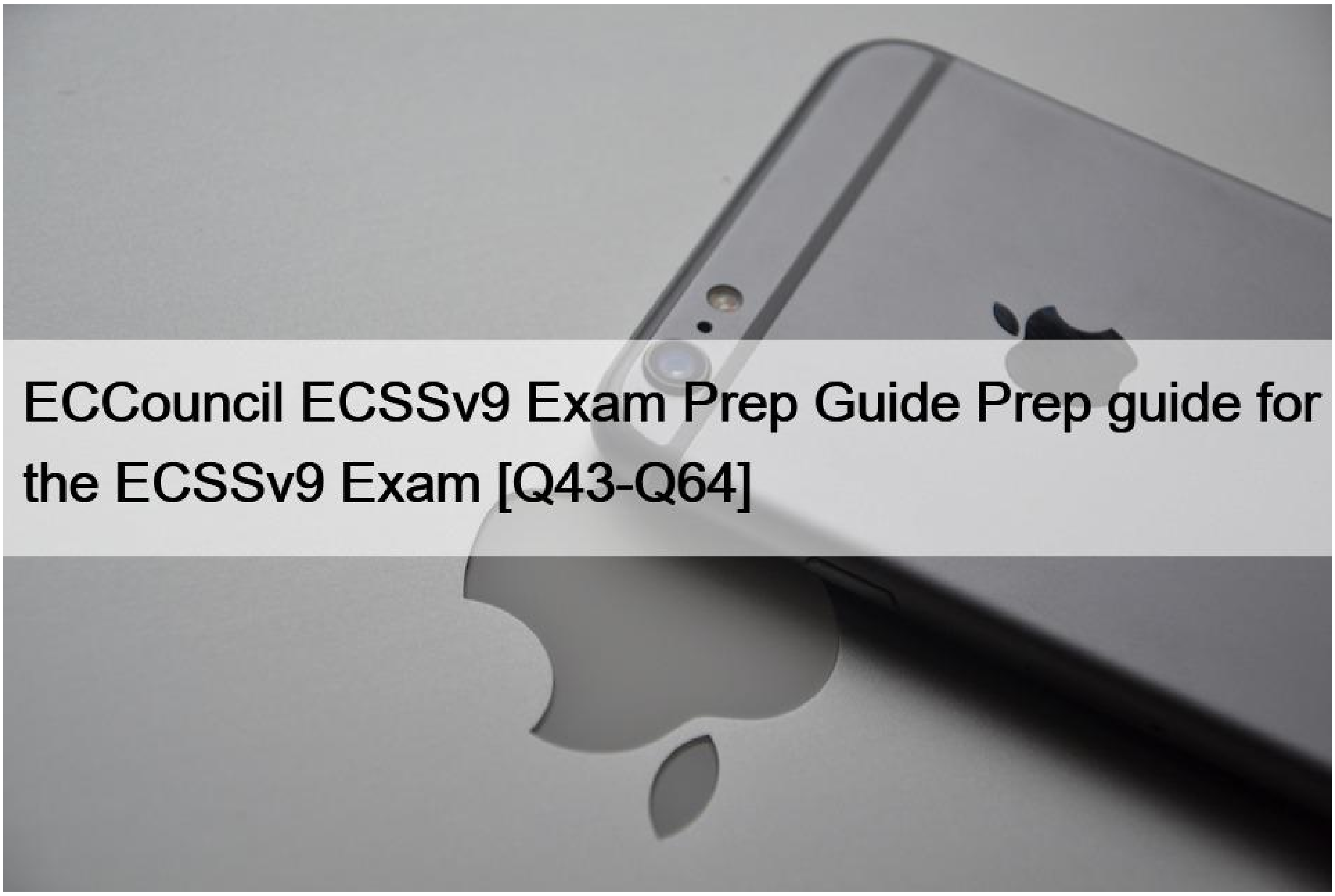
ECCouncil ECSSv9 Exam Prep Guide Prep guide for the ECSSv9 Exam [Q43-Q64



ECCouncil ECSSv9 Exam Prep Guide: Prep guide for the ECSSv9 Exam 2023 New Preparation Guide of ECCouncil ECSSv9 Exam

The ECSSv9 certification exam is recognized by many organizations around the world and is often a requirement for jobs in the field of information security. It is also a valuable credential for individuals who want to advance their careers in this field. EC-Council Certified Security Specialist v9 certification demonstrates that an individual has the knowledge and skills needed to secure information systems and protect against cyber threats.

NEW QUESTION 43

A phishing attack that incorporates personal information about the user is known as which of the following?
* DNS copying.
* Spear phishing.
* Website spoofing.
* Spam filtering.

Explanation: Spear phishing schemes use personal information of the victim to increase the probability of the success of the attack.

NEW QUESTION 44

One of the main points of vulnerability of a system is that data in _____ is not encrypted.
* transmission
* use
* storage
* devices
Explanation: Data in use on the system is not encrypted. There is a point of vulnerability of the system while files are in use.

NEW QUESTION 45

Secure user authentication in cryptography is achieved by _____.
* data authentication
* password encryption
* user checksums
* password compressions
Explanation: The encrypted passwords are similar to the private keys used to decrypt the resources the password has access to.

