BRAINWARE UNIVERSITY

Term End Examination 2025-2026
Programme – B.Sc.(FND)-Hons-2024/B.Sc.(FND)-Hons-2025
Course Name – Digitalization 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 is the primary advantage of Cloud Storage?
   a) Accessibility b) Security
   c) Cost-effectiveness d) Speed

(ii) Choose the primary focus of cyber-crime level 'Phishing'.
   a) Unauthorized Access b) Data Manipulation
   c) Social Engineering d) Network Disruption

(iii) In the context of computer security, what is Authorization associated with?
   a) Authentication b) Access Control
   c) Encryption d) Data Transmission

(iv) Which type of cryptographic key is used for secure communication?
   a) Symmetric Key b) Public Key
   c) Private Key d) Hashing

(v) Choose a technology providing a secure private network over the internet.
   a) VPN b) VLAN
   c) NAT d) DDoS

(vi) Choose a common type of attack exploiting software vulnerabilities.
   a) Cross-site scripting b) SQL injection
   c) Malware d) Buffer overflow

(vii) Recognize a set of email authentication standards to prevent phishing.
   a) DMARC b) DKIM
   c) SPF d) DNSSEC

(viii) Define the primary motivation of Black Hat Hackers.
   a) Financial gain b) Ethical hacking
   c) Knowledge sharing d) Cybersecurity advocacy

(ix) Name a common consequence of hardware vulnerability.

a) System crashes
b) Code execution
c) Data leaks
d) Network congestion

(x) Specify the primary motivation of Black Hat Hackers.

a) Financial gain
b) Ethical hacking
c) Knowledge sharing
d) Cybersecurity advocacy

(xi) 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

(xii) Define spyware.

a) Gather information
b) Display advertisements
c) Self-replicate
d) Encrypt files

(xiii) Describe the primary focus of spear phishing.

a) Targeting high-profile individuals
b) Encrypting files
c) Display advertisements
d) Gathering information

(xiv) 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

(xv) Describe the primary role of Security Incident Response Teams (SIRTs).

a) Develop Software Applications
b) Analyze Threat Intelligence
c) Respond to and Mitigate Incidents
d) Optimize Network Performance

Group-B

(Short Answer Type Questions) 3 x 5=15

2. Illustrate the role of antivirus and anti-malware tools in enhancing internet security, including an example of their functionality. (3)
3. Define Critical Information Infrastructure (CII). (3)
4. What are the challenges of data privacy? (3)
5. Classify any three types of Phishing. (3)

6. Summarize Password Management. (3)

OR

Consider three potential threats and take proactive measures to enhance their cloud security. (3)

Group-C

(Long Answer Type Questions) 5 x 6=30

7. Analyze the importance of sustainability practices in the evolving landscape of modern data centres. (5)
8. What are the key points of Cloud Security? (5)
9. Discuss the impact of hacktivists on cybersecurity, examining their role as online activists, their use of hacking for social or political causes, and the potential consequences of gaining unauthorized access for influencing change. (5)

10. Explore the realm of SQL Injection, discussing how this database manipulation technique exploits vulnerabilities in web applications. Highlight the potential risks and consequences of successful SQL Injection attacks. (5)
11. Discuss the key stages involved in effective incident response and how each contributes to minimizing the impact of security incidents. (5)
12. Evaluate the impact of "script kiddies" on cybersecurity, considering their lack of advanced skills, use of pre-written scripts/tools, and motivations, with a focus on the potential (5)

consequences of their actions.

OR

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)

****