

**Which of the following is a crucial component of network security that acts as a barrier between an internal trusted network and an external untrusted network?**

- a) Firewall b) Router c) Switch d) Hub

Answer: a) Firewall

**The process of converting plaintext into a scrambled and unreadable format known as ciphertext using a secret key is called:**

- a) Encryption b) Decryption c) Hashing d) Salting

Answer: a) Encryption

**In asymmetric encryption, which key is used for encryption?**

- a) Public key b) Private key c) Shared key d) Session

key Answer: a) Public key

**Which of the following is NOT a type of network attack?**

- a) Phishing b) Malware c) Encryption d) Denial of Service (DoS)

Answer: c) Encryption

**The process of verifying the identity of a user or system before granting access to resources is known as:**

- a) Authorization b) Authentication c) Encryption d) Decryption

Answer: b) Authentication

**What is the primary purpose of a Virtual Private Network (VPN)?**

- a) To protect against malware attacks b) To secure the physical network infrastructure c) To provide secure remote access to a private network over the internet d) To prevent denial of service attacks

Answer: c) To provide secure remote access to a private network over the internet

**Which security protocol provides secure communication over a computer network by encrypting data during transmission?**

- a) HTTP b) TCP c) IP d) SSL/TLS

Answer: d) SSL/TLS

**Which cryptographic hash function is commonly used in security protocols and applications, such as SSL certificates?**

- a) MD5 b) SHA-1 c) SHA-256 d) SHA-512

Answer: c) SHA-25

**A common social engineering attack where an attacker deceives individuals into revealing sensitive information, such as passwords or credit card numbers, is called:**

a) Spoofing b) Phishing c) Brute-force attack d) Denial of Service

(DoS) Answer: b) Phishing

**Which security protocol provides secure shell access over a network and uses encryption to protect data during communication?**

a) FTP b) SMTP c) SSH d) SNMP

Answer: c) SSH

---

Which of the following statements about symmetric encryption is true? a) It uses two different keys for encryption and decryption. b) It is more secure than asymmetric encryption. c) It is slower compared to asymmetric encryption. d) Both the sender and receiver use the same key for encryption and decryption.

Answer: d) Both the sender and receiver use the same key for encryption and decryption.

The process of converting ciphertext back into plaintext using the appropriate secret key is known as: a) Encryption b) Decryption c) Hashing d) Salting

Answer: b) Decryption

What is the purpose of a Digital Signature in network security? a) To encrypt data for secure transmission b) To provide authentication of the sender's identity c) To prevent Denial of Service (DoS) attacks d) To protect against malware and viruses

Answer: b) To provide authentication of the sender's identity

Which of the following is an example of a symmetric encryption algorithm? a) RSA b) AES c) Diffie-Hellman d) ECC

Answer: b) AES

A Man-in-the-Middle (MITM) attack involves: a) Intercepting and altering data between two parties without their knowledge. b) Flooding a network with excessive traffic to disrupt services. c) Exploiting a weakness in a system to gain unauthorized access. d) Sending deceptive emails to trick users into revealing sensitive information.

Answer: a) Intercepting and altering data between two parties without their knowledge.

The process of converting passwords or other sensitive data into a fixed-length string of characters, typically for storage or comparison purposes, is known as: a) Encryption b) Decryption c) Hashing d) Salting

Answer: c) Hashing

Which of the following is an essential security measure to protect wireless networks from unauthorized access? a) Using weak and easily guessable passwords b) Enabling MAC filtering c) Disabling encryption d) Broadcasting the network SSID

Answer: b) Enabling MAC filtering

What does the term "Pharming" refer to in the context of network security? a) Forging a sender's address to appear as someone else b) Redirecting users to a malicious website by modifying DNS settings c) Sending massive amounts of traffic to a network to overload it d) Gaining unauthorized access to a system through software vulnerabilities

Answer: b) Redirecting users to a malicious website by modifying DNS settings

Which encryption protocol is commonly used to secure web traffic (HTTPS)? a) AES b) RSA c) SSL/TLS d) ECC

Answer: c) SSL/TLS

What is the purpose of an Intrusion Detection System (IDS) in network security? a) To prevent viruses and malware from infecting the network b) To identify and block unauthorized access attempts c) To encrypt data for secure transmission d) To optimize network performance and traffic routing

---

Which of the following is a common security mechanism used to protect against replay attacks in network communication?

a) Encryption b) Hashing c) Digital Signature d)

Salting Answer: c) Digital Signature

Replay attacks involve the unauthorized capture and subsequent retransmission of data packets, and digital signatures help to prevent such attacks by providing authentication and integrity of the transmitted data.

