[This question paper contains 4 printed pages.]

Your Roll No.....

Sr. No. of Question Paper : 7967 **L**

Unique Paper Code : 2343010018

Name of the Paper : Ethical Hacking

Name of the Course : **DSE**

Semester : VI/VIII

Duration : 3 Hours Maximum Marks : 90

Instructions for Candidates

छात्रों के लिए निर्देश.

1. Write your Roll No- on the top immediately on receipt of this question paper.
2. **Section A** is compulsory (Question 1).
3. Attempt any 4 questions from **Section B**.
4. Parts of a question should be attempted together.

Section A

Q1	(a)	What are ISO standards in cyber security?	3
	(b)	Define Broken Access Control. List any two common causes of Broken Access Control.	3
	(c)	What is the importance of reporting in cyber security?	3
	(d)	What is the purpose of the fping command? What kind of information is obtained from its output?	3
	(e)	A user downloads free software from an untrusted website. After installation of the software, the system became slow, and multiple unwanted pop-ups appeared. Identify the type of malware likely involved in this scenario and explain its impact on system performance and user security.	3

P.T.O.

	(f)	What is DNS enumeration? What kind of information can be extracted from DNS records?	3
	(g)	Explain the role of Wireshark in troubleshooting networks.	3
	(h)	Give any three disadvantages of clearing logs.	3
	(i)	Write any three differences between web server hacking and web application hacking.	3
	(j)	What is a code injection attack? Give one example of a code injection attack.	3

Section B

Q2	(a)	List and describe the five primary stages of penetration testing.	5
	(b)	Explain any two vulnerabilities from the OWASP Top 10 with suitable examples.	5
	(c)	A system administrator observes multiple consecutive failed login attempts followed by a successful login. Identify the password cracking technique that may have been used. Explain how this technique works and discuss possible measures to prevent such attacks.	5
Q3	(a)	Explain the concept of foot printing and reconnaissance in ethical hacking.	5
	(b)	An attacker tries to find valid email addresses and mail server details of a company. Explain the technique that can be used for extracting information from email servers?	5
	(c)	A user receives an email appearing to be from a bank, asking to verify account details through a link. After entering the credentials, the user's account is misused. Identify the attack technique and explain how it is carried out. How can such attacks be prevented?	5

Q4	(a)	What is the NIST Cybersecurity Framework? What are the three core functions of the NIST Cybersecurity Framework.	5
	(b)	Differentiate between white box and black box penetration testing.	5
	(c)	Explain the role of social engineering in ethical hacking. How does it help to identify security weaknesses? Also, suggest two preventive measures to reduce such attacks.	5
Q5	(a)	Differentiate between threat and risk? Describe the role of System and Services Acquisition (SA) in maintaining information security.	5
	(b)	A security analyst needs to scan a network to identify open ports and services. Explain how Nmap can be used to perform this task, including TCP connect scan.	5
	(c)	List any five common techniques of unauthorized system access?	5
Q6	(a)	Explain John the Ripper password cracking tool. How is the SAM file used to crack the password? Mention two ethical considerations associated with its usage.	5
	(b)	Explain how DoS/DDoS attacks affect network availability, performance, and security.	5
	(c)	List three types of non-adversarial threat sources and explain how they impact the CIA triad with suitable examples.	5
Q7	(a)	What is SQL Injection? A website stores user data in a database and does not sanitize inputs. Explain how SQL Injection can compromise the system.	5
	(b)	Define Advanced Persistent Threat (APT). Explain its three characteristics and describe how it differs from other types of cyber-attacks.	5

(c) Write short notes on the following : 5

(i) Ipconfig Command

(ii) HTTRACK Tool