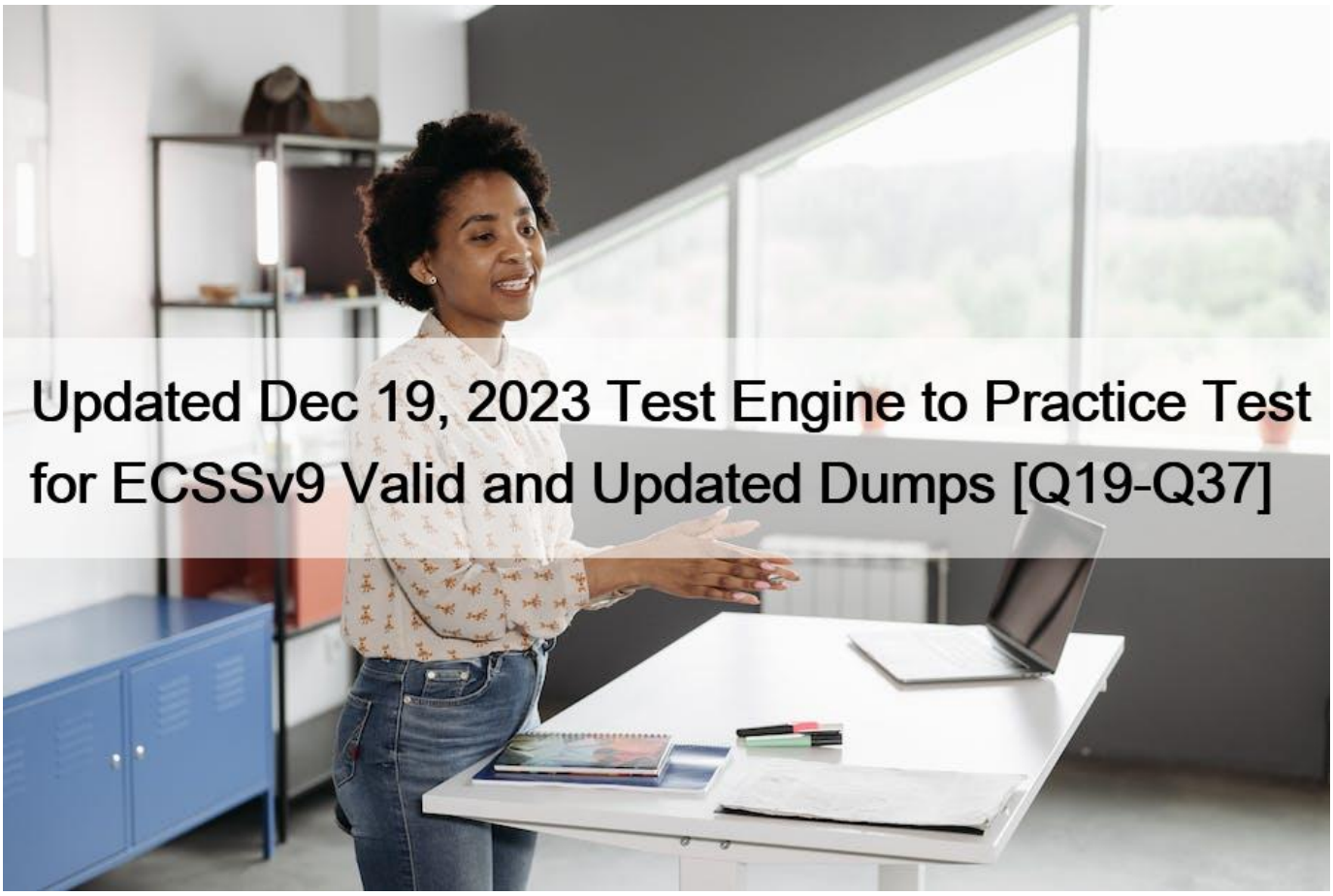
Updated Dec 19, 2023 Test Engine to Practice Test for ECSSv9 Valid and Updated Dumps [Q19-Q37



Updated Dec 19, 2023 Test Engine to Practice Test for ECSSv9 Valid and Updated Dumps
Exam Questions for ECSSv9 Updated Versions With Test Engine

The ECSSv9 certification exam includes multiple-choice questions that cover a wide range of security topics. ECSSv9 exam is designed to test the candidate's ability to understand and implement security solutions in different scenarios. ECSSv9 exam consists of 50 questions, and candidates have two hours to complete it. The passing score for the ECSSv9 exam is 70%, and candidates who pass the exam are awarded the EC-Council Certified Security Specialist v9 certification.

QUESTION 19

Which of the following describes a technological response to phishing attacks?
* User training and awareness.
* Spam filters.
* Private lawsuits.
* FTC investigations.

Explanation: Anti-phishing responses include the development of technical tools, to protect users from phishing attacks, such as increased browser security, new login protocols, and the implementation of spam filters.

QUESTION 20

Encryption strength is a measure of:
* The encryption’s ability to resist brute force attacks.
* How difficult the encryption is to implement.
* How practical the encryption is to break.
* None of these answers are correct.

Explanation: Encryption strength is a measure of the encryption’s ability to resist brute force attacks. This is determined by the encryption community. The remaining items are not related to the definition of encryption strength.

