S. No. of Question Paper	:	**13358**
Unique Paper Code	:	**2344000029**
Name of the Paper	:	**GE : Ethical Hacking**
Name of the Course	:	
Semester	:	**VII**
Duration : **3 Hours**		Maximum Marks : **90**

Instructions for Candidates

1. Write your Roll No. on the top immediately on receipt of this question paper.
2. **Section A** is compulsory.
3. Answer any ***four*** questions from **Section B.**
4. Parts of question must be answered together.

Section A

1. a) Identify the vulnerability in the following scenarios as per OWASP Top 10: 5
   i) Sensitive information transmitted without encryption.
   ii) User input directly used in SQL queries.
   iii) Admin page accessible without authentication.
   iv) Weak password policy implementation.
   v) Hardcoded credentials in application code.

   b) Write full form of the following: 5
   i) OSINT
   ii) NIST
   iii) OWASP
   iv) IDS
   v) VPN

   c) What is risk assessment? What does an organisation do for performing risk assessment? 5

   d) Define Reconnaissance? Explain Social engineering in context of reconnaissance. 5

   e) What is function of following Netstat Parameters? 5
   i) -c
   ii) -s
   iii) -a
   iv) -n
   v) -r

   f) Identify the tools for: 5
   i) Network scanning
   ii) Password cracking
   iii) Packet sniffing
   iv) Vulnerability scanning
   v) Exploitation framework

Section B

2. a) Explain information security threats and attack vectors. 5
   b) Describe SYN, UDP, TCP, NULL and XMAS Nmap scanning techniques. 5
   c) What are different information security controls? 5

3. a) Describe NetBIOS enumeration and tools. 5
   b) Explain six key elements of a vulnerability assessment report. 5
   c) What are steps required to locate the SAM file, assuming the /mnt/sda1 directory is already created? 5

4. a) Define the following Terms 5
      i) Confidentiality
      ii) Data Integrity
      iii) System Integrity
      iv) Availability
      v) Authentication
   b) Explain Cyber Kill Chain steps. 10

5. a) Name the following: 5
      i) A tool to extract metadata about a document
      ii) A tool for extracting information from DNS when the target does not distinguish between internal and external IPs when conducting a zone transfer
      iii) A tool that can be used to query DNS servers and potentially obtain records about the various hosts
      iv) The command to list all the available interfaces for your machine
      v) The command to find the IP addresses, host names and other information of a website
   b) Explain steps of hacking web applications. 10

6. a) Differentiate between 15
      i) Black Box and White Box Penetration Testing
      ii) Ethical and Malicious hacker
      iii) Active and Passive reconnaissance
      iv) Bind and Reverse payload
      v) SQL Injection and XSS

7. a) Write short notes on 15
      i) Alternate Data Stream (ADS) in windows
      ii) OWASP Top 10
      iii) NIST Cyber security framework