17548

BRAINWARE UNIVERSITY

Term End Examination 2024-2025
Programme – B.Sc.(FND)-Hons-2024
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) Define the CIA Triad.

a) Confidentiality, Integrity, Availability b) Cybersecurity, Intrusion, Authorization
c) Complexity, Inaccessibility, Adaptability d) Credibility, Interoperability, Adaptability

(iii) Select an example of Cloud-based Data Centre.

a) Google Cloud Data Centre b) Physical Data Centre
c) Amazon Web Services (AWS) d) Direct Attached Storage (DAS)

(iv) Choose the primary focus of cyber-crime level 'Phishing'.

a) Unauthorized Access b) Data Manipulation
c) Social Engineering d) Network Disruption

(v) What is the primary consideration in Data Centre - Cloud based?

a) Security b) Accessibility
c) Cost d) Speed

(vi) Identify a method used for securing data in transit.

a) Encryption b) Authentication
c) Antivirus d) Firewall

(vii) Choose a technology providing a secure private network over the internet.

a) VPN b) VLAN
c) NAT d) DDoS

(viii) Classify individuals who use pre-written tools based on their skill level.

a) Script Kiddies b) White Hat Hackers
c) Black Hat Hackers d) Grey Hat Hackers

(ix) Define the primary motivation of Black Hat Hackers.

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

(x) Name a common consequence of hardware vulnerability.

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

(xi) Define spyware.

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

(xii) Describe scareware's primary tactic.

a) Displaying scary pop-ups b) Gathering information
c) Encrypting files d) Self-replication

(xiii) 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

(xiv) Identify a primary goal of Security Risk Assessments.

a) Maximize Security Investments b) Identify and Mitigate Risks
c) Optimize Business Processes d) Enhance Employee Productivity

(xv) Choose a type of attack exploiting previously unknown vulnerabilities.

a) Malware b) Zero-day exploit
c) Brute force attack d) Spear phishing

Group-B

(Short Answer Type Questions) 3 x 5=15

2. Show how firewalls contribute to internet security and what their role is in controlling network traffic with an example. (3)
3. Define Threat Intelligence with example. (3)
4. What is N.A.S.? (3)
5. Describe network security. (3)
6. Summarize the importance of continuous monitoring and mitigation efforts in addressing hardware vulnerabilities. (3)

OR

Catagorize Software Vulnerabilities. (3)

Group-C

(Long Answer Type Questions) 5 x 6=30

7. How does encryption contribute to endpoint security? Provide an example of how encryption can protect sensitive data on individual devices. (5)
8. Define the legal aspect of Ethical Hacking. (5)
9. Describe the activities and behaviours associated with a Man-In-The-Middle (MitM) attack, highlighting its potential consequences on intercepted communications and compromised data. (5)

10. Evaluate the characteristics and potential impact of Distributed Denial-of-Service (DDoS) attacks, considering their scale and the difficulties in mitigating such large-scale disruptions. (5)

11. Explore the principles and practices of Password Management, emphasizing how these practices contribute to enhanced cybersecurity. (5)

12. Examine the role and significance of Threat Intelligence in cybersecurity, categorizing its different levels and explaining how collaboration within the industry enhances a collective defense against cyber threats. (5)

OR

Analyze the best practices for ensuring email security, focusing on measures to protect against phishing attempts and the use of encryption for sensitive data. (5)

****