BRAINWARE UNIVERSITY

Term End Examination 2023-2024
Programme – B.Sc.(FND)-Hons-2023
Course Name – Digitalisation and its Impact
Course Code - VAC00005
(Semester II)

Full Marks : 60 **Time : 2:30 Hours**

[The figure in the margin indicates full marks. Candidates are required to give their answers in their own words as far as practicable.]

Group-A
(Multiple Choice Type Question) 1 x 15=15

1. *Choose the correct alternative from the following :*

(i) What does NAS stand for?
   a) Network Allocation System b) Network Attached Storage
   c) New Accessible Server d) Non-stop Application System

(ii) Identify the type of vulnerability involving inadequate validation of user inputs.
   a) Non-validated input b) Buffer overflow
   c) Race conditions d) Access-control problems

(iii) Explain the purpose of legal authorization in ethical hacking.
   a) Permission to test specific systems b) Unlimited access to all systems
   c) Immunity from legal consequences d) Anonymity for the hacker

(iv) Describe the primary focus of White Hat Hackers.
   a) Security testing and defense b) Malicious activities
   c) Financial gain d) Unrestricted access

(v) Identify the type of vulnerability related to timing issues in software.
   a) Race conditions b) Buffer overflow
   c) Non-validated input d) Weaknesses in security practices

(vi) Explain what "Buffer overflow" refers to in the context of software vulnerabilities.
   a) Writing beyond allocated memory b) Underutilization of memory
   c) Proper memory handling d) Efficient memory access

(vii) What does a virus primarily do?
   a) Encrypt files b) Display advertisements
   c) Self-replicate d) Gather information

(viii) Explain the purpose of a worm in cybersecurity.

a) Gather information
b) Encrypting files
c) Display advertisements
d) Self-replication

(ix) What does SQL injection target?

a) Network vulnerabilities
b) SQL databases
c) Browser vulnerabilities
d) Wi-Fi passwords

(x) In a piggyback attack, how does an attacker gain access?

a) Create a scenario
b) Follow someone
c) Piggyback on a legitimate user
d) Intercept communication

(xi) What does filter evasion aim to bypass?

a) Wi-Fi passwords
b) Email filters
c) Keystrokes
d) Browser history

(xii) What is the central goal of Threat Intelligence in a cybersecurity context?

a) Identify Security Weaknesses
b) Predict Future Cyber Threats
c) Manage Incident Response
d) Implement Access Controls

(xiii) Define the term "Zero-Day Exploit" in the realm of cybersecurity.

a) A known software vulnerability
b) A previously unknown vulnerability
c) An encrypted communication channel
d) A type of security audit

(xiv) What is the main purpose of a Security Baseline in an organization?

a) Optimize Employee Productivity
b) Establish Minimum Security Standards
c) Develop Software Solutions
d) Maximize Network Performance

(xv) Describe adware's primary display.

a) Self-replicating ads
b) Information gathering ads
c) Encrypted messages
d) Pop-up advertisements

Group-B

(Short Answer Type Questions) 3 x 5=15

2. Explain DOS and DDOS. (3)

3. Write four examples of Wi-Fi Password Cracking. (3)

4. Discuss the activities and objectives of a Piggyback Attack, highlighting its reliance on legitimate network connections for unauthorized access. (3)

5. Discuss any three Security Operations in short. (3)
6. Explain Vulnerability Exploitation in breif. (3)

OR

Explain Blended Attack in breif. (3)

Group-C

(Long Answer Type Questions) 5 x 6=30

7. Discuss the principles and practices involved in securing wireless networks, emphasizing the importance of strong encryption, regular monitoring, and the use of guest networks. (5)
8. Define the responsibilities and security considerations for System and Network Administrators, focusing on the implementation of least privilege principles, regular system (5)

updates, and vulnerability assessments.

9. Discuss the importance of incident response planning and training in the context of computer security. (5)
10. Explore the motivations, characteristics, and objectives of state/nation-sponsored hackers, considering their appointment by governments, high pay, and their role in gaining confidential information from other countries. (5)
11. Compare and contrast the roles and objectives of "white hat" hackers and "black hat" hackers in the cybersecurity landscape, providing examples of ethical considerations for each. (5)

12. Evaluate the challenges and ethical considerations associated with malicious insiders or whistle-blowers, considering their potential disclosure of illegal activities and blackmailing of organizations, and discuss strategies for organizations to mitigate such risks. (5)

OR

Explain the importance of data privacy in ethical hacking and how ethical hackers should handle sensitive information discovered during testing. (5)

****