Cisco

CCST-Cybersecurity Exam

Questions & Answers

(Demo Version - Limited Content)

Thank you for Downloading CCST-Cybersecurity exam PDF Demo

Get Full File:

https://www.certkillers.net/Exam/CCST-Cybersecurity

Question: 1

What is a common security threat in which an attacker attempts to overwhelm a targeted system by flooding it with Internet traffic?

A. Ransomware

B. Distributed Denial of Service (DDoS) attack

C. Phishing

D. SQL injection

Answer: B

Explanation:

Option 1: Ransomware is a type of malicious software that encrypts a victim's files and demands a ransom in exchange for the decryption key. While it can cause damage to systems, it is not specifically designed to overwhelm a system with Internet traffic. Option 2: Correct. A Distributed Denial of Service (DDoS) attack is a common security threat in which an attacker attempts to overwhelm a targeted system by flooding it with Internet traffic. This can result in a loss of service availability for legitimate users. Option 3: Phishing is a type of social engineering attack in which an attacker masquerades as a trustworthy entity to trick individuals into providing sensitive information. It does not involve overwhelming a system with Internet traffic. Option 4: SQL injection is a type of web application attack in which an attacker manipulates a SQL query to gain unauthorized access to a database. It does not involve overwhelming a system with Internet traffic.

Question: 2

Which of the following statements about multi-factor authentication (MFA) is correct?

A. MFA is a security measure that requires users to provide two or more forms of identification to gain access to a system or application.

B. MFA is a security measure that requires users to provide only one form of identification to gain access to a system or application

C. MFA is a security measure that is no longer recommended due to its complexity and potential for user errors.

D. MFA is a security measure that only applies to physical access control systems.

Answer: A

Explanation:

Option 1: This is the correct statement. MFThis is a security measure that requires users to provide two or more forms of identification to gain access to a system or application. It adds an extra layer of security by combining multiple credentials, such as passwords, one-time passcodes, biometrics, or smart cards, to verify a user's identity. Option 2: This statement is incorrect. MFA requires users to provide two or more forms of identification, not just one. Option 3: This statement is incorrect. MFThis is still recommended as an effective security measure and is widely used in many industries. Option 4: This statement is incorrect. MFA can be used for both physical and logical access control systems.

Question: 3

Which of the following is a common security threat that targets web applications?

A. SQL injection
B. DNS poisoning
C. Man-in-the-middle attack
D. Distributed Denial of Service (DDoS)

Answer: A

Explanation:

Option 1: Correct: SQL injection is a common security threat that targets web applications. It involves inserting malicious SQL code into input fields to manipulate the application's database and gain unauthorized access or retrieve sensitive information. Option 2: Incorrect: DNS poisoning is not a common security threat that targets web applications. It involves corrupting the DNS cache and redirecting users to malicious websites. Option 3: Incorrect: Man-in-the-middle attack is not a common security threat that specifically targets web applications. It involves intercepting communication between two parties and can affect various types of network communication. Option 4: Incorrect: Distributed Denial of Service (DDoS) is not a common security threat that targets web applications specifically. It involves overwhelming a target system with a flood of traffic from multiple sources, rendering it inaccessible.

Question: 4

Which of the following protocols can be used to securely transfer files over a network?

A. HTTP
B. FTP
C. SMTP
D. DNS

Answer: B

Explanation:

Option 1: Incorrect. HTTP is a protocol for transferring hypertext documents, not files. Option 2: Correct. FTP (File Transfer Protocol) is a protocol used for secure file transfer over a network. Option 3: Incorrect. SMTP is a protocol used for sending email, not transferring files. Option 4: Incorrect. DNS is a protocol used for translating domain names to IP addresses, not transferring files.

Question: 5

Which feature allows endpoints to communicate directly with each other, bypassing the network?

A. Firewall
B. IPS
C. VPN
D. Peer-to-Peer

Answer: D

Explanation:

Option 1: Incorrect. A firewall is a network security device that monitors and filters incoming and outgoing network traffic based on predetermined security rules. Option 2: Incorrect. An IPS (Intrusion Prevention System) is a network security device that monitors network traffic for malicious activity and takes immediate action to prevent attacks. Option 3: Incorrect. A VPN (Virtual Private Network) is a secure connection between two or more endpoints over a public network, providing encryption and privacy for data communication. Option 4: Correct. Peer-to-peer (P2P) is a decentralized communication model where endpoints can directly communicate with each other without the need for a central server or network infrastructure.

Thank You for trying CCST-Cybersecurity PDF Demo

https://www.certkillers.net/Exam/CCST-Cybersecurity

Start Your CCST-Cybersecurity Preparation

[Limited Time Offer] Use Coupon "CKNET " for further discount the purchase of PDF file. Test your CCST-Cybersecurity preparation with actual exam questions