
(c) Exploiting vulnerabilities
(d) Running brute force

1-d. _____of the following is a scanning technique?(CO2,K1) 1

(a) SYN Scan
(b) Hashing

(c) SQL Injection
(d) Phishing

1-e. Select the category that describes failing to restrict users from accessing resources they shouldn't.(CO3,K1) 1

(a) Broken Authentication
(b) Broken Access Control
(c) Security Misconfiguration
(d) Insufficient Logging & Monitoring

1-f. Pick the category that includes poor configuration of servers, platforms or frameworks.(CO3,K2) 1

(a) Injection
(b) Security Misconfiguration
(c) Cross-Site Request Forgery
(d) Broken Authentication

1-g. Identify the Android component primarily responsible for inter-app communication.(CO4,K1) 1

(a) Activity
(b) Service
(c) Content Provider
(d) Broadcast Receiver

1-h. Choose the mobile OS feature that provides an isolated execution environment for apps.(CO4,K1) 1

(a) Multitasking
(b) Sandboxing
(c) Root access
(d) Auto-rotate

1-i. Identify the exploitation technique that leverages return-oriented programming to bypass DEP.(CO5,K1) 1

(a) Heap spraying
(b) Return-Oriented Programming (ROP)
(c) Format-string attack
(d) SQL Injection

1-j. Select the vulnerability class typically exploited using heap-spraying in browser attacks.(CO5,K1) 1

(a) Broken Authentication
(b) Use-after-free
(c) Insecure Direct Object Reference
(d) CSRF

2. Attempt all parts:-

2.a. Mention two objectives of penetration testing.(CO1,K2) 2

2.b. Differentiate between active and passive reconnaissance?(CO2,K1) 2

2.c.	Give two controls to reduce risks from using vulnerable components.(CO3,K1)	2
2.d.	List two benefits of using Android Keystore.(CO4,K1)	2
2.e.	Name two common mitigations against memory corruption exploits.(CO5,K2)	2

SECTION-B 30

3. Attempt all parts:-

3.a. Answer any one of the following:-

3.a.(i)	Explain white box testing? How it is different from Grey box testing?(CO1,K2)	6
3.a.(ii)	Describe ethical issues in penetration testing.(CO1,K2)	6

3.b. Answer any one of the following:-

3.b.(i)	Explain different phases of reconnaissance(CO2,K2)	6
3.b.(ii)	Write a short note on enumeration and its significance(CO2,K2)	6

3.c. Answer any one of the following:-

3.c.(i)	Discuss the role of dependency management in preventing component vulnerabilities(CO3,K2)	6
3.c.(ii)	Analyse how insufficient logging can affect incident response.(CO3,K2)	6

3.d. Answer any one of the following:-

3.d.(i)	Explain how OS-level sandboxing helps prevent privilege escalation in mobile apps(CO4,K2)	6
3.d.(ii)	Compare certificate pinning and standard TLS validation for mobile apps(CO4,K2)	6

3.e. Answer any one of the following:-

3.e.(i)	Explain how ROP bypasses non-executable stack protections and typical mitigations(CO5,K2)	6
3.e.(ii)	Describe a safe lab workflow to develop and test proof-of-concept exploits.(CO5,K2)	6

SECTION-C 50

4. Answer any one of the following:-

4-a.	Explain the different phases of penetration testing and discuss why each phase is important for identifying and fixing security vulnerabilities.(CO1,K2)	10
4-b.	Evaluate legal frameworks governing penetration testing(CO1,K2)	10

5. Answer any one of the following:-

5-a.	Describe types of network scanning techniques in detail(CO2,K2)	10
5-b.	Explain different enumeration techniques with tools(CO2,K2).	10

6. Answer any one of the following:-

6-a.	Evaluate how an organization should use the OWASP Top 10 to shape secure SDLC practices(CO3,K2)	10
6-b.	Discuss how threat modeling complements the OWASP Top 10 in application security planning.(CO3,K2)	10

7. Answer any one of the following:-

7-a.	Evaluate a mobile app security checklist for release across Android and iOS platforms.(CO4,K2)	10

.

7-b.	Design a secure update mechanism for a mobile app to prevent supply-chain tampering(CO4,K2)	10

8. Answer any one of the following:-

8-a.	Evaluate the effectiveness of modern compiler mitigations (e.g., CFI, stack canaries) against advanced memory attacks.(CO5,K2)	10
8-b.	Assess the risks and mitigations of using automated exploit tools in penetration tests.(CO5,K2)	10