This question paper contains 4 printed pages]

Roll No. | | | | | | | | | | |

S. No. of Question Paper : **8076**

Unique Paper Code : **2343010018**

Name of the Paper : **Ethical Hacking**

Name of the Course : **B.Sc. (H)/B.A. (Prog) DSE (NEP-UGCF-2022)**

Semester : **VI**

Duration : **3 Hours** Maximum Marks : **90**

(Write your Roll No. on the top immediately on receipt of this question paper.)

Section A is compulsory.

Attempt any *four* questions from Section B.

Parts of a question should be attempted together.

Section – A

1. (*a*) What is a password attack ? Name *two* techniques used to carry out password attacks ? 3

   (*b*) What do you mean by website attack vectors ? Give an example. 3

   (*c*) What is a threat in information security ? Write any *two* threat sources. 3

   (*d*) What is session hijacking ? 3

   (*e*) Describe SQL injection with a suitable example. 3

P.T.O.

(*f*) Give any *three* disadvantages of clearing logs. 3

(*g*) Define the following terms : 3

(*i*) Phishers

(*ii*) Spammers

(*iii*) Ransomware.

(*h*) What is meant by DNS server hijacking ? 3

(*i*) What is the use of NetBIOS tool ? 3

(*j*) What is the use of vulnerability scanning in ethical hacking ? 3

Section – B

2. (*a*) Differentiate between ethical hacking and malicious hacking. 5

(*b*) What is reconnaissance ? Differentiate between active and passive reconnaissance. 5

(*c*) What is the use of social engineering in penetration testing ? Give a suitable example. 5

3. (*a*) What is a Denial-of-Service (DoS) attack ? How does it affect a network ? 6

(*b*) What is Metasploit ? Describe any *three* payloads used with Metasploit. 5

(*c*) Write any *four* impacts of a web server attack. 4

4. (*a*) Differentiate between white box and black box penetration testing. 6

(*b*) List any *five* OWASP Top vulnerabilities. 5

(*c*) What are the ethical implications of gaining access to an organization's network ? 4

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

(*b*) List any *five* threat and vulnerability management controls. 5

(*c*) Discuss the Alternate Data Stream (ADS). How is it used by the attackers ? 5

6. (*a*) What is the NIST Cybersecurity Framework ? Explain the *three* components of NIST Cybersecurity framework. 5

(*b*) Describe the following information exploitation techniques : 5

(*i*) privilege escalation

(*ii*) remote password cracking.

(*c*) What is the purpose of a vulnerability assessment report in security of an organization ? 5

7. (*a*) Discuss the role of risk management in supporting an organization's information security. 5

(*b*) Write short notes on any *five* of the following : 10

(*i*) Ipconfig

(*ii*) Ping

(*iii*) Nslookup

(*iv*) Wireshark

(*v*) Burpsuite

(*vi*) Nmap.