QUESTION 21

_____ is anything that can negatively affect information.
* None of these answers are correct
* An information security threat
* A rule
* A threat

Explanation: An information security threat is anything that can negatively affect information. A threat doesn’t deal specifically with information, and a rule is used to protect information.

QUESTION 22

The operating system uses _____ to ensure users have authorised access to the computer system.
* augmentation
* authorization
* availability
* authentication

Explanation: The OS uses authentication to ensure that the user accessing a program is authorised or legitimate.

QUESTION 23

A key is:
* An external piece of information used in the encryption and decryption process.
* The same for encryption and decryption in symmetric encryption.
* All of these answers are correct.
* Different for encryption and decryption in asymmetric encryption.

Explanation: Each describes a characteristic of a key, in certain situations.

QUESTION 24

What is cryptography?
* Cryptography is the process of encrypting data keys in transmission or in storage preventing unauthorised key decryption on receipt
* Cryptography is the process of authenticating data in transmission or in storage before user access is permitted
* Cryptography is the process of authenticating software encoding in transmission for user access to be permitted
* Cryptography is the process of encrypting data in transmission or in storage preventing unauthorised access or snooping

Explanation: Cryptography is defined as the system by which data and information of value are stored or transmitted in such a way

that only those for whom it is intended can read, interpret or process it.

QUESTION 25

On the staff of Kumquat Computing, Inc.-

* Jarded’s main task is to protect the confidentiality of a customer database that’s kept on a LAN in the lobby and waiting rooms.

* Tyrone’s main task is to protect the confidentiality of client files that are stored in the cloud.

Which is true of Jared’s and Tyrone’s main tasks?
* Both Jared and Tyrone are doing information security and cybersecurity.
* Jared is doing information security. Tyrone is doing both information security and cybersecurity.
* Both Jared and Tyrone are doing information security. Neither of them is doing cybersecurity.
* Jared is doing information security only. Tyrone is doing cybersecurity only.

Explanation: Information security includes three basic tenets: Confidentiality, Integrity and Availability. It entails the security of information either stored in digital form or otherwise while cybersecurity entails the protection of all data, devices and networks in digital form.

QUESTION 26

A Bluetooth device’s unique address is _____?
* BD_MAC
* BD_ID
* BD_ADDR
* BD_ADD

Explanation: Bluetooth devices transmit an unique identifier BD_ADDR, similar to a MAC Address.

QUESTION 27

A/An _____ can happen if you’re not careful when using public Wi-Fi.
* DDoS attack
* man-in-the-middle attack
* SSID launch
* encryption lapse

Explanation: A man-in-the-middle is when a hacker broadcasts a phoney SSID to fool a public Wi-Fi user.

QUESTION 28

Strictly speaking, which of the following is NOT a Linux distribution?
* CentOS
* Debian
* Android
* Kali

Explanation: Android uses the Linux kernel, but technically is not a Linux distribution.

QUESTION 29

Which is considered the ‘ethical’ hacker?

* The grey hat
* The white hat
* There is no such thing as an ‘ethical hacker’.
* The black hat

QUESTION 30

Asymmetric encryption uses:
* The same key for encryption and decryption.
* Different keys for encryption and decryption.
* A key for decryption, but no key for encryption.
* A key for encryption, but no key for decryption.

Explanation: Asymmetric encryption uses different keys for encryption and decryption. The remaining items either do not describe asymmetric encryption, or would produce unreadable information.

QUESTION 31

Which term is used to describe the attack virus that is easily transferred to a device without asking for any permission?
* Bluesnarfing
* BlueBorne
* Bluejacking
* BlueStacking

QUESTION 32

Which of the following intrusion detection methods deals with known patterns or attributes?
* Anomaly
* Signature
* Passive
* Reactive

Explanation: Signature is the intrusion detection method that deals with known patterns or attributes. Passive, anomaly, and reactive deal with other things.

QUESTION 33

Encryption is based on _____.
* Phrenology
* Chronology
* Cryptography
* Cartography

Explanation: Encryption is based on cryptography. Cryptography is the art of hiding information to make it unreadable without special knowledge or a key.

QUESTION 34

Which of the following distributions is no longer available?
* Fedora
* CentOS
* Red Hat
* Debian

Explanation: Red Hat was discontinued in 2003, although its Enterprise distribution remains active.

QUESTION 35

What type of information is typically subject to phishing attacks?
* All answers are correct.
* Social security numbers.
* Bank account numbers.
* Passwords.

Explanation: Phishing schemes target personal and sensitive information that can be exploited for the phishers financial gain. These include passwords, usernames, bank account numbers, and social numbers.

QUESTION 36

Which organisation created the suggested standard for communications that describes how data is sent and received over a network?
* Federal Communications Commission (FCC)
* International Organisation for Standardisation (ISO)
* World Wide Web Consortium (W3C)
* American Communication Consortium (ACC)

Explanation: The OSI model is a suggested standard for communication that was developed by the International Organisation for Standardisation (ISO). It describes how data is sent and received over a network and breaks down data transmission over a series of seven layers.

QUESTION 37

Fire is an example of a _____ information security threat.
* External
* Physical
* Logical
* Internal

Explanation: Fire is an example of a physical information security threat. Internal are external threat categories, and logic is not related to threats.