



Brainware University  
393, Ramkrishnapur Road, Barasat  
Kolkata, West Bengal-700125

## BRAINWARE UNIVERSITY

Term End Examination 2022  
Programme – B.Sc.(ANCS)-Hons-2020  
Course Name – Security Operations Center  
Course Code - BNCSD502C  
( Semester V )

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) The secure Hash Algorithm (SHA) is specified in the:

- a) Data Encryption Standard
- b) Digital Signature Standard
- c) Digital Encryption Standard
- d) Advanced Encryption Standard

(ii) Which statement below is accurate about the reasons to implement a layered security architecture?

- a) A layered security approach is not necessary when using COTS products.
- b) A good packet-filtering router will eliminate the need to implement a layered security architecture.
- c) A layered security approach is intended to increase the work-factor for an attacker.
- d) A layered approach doesn't really improve the security posture of the organization.

(iii) How Many Tiers / levels are there by job roles in a SOC?

- a) 4
- b) 3
- c) 2
- d) 1

(iv) Compromising confidential information comes under \_\_\_\_\_

- a) Bug
- b) Threat
- c) Vulnerability
- d) Attack

(v) What is the sequence of a TCP connection?

- a) A. SYN-ACK
- b) B. SYN-ACK-FIN
- c) C. SYN-SYN-ACK
- d) D. SYN-SYN ACK-ACK

(vi) In terms of a threat informed defense, which element examines TTPs, malware hashes, or domain names?

- a) Defensive Engagement of The Threat
- b) Focused Sharing and Collaboration
- c) Cyber Threat Intelligence Analysis
- d) Incident Response & Intelligence Gathering

(vii) Wazuh server RESTful API running on?

- a) 50050
- b) 50550
- c) 55500
- d) 55000

(viii) APT stands for ?

- a) Advanced Packaging Tool  
c) Advanced Potential Threat
- b) Advanced Persistent Threat  
d) Attack Persistent Threat
- (ix) Which comes under the types of Threat Intelligence?  
a) Tactical intelligence  
c) Strategic intelligence
- b) Operational intelligence  
d) All of the above
- (x) Sysmon logs/evnts can be viewed primarily from?  
a) Event Viewer  
c) Syslog
- b) Windows defender  
d) Notepad
- (xi) How many tactics are there in the latest version(version 9) of the Enterprise ATT&CK matrix?  
a) 17  
c) 21
- b) 14  
d) 18
- (xii) Which is used by Nmap to identify Operating Systems?  
a) Kernel  
c) TTL
- b) BIOS  
d) Shell
- (xiii) Which tools can be used for creating payload?  
a) Metasploit  
c) Recon-ng
- b) Xsfer  
d) Aircrack-ng
- (xiv) Which one of the following can be considered as the class of computer threats?  
a) Dos Attack  
c) Soliciting
- b) Phishing  
d) Both A and C
- (xv) Which of the following is not a type of scanning?  
a) Xmas Tree Scan  
c) Null Scan
- b) Cloud scan  
d) SYN Stealth

**Group-B**

(Short Answer Type Questions)

3 x 5=15

2. Discuss about Threat Intelligence? (3)
3. Illustrate the Techniques in MITRE ATT&CK ? (3)
4. Write about the difference between SIEM and IDS? (3)
- OR
- Explain Command and Control Center? (3)
5. What is Bruteforce attack? (3)
- OR
- Explain Hashing ? (3)
6. Express about DNS? (3)
- OR
- Write about SSL? (3)

**Group-C**

(Long Answer Type Questions)

5 x 6=30

7. Describe Vulnerability with types ? (5)
8. Describe the importance of Threat Intelligence. (5)
9. "Explain the Threat Intelligence Lifecycle? " (5)
10. Explain the wazuh server components ? (5)
11. Write about Antivirus ? (5)
12. Illustrate about the Wazuh agent modules ? (5)
- OR
- What is a three-way handshake? Explain. (5)