Exam Name: Cisco Certified Support Technician (CCST) Cybersecurity
Exam Code: 100-160 CCST Cybersecurity_V_1.0
Total No. of Questions In Dumps: 300
Total no. of questions in Real Exam: 50
Passing Percentage: 70
Exam Duration: 50 minutes

Contact Us

Website: www.originaldumps.com
Email Id:Info@originaldumps.com
Contact: +91-8102473804

QUESTION: 1

Which of the following is a key component of a Security Incident Response Plan?

Option A : gularly testing and updating the plan
Option B : igning blame to individuals involved in the incident
Option C : noring incidents that do not have a significant impact
Option D : plementing security measures after an incident occurs

Correct Answer: A

Explanation/Reference:

Option 1: Correct. Regularly testing and updating the plan is an essential component of a Security Incident Response Plan. It ensures that the plan remains effective and up to date. Option 2: Incorrect. Assigning blame to individuals involved in the incident is not a recommended practice in a Security Incident Response Plan. The focus should be on resolving the incident and preventing future occurrences. Option 3: Incorrect. Ignoring incidents that do not have a significant impact is not a best practice. All incidents should be investigated and classified according to their severity. Option 4: Incorrect. Implementing security measures after an incident occurs is not sufficient. Proactive security measures should be in place before an incident happens.

QUESTION: 2

Which AWS service can be used to secure data at rest in Amazon S3?

Option A : CloudTrail
Option B : Key Management Service (KMS)
Option C : Identity and Access Management (IAM)
Option D : Shield

Correct Answer: B

Explanation/Reference:

Option 1: AWS CloudTrail is a service for logging and monitoring account activity, and does not directly secure data at rest in Amazon S Option 2: AWS Key Management Service (KMS) is the correct answer. It is a managed service that makes it easy for you to create and control the encryption keys used to encrypt your data, and manages the underlying hardware and software needed for the cryptographic operations. Option 3: AWS Identity and Access Management (IAM) is a service for managing user access and permissions, and does not directly secure data at rest in Amazon S Option 4: AWS Shield is a managed Distributed Denial of Service (DDoS) protection service, and does not directly secure data at rest in Amazon S

QUESTION: 3

Which feature provides secure remote access to corporate resources while ensuring confidentiality, integrity, and authenticity of the data transmitted over the internet?

Option A : rtual Private Network (VPN)
Option B : cure Shell (SSH)
Option C : cure Sockets Layer (SSL)
Option D : trusion Detection System (IDS)

Correct Answer: A

Explanation/Reference:

Option 1: Virtual Private Network (VPN) is the correct answer. VPN provides a secure remote access solution by encrypting the data transmitted over the internet, ensuring confidentiality. It also uses protocols like IPSec to provide integrity and authentication, ensuring that the data is not tampered with and the users are verified. Option 2: Secure Shell (SSH) is incorrect. SSH is primarily used for secure remote logins to a server or device. While it provides encryption and authentication, it does not offer the same level of network-wide secure remote access as a VPN. Option 3: Secure Sockets Layer (SSL) is incorrect. SSL is primarily used to establish secure connections between a client and a server, such as during HTTPS communication. While it provides encryption and authentication, it does not provide the same level of secure remote access capabilities as a VPN. Option 4: Intrusion Detection System (IDS) is incorrect. IDS is a security system that monitors network traffic for suspicious activity and helps detect and respond to potential intrusions. It does not provide secure remote access functionality like a VPN.

QUESTION: 4

Which of the following best describes a Man-in-the-Middle (MitM) attack?

Option A : attacker intercepts communication between two parties to steal information or conduct malicious activity.
Option B : attacker floods a network with traffic to overwhelm and disrupt normal operations.
Option C : attacker gains unauthorized access to a system by exploiting a vulnerability.
Option D : attacker tricks a user into clicking a malicious link or downloading a harmful file.

Correct Answer: A

Explanation/Reference:

Option 1: Correct: A Man-in-the-Middle (MitM) attack occurs when an attacker intercepts communication between two parties to steal information or conduct malicious activity. The attacker positions themselves between the two parties, capturing data as it flows between them. Option 2: Incorrect: This answer describes a Denial-of-Service (DoS) attack, not a Man-in-the-Middle (MitM) attack. In a DoS attack, an attacker floods a network with traffic to overwhelm and disrupt normal operations. Option 3: Incorrect: This answer describes unauthorized access via exploitation of vulnerabilities, which is a different type of attack. It does not involve intercepting communication between two parties, which is a characteristic of a Man-in-the-Middle (MitM) attack. Option 4: Incorrect: This answer describes a phishing attack, where an attacker tricks a user into clicking a malicious link or downloading a harmful file. While phishing attacks can be part of a broader MitM attack, the specific definition of a MitM attack is intercepting communication between two parties.

QUESTION: 5

What security measure can be used to protect data in transit between a user's device and a cloud service?

Option A : TPS
Option B : N
Option C : L
Option D : H

Correct Answer: B

Explanation/Reference:

Option 1: Incorrect. HTTPS is a secure protocol used for encrypting communication between a web browser and a web server. Option 2: Correct. A VPN (Virtual Private Network) can be used to create a secure, encrypted tunnel between a user's device and a cloud service, protecting the data in transit. Option 3: Incorrect. SSL (Secure Sockets Layer) is a deprecated protocol that was used for securing data in transit. Option 4: Incorrect. SSH (Secure Shell) is a secure protocol used for remote login and command execution, and is not typically used for protecting data in transit between a user's device and a cloud service.

