Time left 0:14:47

Question 1

Not yet answered

Marked out of 1.00

A man-in-the-middle attack on public-key systems is prevented using:

- ○ a. Digital certificates
- ○ b. IPv6
- ○ c. Hash chaining
- ○ d. Symmetric encryption only

Question 2

Not yet answered

Marked out of 1.00

A VPN provides confidentiality mainly through:

- ○ a. Encryption
- ○ b. DNS caching
- ○ c. MAC addresses
- ○ d. IP tunnelling

Question 3

Not yet answered

Marked out of 1.00

AES is a:

- ○ a. Block cipher
- ○ b. Public-key algorithm
- ○ c. Hash function
- ○ d. Stream cipher

Question 4

Not yet answered

Marked out of 1.00

DNS primarily uses which transport protocol?

- ○ a. TCP for queries, UDP for zone transfers
- ○ b. UDP only
- ○ c. TCP only
- ○ d. UDP for queries, TCP for zone transfers

Question 5

Not yet answered

Marked out of 1.00

Hash functions must satisfy all except:

○ a. Avalanche effect

○ b. Collision resistance

○ c. Key distribution

○ d. Pre-image resistance

Question 6

Not yet answered

Marked out of 1.00

HMAC provides:

○ a. Public-key verification

○ b. Integrity and Authentication

○ c. Hashing with no key

○ d. Encryption

Question 7

Not yet answered

Marked out of 1.00

In BGP, the path selection is based on:

○ a. Link bandwidth

○ b. Hop count

○ c. Shortest distance

○ d. Policy-based attributes

Question 8

Not yet answered

Marked out of 1.00

In CIDR addressing, the notation /20 indicates:

○ a. Both B and C

○ b. Subnet mask 255.255.240.0

○ c. 20 host bits

○ d. 20 network bits

Question 9

Not yet answered

Marked out of 1.00

In TCP, congestion is primarily detected by:

○ a. Packet loss or timeout
○ b. Checking IP TTL
○ c. Increasing window size
○ d. SYN flood prevention

Question 10

Not yet answered

Marked out of 1.00

In TCP, the TIME_WAIT state exists mainly to:

○ a. Prevent port reuse
○ b. Improve performance
○ c. Reduce congestion
○ d. Re-establish the connection quickly

Question 11

Not yet answered

Marked out of 1.00

Perfect forward secrecy ensures:

○ a. Messages cannot be modified
○ b. Future keys will always be secure
○ c. Past sessions cannot be decrypted even if keys are compromised
○ d. Hashes cannot be reversed

Question 12

Not yet answered

Marked out of 1.00

RSA security primarily relies on:

○ a. AES block structure
○ b. Elliptic curve problem
○ c. Discrete logarithm problem
○ d. Integer factorization problem

Question 13

Not yet answered

Marked out of 1.00

SSL/TLS uses which cryptographic mechanism during handshake?

- ○ a. Neither symmetric nor asymmetric
- ○ b. Only asymmetric keys
- ○ c. Only symmetric keys
- ○ d. Both symmetric and asymmetric keys

Question 14

Not yet answered

Marked out of 1.00

The avalanche effect in cryptography ensures:

- ○ a. Ciphertext remains stable
- ○ b. Small key changes produce large ciphertext changes
- ○ c. Keys rotate frequently
- ○ d. Blocks are padded correctly

Question 15

Not yet answered

Marked out of 1.00

The main purpose of ARP is to map:

- ○ a. IP to Port
- ○ b. Port to MAC
- ○ c. IP to MAC
- ○ d. MAC to IP

Question 16

Not yet answered

Marked out of 1.00

The main reason IPv6 removes checksum from the header is:

- ○ a. Because transport layer already checks for errors
- ○ b. To reduce header overhead
- ○ c. To reduce security
- ○ d. To maintain backward compatibility

Question 17

Not yet answered

Marked out of 1.00

The property ensuring message was not altered during transmission is:

○ a. Anonymity
○ b. Confidentiality
○ c. Availability
○ d. Integrity

Question 18

Not yet answered

Marked out of 1.00

Which attack involves tricking a device into sending frames to an attacker's MAC address?

○ a. DNS Poisoning
○ b. SYN Flood Attack
○ c. ARP Spoofing
○ d. IP Fragmentation Attack

Question 19

Not yet answered

Marked out of 1.00

Which device operates primarily at Layer 2 of the OSI model?

○ a. Switch
○ b. Router
○ c. Gateway
○ d. Firewall

Question 20

Not yet answered

Marked out of 1.00

Which field of the TCP header ensures data integrity?

○ a. Sequence Number
○ b. Checksum
○ c. Window Size
○ d. Acknowledgement Number

Question 21

Not yet answered

Marked out of 1.00

Which firewall type inspects packets at all layers including payload?

○ a. Packet-filtering firewall
○ b. Application-layer firewall
○ c. NAT firewall
○ d. Circuit-level gateway

Question 22

Not yet answered

Marked out of 1.00

Which key exchange protocol is widely used in secure communication?

○ a. SHA-256
○ b. Diffie–Hellman
○ c. RSA
○ d. ECC

Question 23

Not yet answered

Marked out of 1.00

Which layer of the OSI model is responsible for end-to-end reliable communication?

○ a. Transport Layer
○ b. Data Link Layer
○ c. Network Layer
○ d. Session Layer

Question 24

Not yet answered

Marked out of 1.00

Which mode of AES turns block cipher into stream-like cipher?

○ a. CBC
○ b. ECB
○ c. GCM
○ d. CTR

Question 25

Not yet answered

Marked out of 1.00

Which of the following ensures authentication and non-repudiation?

○ a. Digital signatures
○ b. MAC (Message Authentication Code)
○ c. Symmetric key encryption
○ d. Hashing only

Question 26

Not yet answered

Marked out of 1.00

Which of the following is a Transport Layer protocol?

○ a. OSPF
○ b. ARP
○ c. TCP
○ d. ICMP

Question 27

Not yet answered

Marked out of 1.00

Which of the following is NOT a congestion control mechanism?

○ a. Fast Retransmit
○ b. Slow Start
○ c. Error Detection
○ d. Fast Recovery

Question 28

Not yet answered

Marked out of 1.00

Which of the following uses elliptic curve mathematics?

○ a. SHA-3
○ b. ECC
○ c. RSA
○ d. DES

Question 29

Not yet answered

Marked out of 1.00

Which protocol is used for IPsec key exchange?

○ a. IKE
○ b. ISAKMP
○ c. AH
○ d. ESP

Question 30

Not yet answered

Marked out of 1.00

Which routing protocol uses Dijkstra’s shortest path algorithm?

○ a. RIP
○ b. BGP
○ c. OSPF
○ d. EIGRP