(c) What is Metasploit? Describe any three payloads available in Metasploit. (5)

6. (a) Explain any five preventive measures to protect a system from malware attacks. (5)

(b) Explain any two password attack techniques with suitable examples. Suggest two preventive measures to protect systems against these attacks. (5)

(c) How does port scanning and vulnerability scanning assist an attacker during the reconnaissance phase of penetration testing? (5)

7. (a) Define web server hacking. Identify any two common vulnerabilities associated with web servers. How can these vulnerabilities be mitigated? (5)

(b) Discuss any three major causes of identity theft. Also, recommend appropriate preventive measures to avoid the risk of such attacks. (5)

(c) Write short notes on the following : (5)

(i) The Harvester Tool

(ii) DDoS attack

[This question paper contains 4 printed pages.]

Your Roll No.....

Sr. No. of Question Paper : 7290 **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

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

Section A

1. (a) How is penetration testing different from vulnerability assessment? (3)

(b) What are Google directives? List any two Google search operators useful in reconnaissance. (3)

(c) Differentiate between advanced persistent threat attacks and ransomware attacks. (3)

(d) How does the CIA triad help in securing information systems? (3)

(e) Discuss the role of log files in system security. Why might they be deleted or cleared? (3)

(f) Define MetaGooFil. What kind of data does it collect? (3)

(g) What is Cross-Site Scripting (XSS)? How does it exploit web applications? (3)

(h) Write any three differences between a virus and a worm? (3)

(i) Define Alternate Data Streams (ADS). How are they used in file systems? (3)

(j) Write any three differences between active scanning and passive scanning? (3)

Section B

2. (a) Explain any five stages of the Cyber Kill Chain. (5)

(b) Discuss the key implementation guidelines for an effective threat and vulnerability management program in an organization. (5)

(c) What are post-testing findings? Explain their significance in security assessment. (5)

3. (a) Differentiate between Active reconnaissance and Passive reconnaissance. (5)

(b) Explain the role of HTTrack in website footprinting and analysis. (5)

(c) Write short note on the following :

(i) Nslookup

(ii) Netstat (5)

4. (a) What is phishing? Write any three methods to prevent phishing attacks. (5)

(b) What is the role of Nmap tool in network security assessment? Explain its any three features. (5)

(c) What is insecure design in web applications? Explain its consequences. (5)

5. (a) Explain session hijacking with examples. Discuss the causes and impacts of session hijacking attacks. (5)

(b) A login page accepts user input without validations. Explain how an attacker can exploit it using SQL Injection. (5)