QUESTION: 6

Which of the following is NOT a common security threat inside the Common Security Threats section of CCST Cybersecurity?

Option A : lware
Option B : cial Engineering
Option C : rewall
Option D : ishing

Correct Answer: C

Explanation/Reference:

Option 1: Incorrect. Malware is a common security threat inside the Common Security Threats section of CCST Cybersecurity. Malware refers to malicious software, such as viruses, worms, trojans, and ransomware, that can infect and harm computer systems. Option 2: Incorrect. Social Engineering is a common security threat inside the Common Security Threats section of CCST Cybersecurity. Social Engineering refers to the manipulation of people into performing actions or divulging confidential information, often through deceptive techniques. Option 3: Correct. Firewall is not a common security threat inside the Common Security Threats section of CCST Cybersecurity. A firewall is a security device that monitors and filters network traffic based on predetermined security rules and policies. While firewalls can help mitigate security threats, they are not themselves a threat. Option 4: Incorrect. Phishing is a common security threat inside the Common Security Threats section of CCST Cybersecurity. Phishing refers to attempts to deceive individuals into providing sensitive information, such as passwords or credit card numbers, by impersonating a trustworthy entity through electronic communication.

QUESTION: 7

Which feature in Windows 10 allows administrators to manage, secure, and monitor devices within an organization?

Option A : ndows Defender Firewall
Option B : crosoft Intune
Option C : ndows Defender SmartScreen
Option D : tLocker Drive Encryption

Correct Answer: B

Explanation/Reference:

Option 1: Incorrect. Windows Defender Firewall is a feature that provides network protection and controls inbound and outbound network traffic. It does not allow administrators to manage, secure, and monitor devices within an organization. Option 2: Correct. Microsoft Intune is a cloud-based endpoint management solution that allows administrators to manage, secure, and monitor devices within an organization. It provides features such as device enrollment, policy management, software deployment, and remote device management. Option 3: Incorrect. Windows Defender SmartScreen is a feature that helps protect users from malicious websites and downloads. It does not allow administrators to manage, secure, and monitor devices within an organization. Option 4: Incorrect. BitLocker Drive Encryption is a feature that provides full disk encryption for Windows devices. It does not allow administrators to manage, secure, and monitor devices within an organization.

QUESTION: 8

Which of the following is a best practice for securing sensitive data in transit?

Option A : ing HTTP over TLS (HTTPS)
Option B : ing FTP
Option C : ing Telnet
Option D : ing unencrypted HTTP

Correct Answer: A

Explanation/Reference:

Option 1: Using HTTP over TLS (HTTPS) is the correct answer. HTTPS encrypts the data in transit and ensures that it cannot be intercepted or modified by unauthorized entities. Option 2: Using FTP is incorrect because FTP does not encrypt data in transit by default. It can expose sensitive information to eavesdropping and tampering. Option 3: Using Telnet is incorrect because Telnet does not encrypt data in transit. It sends information in clear text, making it vulnerable to interception and unauthorized access. Option 4: Using unencrypted HTTP is incorrect because it does not provide any encryption for data in transit. Data sent over unencrypted HTTP can be intercepted and tampered with by attackers.

QUESTION: 9

Which of the following is a network-level security threat that targets the network infrastructure to disrupt network functionality or gain unauthorized access?

Option A : lware
Option B : ute-force attack
Option C : tributed Denial of Service (DDoS)
Option D : cial Engineering

Correct Answer: C

Explanation/Reference:

Option 1: Incorrect. Malware refers to various malicious software programs that can be used to damage or gain unauthorized access to computer systems, but it is not specifically focused on targeting network infrastructure. Option 2: Incorrect. A brute-force attack is a trial-and-error method used by attackers to decode encrypted data or discover passwords by systematically trying all possible combinations. While it can impact network security, it does not specifically target the network infrastructure itself. Option 3: Correct. Distributed Denial of Service (DDoS) is a network-level security threat that floods a targeted system or network with an overwhelming amount of traffic, rendering it unavailable to legitimate users. It disrupts network functionality and can lead to unauthorized access. Option 4: Incorrect. Social engineering involves manipulating individuals to disclose confidential information or perform actions that compromise security. While it can impact network security, it is not specifically focused on targeting network infrastructure.

QUESTION: 10

Which of the following is an important component of security policies and procedures?

Option A : rewall
Option B : tivirus software
Option C : word policy
Option D : trusion detection system

Correct Answer: C

Explanation/Reference:

Option 1: Incorrect. While a firewall is an important security tool, it is not specifically related to security policies and procedures. Firewalls help protect networks by implementing access control policies, but they are not policies themselves. Option 2: Incorrect. Antivirus software is an essential tool for protecting against malware, but it is not directly related to security policies and procedures. Security policies and procedures provide guidelines and rules for managing security risks in an organization. Option 3: Correct. A password policy is an important component of security policies and procedures. It specifies requirements for creating and managing passwords, such as minimum length, complexity, and expiration. Option 4: Incorrect. An intrusion detection system (IDS) is a security tool that monitors network traffic for suspicious activity, but it is not directly related to security policies and procedures. Policies and procedures define how security controls are implemented and managed.