BRAINWARE UNIVERSITY

Term End Examination 2025-2026
Programme – B.Sc.(ANCS)-Hons-2024/B.Sc.(ANCS)-Hons-2025
Course Name – Cyber Security Essentials
Course Code - BNC27002 (T)
(Semester II)

Full Marks : 40 **Time : 2:0 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 10=10

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

(i) Identify the primary purpose of network scanning and enumeration in cybersecurity.

a) To identify vulnerabilities and gather information about a network
b) To encrypt sensitive data
c) To block unauthorized access to a system
d) To perform penetration testing on a server

(ii) Recall the default TCP ports used by HTTP and HTTPS.

a) 20 and 21
b) 25 and 110
c) 80 and 443
d) 53 and 22

(iii) Why are NULL, FIN, and Xmas scans limited against firewalls?

a) They send encrypted packets
b) Firewalls may block packets with unusual flags
c) They require additional authentication
d) They rely on ICMP responses

(iv) What is the purpose of encoders in Metasploit?

a) To avoid antivirus detection by encoding exploits and payloads
b) To compress payloads for smaller size
c) To analyze vulnerabilities
d) To automate brute-force attacks

(v) Choose a key element of endpoint security.

a) Threat actors
b) Behavioral analysis
c) Social engineering
d) Public-key infrastructure

(vi) Recall why addressing Advanced Persistent Threats (APTs) is challenging in endpoint security.

a) They rely on social engineering tactics
b) They involve prolonged and sophisticated attacks
c) They cannot target remote workers
d) They affect only outdated systems

(vii) Recognize which is NOT a common threat targeting endpoints.

a) Ransomware
b) Drive-by downloads
c) SQL injection
d) Fileless malware

(viii) Recall the primary goal of continuous monitoring in the context of cybersecurity.

a) Proactively detect and identify security threats
b) Analyze system behavior for anomalies
c) Respond to security incidents in real-time
d) Implement preventative security controls

(ix) Choose the purpose of digital certificates in cybersecurity.

a) Verify the identity of entities in online interactions
b) Encrypt communication channels
c) Establish trust between parties
d) Both (a) and (c)

(x) Recognize the primary focus of social engineering attacks.

a) Disrupting systems
b) Manipulating people
c) Stealing data
d) Spreading malware

Group-B

(Short Answer Type Questions) 3 x 5=15

2. Express the importance of Endpoint Detection and Response (EDR) systems. (3)
3. Articulate the role of access controls in safeguarding sensitive information. (3)
4. Write the types of modules found under the Auxiliary category and their applications. (3)
5. Show how the WHOIS protocol works and the types of information it provides. (3)
6. Justify the importance of sufficient logging and monitoring in web application security assessments. (3)

OR

Assess the disruption capabilities of Denial-of-Service (DoS) attacks and their impact on availability. (3)

Group-C

(Long Answer Type Questions) 5 x 3=15

7. Express the key details Shodan.io provides when conducting passive reconnaissance. (5)
8. Explain the appropriate Metasploit module categories and provide examples of their use cases. (5)
9. Assess the functionalities of the Post module in Metasploit and its significance in post-exploitation activities. (5)

OR

Evaluate the risks and challenges associated with using Metasploit exploits, particularly low-ranking ones. (5)

****