This question paper contains **3** printed pages]

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

S. No. of Question Paper : **7537**

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 are the following network tools used for : 4

(*i*) Ping

(*ii*) ipconfig

(*b*) How does SQL injection attack work ? Give a suitable example. 4

(*c*) Differentiate between passive and active scanning in OWASP ZAP. 4

(*d*) What is Alternate Data Stream ? How is it used by the attackers ? 4

(*e*) Discuss the role of social engineering in penetration testing. 4

P.T.O.

(*f*) What is session hijacking ? 3

(*g*) What do you understand by confidentiality, integrity, and availability of the information ? 3

(*h*) Describe *two* techniques of password cracking. 2

(*i*) What is the use of Wireshark tool ? 2

SECTION B

2. (*a*) Write any *five* steps to hack a web server. 5

(*b*) State the importance of clearing windows logs. Mention any *two* tools that can be used to clear windows logs ? 5

(*c*) What is a Denial of Service (Dos) attack ? Discuss any scenario depicting DoS attack. 5

3. (*a*) Discuss the role of HTTRACK in the reconnaissance phase of penetration testing. 5

(*b*) What is Cross-Site Scripting (XSS) ? Differentiate between stored and reflected XSS attacks. 5

(*c*) What is the role of threat and vulnerability management in identifying security flaws of an organization ? How does it help improve network security ? 5

4. (*a*) Describe any *two* techniques of gaining unauthorized access into a computer system. 5

(*b*) What is DNS server hijacking ? How does an attacker exploit DNS servers to redirect users to malicious sites ? 5

(*c*) List *five* best practices to prevent privilege escalation attacks. 5

5. (*a*) Describe the following : 6

(*i*) Trojan Horse

(*ii*) Logic Bomb

(*iii*) Worm.

(*b*) List *five* techniques used for maintaining access in ethical hacking. 5

(*c*) Describe the purpose of Whois and nslookup commands. 4

6. (*a*) Discuss *three* core functions of NIST Cyber Security Framework. 6

(*b*) Explain any *five* steps of cyber kill chain model. 5

(*c*) What is the use of Nmap tool in penetration testing ? How Nmap is used to perform a TCP connect scan ? 4

7. (*a*) Write short notes on the following : 6

(*i*) threat

(*ii*) attack

(*iii*) spyware.

(*b*) How does port scanning and brute force attack help an attacker during the reconnaissance phase of penetration testing ? 5

(*c*) Discuss any *four* elements of vulnerability assessment report. 4