Remember to study the concepts and topics thoroughly to excel in your exams. Good luck with your preparations! If you need more questions or any further assistance, feel free to ask.



I need more questions

ChatGPT

Certainly! Here are some more multiple-choice questions for your preparation in the subject CS 315 - Network Security:

Which of the following statements best describes the role of a Certificate Authority (CA) in network security?

a) CA is responsible for managing network firewalls and intrusion detection systems. b) CA issues and manages digital certificates used for secure communication and authentication. c) CA encrypts data during transmission to protect it from eavesdropping. d) CA scans and removes malware from the network.

Answer: b) CA issues and manages digital certificates used for secure communication and authentication.

What is the purpose of a Virtual Private Network (VPN) in network security?

a) To encrypt data for secure transmission over the internet. b) To prevent unauthorized access to a physical network. c) To block malicious websites and phishing attempts. d) To scan and remove viruses from network devices.

Answer: a) To encrypt data for secure transmission over the internet.

Which of the following is NOT an example of a symmetric encryption algorithm?

a) AES (Advanced Encryption Standard) b) DES (Data Encryption Standard) c) RSA (Rivest-Shamir-Adleman) d) 3DES (Triple Data Encryption Standard)

Answer: c) RSA (Rivest-Shamir-Adleman)

What does the term "Denial of Service (DoS)" refer to in the context of network security?

a) Intercepting and altering data between two parties without their knowledge. b) Sending massive amounts of traffic to a network to overload it and disrupt services. c) Exploiting a weakness in a system to gain unauthorized access. d) Forging a sender's address to appear as someone else.

Answer: b) Sending massive amounts of traffic to a network to overload it and disrupt services.

The process of converting a hash value back into its original plaintext form is known as:

a) Encryption b) Decryption c) Hashing d) Salting

Answer: Decryption (b) is incorrect for this question; the correct answer is "c) Hashing."

What is the primary function of an Intrusion Detection System (IDS) in network security?

a) To prevent viruses and malware from infecting the network. b) To identify and block unauthorized access attempts. c) To encrypt data during transmission to protect it from eavesdropping. d) To manage network switches and routers.

Answer: b) To identify and block unauthorized access attempts.

Which of the following is a social engineering attack where an attacker deceives individuals into revealing sensitive information by posing as a trustworthy entity?

a) Phishing b) Ransomware c) Brute-force attack d) Distributed Denial of Service

(DDoS) Answer: a) Phishing

Which security protocol provides secure communication between a client and a server over an unsecured network?

a) IPsec (Internet Protocol Security) b) SSH (Secure Shell) c) SSL/TLS (Secure Sockets Layer/Transport Layer Security) d) PGP (Pretty Good Privacy)

Answer: c) SSL/TLS (Secure Sockets Layer/Transport Layer Security)

The process of converting plaintext into ciphertext using a cryptographic key is known as:

- a) Decryption
- b) Hashing
- c) Salting
- d) Encryption

Encryption Answer: d) Encryption

---

This set of Computer Fundamentals Multiple Choice Questions & Answers (MCQs) focuses on "Network Security".

1. The field that covers a variety of computer networks, both public and private, that are used in everyday jobs.
  - a) Artificial Intelligence
  - b) ML
  - c) Network Security
  - d) IT
  
2. Network Security provides authentication and access control for resources.
  - a) True
  - b) False
  
3. Which is not an objective of network security?
  - a) Identification
  - b) Authentication
  - c) Access control
  - d) Lock
  
4. Which of these is a part of network identification?
  - a) UserID
  - b) Password
  - c) OTP
  - d) fingerprint
  
5. The process of verifying the identity of a user.
  - a) Authentication
  - b) Identification
  - c) Validation
  - d) Verification

6. A concern of authentication that deals with user rights.

- a) General access
- b) Functional authentication
- c) **Functional authorization**
- d) Auto verification

7. CHAP stands for?

- a) **Challenge Handshake authentication protocol**
- b) Challenge Hardware authentication protocol
- c) Circuit Hardware authentication protocol
- d) Circuit Handshake authentication protocol

8. Security features that control that can access resources in the OS.

- a) Authentication
- b) Identification
- c) Validation
- d) **Access control**

9. An algorithm in encryption is called \_\_\_\_\_

- a) Algorithm
- b) Procedure
- c) **Cipher**
- d) Module

10. The information that gets transformed in encryption is \_\_\_\_

- a) **Plain text**
- b) Parallel text
- c) Encrypted text
- d) Decrypted text

1. WTLS stands for?
  - a) **Wireless Transport Security Layer**
  - b) Wireless Transfer System Layer
  - c) Wireless Transfer Security Layer
  - d) Wireless Transport System Layer
  
