BRAINWARE UNIVERSITY

Term End Examination 2023-2024
Programme – M.Sc.(ANCS)-2022
Course Name – Vulnerability Analysis and Penetration Testing
Course Code - MNCS302
(Semester III)

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) State the role of "intrusion detection systems (IDS)" as a countermeasure against web server attacks.

a) To capture network packets
b) To block all network traffic
c) To detect and respond to suspicious activity on the network
d) To launch DDoS attacks

(ii) Classify the role of "virtualization" in cloud computing and its impact on resource allocation and management.

a) To capture network packets
b) To block all network traffic
c) To create virtual instances of servers and resources for efficient allocation and management
d) To launch DDoS attacks

(iii) Choose the potential "security challenges" associated with serverless computing, including code vulnerabilities and access control.

a) To implement strong authentication mechanisms
b) To open network ports
c) To address security challenges related to code vulnerabilities, access control, and data protection in serverless environments
d) To share sensitive information publicly

(iv) Define "credential stuffing" in the context of penetration testing.

a) A method to generate strong passwords
b) A technique for brute-force attacks
c) The use of stolen usernames and passwords from one service on another
d) A type of penetration testing tool

(v) Choose the role of "DevSecOps" in cloud security and its integration of security practices into the software development and deployment process.

a) To capture network packets
b) To block all network traffic
c) To integrate security into the entire software development and deployment
d) To launch DDoS attacks

lifecycle through DevSecOps practices

(vi) Identify the "scope" of a penetration test affect the results.

a) It has no impact on the test results
b) It defines the specific systems and areas to be tested
c) It determines the penetration tester\'s skills
d) It restricts the use of automated tools

(vii) Provide an in-depth explanation of OS fingerprinting and its role in network scanning.

a) SYN scanning
b) Ping scanning
c) UDP scanning
d) ACK scanning

(viii) Recognize the characteristics of "symmetric-key cryptography" and its use of a single secret key for both encryption and decryption.

a) Asymmetric-key cryptography
b) Hashing algorithms
c) Public Key Infrastructure (PKI)
d) Symmetric-key cryptography

(ix) Define the "Diffie-Hellman key exchange" as a cryptographic protocol for secure key exchange over an insecure channel.

a) Asymmetric-key cryptography
b) Block ciphers
c) Stream ciphers
d) Symmetric-key cryptography

(x) Identify the concept of a "brute-force attack" and its attempt to discover a secret key by trying all possible combinations.

a) Cryptography attacks
b) Block ciphers
c) Asymmetric-key cryptography
d) Stream ciphers

(xi) Which control focuses on securing physical access to data centers?

a) Operations Security Controls
b) Media Management Controls
c) Incident Response Controls
d) Backup Controls

(xii) Choose the methods through which computer viruses typically spread.

a) Via physical media (e.g., USB drives)
b) Through email attachments
c) By exploiting vulnerabilities
d) Over the phone

(xiii) Recognize one security challenge associated with information security.

a) Data encryption
b) User authentication
c) Insider threats
d) Data backup

(xiv) State what network security aims to protect data against.

a) Physical threats
b) Unauthorized access
c) System performance issues
d) Data sharing

(xv) Identify the primary objective of a "SQL injection" attack.

a) Stealing user data
b) Disrupting network traffic
c) Crashing the target system
d) Manipulating website design

Group-B

(Short Answer Type Questions) 3 x 5=15

2. Describe how hashes are employed to ensure data integrity and security. (3)
3. Apply understanding of the Security Content Automation Protocol (SCAP) and its advantages. (3)
4. Analyze how a network risk trend report can proactively assist in risk management. (3)
5. What is a "vulnerability framework," and how does it aid in managing cybersecurity risks? (3)
6. Develop a comprehensive list of the key components or elements that define a service according to "ITIL." (3)

OR

Formulate an explanation of the process involved in "service definition" within "IT service management." (3)

Group-C

(Long Answer Type Questions) 5 x 6=30

7. Explain the concepts of Confidentiality, Integrity, and Privacy in information security. How do these concepts contribute to overall security? (5)

8. Describe the concept of API Management Patterns. Provide examples of common API management patterns and their applications. (5)

9. What is a Business Case in the context of Vulnerability Management? How can a well-constructed business case support VM initiatives within an organization? (5)

10. Explain the Basic Strategy for Vulnerability Management. What are the key steps involved in this strategy, and how does it help organizations address vulnerabilities? (5)

11. Explain the concept of Configuration Management in IT Service Management. How does Configuration Management help organizations maintain control over IT assets and resources? (5)

12. Explain the purpose and significance of the OWASP Application Security Verification Standard (ASVS). How does ASVS assist organizations in improving the security of their web applications? (5)

OR

What is Payment Card Industry (PCI) compliance, and why is it crucial for businesses that handle payment card data? (5)

****