NEW QUESTION 46

Computer security is:
* the maintenance of system integrity, availability and confidentiality at all times
* the regulation by the access-control model of data files and folders
* the maintenance of the integrity and availability of the system firewall at all times
* the maintenance of the integrity of the operating system at all times
Explanation: The three important elements of computer security are confidentiality, integrity and availability (CIA).

NEW QUESTION 47

Digital evidence is said to be authentic when _____.
* it is similar to the original, originates from the purported device, and timestamps associated with the data are correct.
* it is unchanged, originates from the purported device, and timestamps associated with the data are correct.
* it is unchanged, originates from the purported device, and timestamps associated with the data are inconsistent.
* it is based on hearsay, unchanged and similar to the original.

NEW QUESTION 48

The operating system&#8217;s role in the protection of the system from physical threats involves:
* providing tools to enable system backups and restoration of the OS itself, files, programs and data
* providing port scanning mechanisms
* triggering denial of service attacks to prevent malicious users from using the system
* providing tools to enable system firewall deployments
Explanation: The physical security of a system is external to the OS and has to be ensured by physical or external security measures. The OS comprises systems that enable users to create backups of programs and data that will facilitate a successful restore following any physical threat.

NEW QUESTION 49

Annabelle, the CEO of Kumquat Computing, Inc., emails her vice president, Roland, to discuss an upcoming merger. Evelyn intercepts the email and changes the content of the message, altering the proposed terms of the merger, before Roland sees it. Which of these is true?
* This describes a Man-in-the-Middle attack. Roland will probably NOT realise that the email was tampered with.
* This describes a Phishing attack. Roland will probably realise that the email was tampered with.
* This describes a Man-in-the-Middle attack. Roland will probably realise that that the email was tampered with.
* This describes a Phishing attack. Roland will probably NOT realise the email was tampered with.

NEW QUESTION 50

A Bluetooth device&#8217;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.

NEW QUESTION 51

Copies of originals of digital evidence are used as best evidence to ensure _____.
* photocopiers, scanners and other replicating devices are properly utilised.
* the original evidence is kept hidden from the culprit.
* there is no misrepresentation or damage to the original evidence.
* every member of the courtroom has a copy of the evidence.

NEW QUESTION 52

How can you tell if an account on social media has been compromised?
* Check Internet lists of compromised accounts
* Avoid password reuse
* Update security regularly
* Constantly monitor sites

NEW QUESTION 53

IPv4 requires that every system with connectivity to the Internet have a unique

_____ internet address.
* 64-bit
* 32-bit
* 16-bit
* 128-bit

NEW QUESTION 54

Which of the following distributions was designed primarily for security and penetration testing?
* Red Hat
* Fedora
* Debian
* Kali

Explanation: Kali is a Linux distribution designed primarily for security and penetration testing.

NEW QUESTION 55

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.

NEW QUESTION 56

The CIA model of information security contains what three principles?
* Confidentiality, Integrity, and Authorization
* Completion, Invisibility, and Accuracy
* Integrity, Confidentiality, and Availability
* Authentication, Corroboration, and Integrity
Explanation: The CIA model relies on confidentiality, integrity, and availability to secure and protect information.

NEW QUESTION 57

Bluesnarfing requires which of these?
* Device passcode
* The BD_ADDR identifier
* Authentication by the target
* Wifi access
Explanation: For Bluesnarfing, the BD_ADDR is needed. This can be obtained by a brute-force attack, but there are 8.4 Million possible combinations.

NEW QUESTION 58

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.

NEW QUESTION 59

A program which stands as a barrier between a computer system and external traffic is known as _____.
* a firewall
* a firethorn
* a firebomb
* a fire-board
Explanation: The firewall is a program that controls incoming and outgoing traffic to a system.

NEW QUESTION 60

Which of the following distributions is the oldest?
* Kali
* openSUSE
* Debian
* Ubuntu
Explanation: Debian is one of the oldest Linux distributions, dating back to 1993.

NEW QUESTION 61

Ransomware is a malicious program that can encrypt intercepted data. The attacker controlling the software can demand a ransom before allowing the data to be decrypted, rendering it useless until the price is paid. Which of the following is TRUE about ransomware?
* Up-to-date antivirus software will effectively prevent all possible ransomware attacks.
* Using a VPN to exchange information prevents it from being encrypted, making ransomware attacks impossible.
* Defining a password security policy will prevent system infection with ransomware.
* Ransomware is a type of malware.
Explanation: The effect of a ransomware is that of performing malicious operations that effectively makes it a malware.

NEW QUESTION 62

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.

NEW QUESTION 63

Which of the following is NOT a characteristic of an intrusion detection system?
* Identifies patterns
* Continually monitors
* Blocks attacks
* Generates alerts
Explanation: Blocking attacks is NOT a characteristic of an intrusion detection system. The attack has already occured by the time an intrusion detection system is activated.

NEW QUESTION 64

HTTPS _____ the data sent between your web browser and the web site.
* authenticates
* encapsulates
* intercepts
* encrypts

The EC-Council Certified Security Specialist (ECSSv9) exam is a certification program designed to provide individuals with a comprehensive understanding of the essential principles of information security. It is an entry-level certification that focuses on foundational knowledge and skills required to develop a career in the security industry. The ECSSv9 certification is vendor-neutral, meaning that it is not tied to any specific technology or product, making it a valuable asset to any organization.

Latest Questions ECSSv9 Guide to Prepare Free Practice Tests:
https://www.test4engine.com/ECSSv9_exam-latest-braindumps.html]