



BRAINWARE UNIVERSITY

Library
Brainware University
398, Ramkrishnapur Road, Barasat
Kolkata, West Bengal-700125

Term End Examination 2024-2025
Programme – B.Sc.(ANCS)-Hons-2022
Course Name – Security Specialist
Course Code - BNCSD501C
(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) Name the compromising confidential information that comes under.

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

(ii) Select those individuals who maintain and handle IT security in any firm or organization.

- | | |
|---------------------------------|---------------------------|
| a) IT Security Engineer | b) Cyber Security Interns |
| c) Software Security Specialist | d) Security Auditor |

(iii) What is a common method used by attackers to spread malware?

- | | |
|----------------------|---------------------|
| a) Phishing emails | b) Strong passwords |
| c) Firewall settings | d) Data encryption |

(iv) Write the layer of the OSI model that IPsec operates at.

- | | |
|----------------------|--------------------|
| a) Application layer | b) Data link layer |
| c) Physical layer | d) Network layer |

(v) What does the term "split tunneling" refer to in a VPN context?

- | | |
|-------------------------------------------------------------------------|----------------------------------------------|
| a) Directing some traffic through the VPN and some through the internet | b) Creating multiple VPN tunnels |
| c) Encrypting data multiple times | d) Using multiple VPN clients simultaneously |

(vi) Choose the command that is used to create a standard ACL in Cisco IOS.

- | | |
|---------------------------------------------------------|-------------------------------------------------------|
| a) access-list 10 permit 192.168.1.0 0.0.0.255 | b) ip access-list 10 permit 192.168.1.0 0.0.0.255 |
| c) standard access-list 10 permit 192.168.1.0 0.0.0.255 | d) create access-list 10 permit 192.168.1.0 0.0.0.255 |

(vii) What is the main difference between Static NAT and Dynamic NAT?

- a) Static NAT maps a fixed IP address, while Dynamic NAT maps from a pool of addresses
b) Static NAT uses port numbers, while Dynamic NAT does not
c) Static NAT changes IP addresses dynamically, while Dynamic NAT is fixed
d) Static NAT does not support private IPs, while Dynamic NAT does
- (viii) Compare and contrast NAT and PAT.
a) NAT: One-to-One Mapping PAT: Many-to-One Mapping
b) NAT: One-to-One Mapping PAT: One-to-One Mapping
c) NAT: Many-to-many Mapping PAT: Many-to-Many Mapping
d) NAT: Many-to-One Mapping PAT: Many-to-One Mapping
- (ix) Indicate the command to display the NAT translation table.
a) show ip nat
b) show ip nat translation
c) show nat
d) All of these
- (x) Which protocol is RADIUS based on?
a) UDP
b) TCP
c) ICMP
d) HTTP
- (xi) What port does RADIUS use by default?
a) 1812
b) 80
c) 22
d) 23
- (xii) What is the purpose of using named ACLs in Cisco devices?
a) To increase processing speed
b) To enhance security
c) To provide a more descriptive and manageable way to configure ACLs
d) To simplify hardware requirements
- (xiii) Relate the security threat involves manipulating people to gain confidential information.
a) Social engineering
b) DDoS
c) Man-in-the-middle
d) Ransomware
- (xiv) Select from the options below, which of them is not a vulnerability to information security.
a) Flood
b) without deleting data, disposal of storage media
c) unchanged default password
d) latest patches and updates not done
- (xv) Which command is used to configure AAA authentication with a RADIUS server?
a) ip auth group radius
b) aaa radius enable
c) aaa authentication login default group radius
d) auth-group login radius

Group-B

(Short Answer Type Questions)

3 x 5=15

2. Write about ransomware attacks target and encrypt network data. (3)
3. How does a VPN help in bypassing geographical restrictions? (3)
4. Explain a man-in-the-middle attack, and how does it compromise network communications. (3)
5. Classify the benefits of using NAT for security purposes. (3)
6. Evaluate the role of AAA (Authentication, Authorization, and Accounting) in enforcing security policies in a network and how it can be integrated with existing security frameworks. (3)

OR

Analyze the potential challenges and solutions associated with implementing AAA mechanisms in a cloud-based environment compared to a traditional on-premises network. (3)

Group-C

(Long Answer Type Questions)

5 x 6=30

7. Analyze the function of an Access Control List (ACL) within a network security framework. (5)
8. Simplify the process of authentication in the AAA framework. (5)
9. Outline the role of authorization within AAA. (5)
10. Explain the concept of multi-factor authentication (MFA). (5)
11. Define the concept of a VPN (Virtual Private Network). (5)
12. Evaluate the role of the implicit deny rule in an ACL and its implications for network security. (5)

OR

Assess the significance of ACL order in the processing of rules and its impact on access control. (5)