2. The protocol designed to make the security of wireless LAN as good as that of wired LAN.
  - a) WTLS
  - b) **WEP**
  - c) RSN
  - d) WP
  
3. A person who enjoys learning details about computers and how to enhance their capabilities.
  - a) Cracker
  - b) **Hacker**
  - c) App controller
  - d) Site controller
  
4. A program created by Farmer and Venema for auditing capability.
  - a) SAAS
  - b) **SATAN**
  - c) SAN
  - d) SAT
  
5. A small program that changes the way a computer operates.
  - a) Worm
  - b) Trojan
  - c) Bomb
  - d) **Virus**
  
6. A program that copies itself.
  - a) **Worm**
  - b) Virus
  - c) Trojan
  - d) Bomb

7. 7. An attack in which the site is not capable of answering valid request.
  - a) Smurfing
  - b) Denial of service
  - c) E-mail bombing
  - d) Ping storm
8. Creating a computer or paper audit that can help detect wrong doings.
  - a) Auditing
  - b) Validation
  - c) RSN
  - d) Verification
9. An indirect form of surveillance.
  - a) Honey pot
  - b) Logical
  - c) Security
  - d) Intrusion
10. A malicious code hidden inside a seemingly harmless piece of code.
  - a) Worm
  - b) Bomb
  - c) Trojan Horse
  - d) Virus
11. Attack in which a user creates a packet that appears to be something else.
  - a) Smurfing
  - b) Trojan
  - c) E-mail bombing
  - d) Spoofing
12. A technique in which a program attacks a network by exploiting IP broadcast addressing operations.
  - a) Smurfing
  - b) Denial of service
  - c) E-mail bombing
  - d) Ping storm

14. An attack in which the user receives unwanted amount of e-mails.

- a) Smurfing
- b) Denial of service
- c) E-mail bombing
- d) Ping storm

15. A cipher in which the order is not preserved.

- a) Polyalphabetic substitution based
- b) Transposition-based
- c) Substitution based
- d) Public key based

16.2. Plain text is the data after encryption is performed.

- a) True
- b) False

17.3. A unique piece of information that is used in encryption.

- a) Cipher
- b) Plain Text
- c) Key
- d) Cipher

3. Study of creating a d using encryption and decryption techniques.

- a) Cipher
- b) Cryptography
- c) Encryption
- d) Decryption

4. The process of transforming plain text into unreadable text.

- a) Decryption
- b) Encryption
- c) Network Security
- d) Information Hiding

5. An algorithm used in encryption is referred to as cipher.  
a) True  
b) False
6. A process of making the encrypted text readable again.  
a) Decryption  
b) Encryption  
c) Network Security  
d) Information Hiding
1. These ciphers replace a character or characters with a different character or characters, based on some key.  
a) Polyalphabetic substitution based  
b) Transposition-based  
c) Substitution based  
d) Mono alphabetic substitution based
2. Encryption is the study of creating and using decryption techniques.  
a) True  
b) False
2. A type of cipher that uses multiple alphabetic strings.  
a) Substitution based  
b) Transposition-based  
c) Polyalphabetic substitution based  
d) Mono alphabetic substitution based
3. An encryption technique with 2 keys is \_\_\_\_\_  
a) Monoalphabetic Cipher  
b) Cryptography  
c) Private key cryptography  
d) Public key cryptography

4. In public key cryptography, a key that decrypts the message.
- a) public key
  - b) unique key
  - c) private key
  - d) security key
5. DES stands for?
- a) Data Encryption Standard
  - b) Data Encryption Statistics
  - c) Data Encryption System
  - d) Data Encryption Sequence
6. Under DES, the data encryption standard took a 64-bit block of data and subjected it to \_\_\_\_ levels of encryption.
- a) 64
  - b) 8
  - c) 16
  - d) 4
7. Triple-DES has \_\_\_\_ keys.
- a) 1
  - b) 2
  - c) 5
  - d) 4
8. Encryption standard that is selected by the US government to replace DES.
- a) AES
  - b) BES
  - c) CES
  - d) DES

9. An electronic document that establishes your credentials when you are performing transactions.

- a) Digital code
- b) OTP
- c) E-mail
- d) Digital certificate

10.