2022 Latest EC-COUNCIL 212-81 Real Exam Dumps PDF [Q114-Q132

2022 Latest EC-COUNCIL 212-81 Real Exam Dumps PDF
212-81 Exam Dumps, 212-81 Practice Test Questions

EC-COUNCIL 212-81 Exam Syllabus Topics:

TopicDetailsTopic 1- Server-based Certificate Validation Protocol- Classification of Random Number GeneratorTopic 2- Steganography Implementations- Example of Symmetric Stream Ciphers: RC4Topic 3- Symmetric Cryptography & Hashes- Single Substitution WeaknessesTopic 4- Number Theory and Asymmetric Cryptography- Advanced Encryption Standard (AES)Topic 5- International Data Encryption Algorithm (IDEA)- History of CryptographyTopic 6- Shiva Password Authentication Protocol (S-PAP)- Challenge-Handshake Authentication Protocol (CHAP)Topic 7- Cracking Modern Cryptography: Ciphertext-only and Related-key Attack- Cracking Modern Cryptography: Chosen Plaintext Attack

NEW QUESTION 114

Network of trusted certificate authority servers. Use asymmetric key pairs and combines software, encryption and services to provide a means of protecting security of business communication and transactions.
* PKI
* GOST
* CA
* PIKE
PKI

https://en.wikipedia.org/wiki/Public_key_infrastructure

A public key infrastructure (PKI) is a set of roles, policies, hardware, software and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption. The purpose of a PKI is to facilitate the secure electronic transfer of information for a range of network activities such as e-commerce, internet banking and confidential email. It is required for activities where simple passwords are an inadequate authentication method and more rigorous proof is required to confirm the identity of the parties involved in the communication and to validate the information being transferred.

Incorrect answers:

PIKE &#8211; stream cipher was invented by Ross Anderson to be a &#8220;leaner and meaner&#8221; version of FISH after he broke FISH in 1994. Its name is supposed to be a humorous allusion to the pike fish.

GOST &#8211; hash function, defined in the standards GOST R 34.11-94 and GOST 34.311-95 is a 256-bit cryptographic hash function. It was initially defined in the Russian national standard GOST R 34.11-94 Information Technology &#8211; Cryptographic Information Security &#8211; Hash Function. The equivalent standard used by other member-states of the CIS is GOST 34.311-95.

CA &#8211; certificate authority or certification authority (CA) is an entity that issues digital certificates. A digital certificate certifies the ownership of a public key by the named subject of the certificate. This allows others (relying parties) to rely upon signatures or on assertions made about the private key that corresponds to the certified public key. A CA acts as a trusted third party-trusted both by the subject (owner) of the certificate and by the party relying upon the certificate. The format of these certificates is specified by the X.509 or EMV standard.

NEW QUESTION 115

Which of the following is required for a hash?
* Not vulnerable to a brute force attack
* Few collisions
* Must use SALT
* Not reversible
* Variable length input, fixed length output
* Minimum key length
Correct answers: Variable length input, fixed length output and Not reversible

https://en.wikipedia.org/wiki/Hash_function

A hash function is any function that can be used to map data of arbitrary size to fixed-size values. The values returned by a hash function are called hash values, hash codes, digests, or simply hashes. The values are used to index a fixed-size table called a hash table. Use of a hash function to index a hash table is called hashing or scatter storage addressing.

NEW QUESTION 116

The most widely used asymmetric encryption algorithm is what?
* Vigenere
* Caesar Cipher
* RSA
* DES
RSA

The RSA encryption algorithm is one of the most widely used public key encryption algorithms that have ever been invented. It was created by the three scientists Ronald Rivest, Adi Shamir, and Leonard Adleman in 1977, and today it is increasingly being used in the network area.

Incorrect answers:

Caesar Cipher &#8211; Monoalphabetic cipher where letters are shifted one or more letters in either direction. The method is named after Julius Caesar, who used it in his private correspondence.

Vigenere &#8211; Multi alphabet cipher Invented by Giovan Battista Bellaso in middle 1553. Vigenere created a stronger version of the cipher. Combining/Weaving Caesar cipher. Not cracked until late 1800s. Widely used from 16th century to early 20th century. It is a cipher square with A to Z across all the columns and rows. You then use a keyword to encrypt the message DES &#8211; The Data Encryption Standard is a symmetric-key algorithm for the encryption of digital data.

NEW QUESTION 117

The ATBASH cipher is best described as what type of cipher?
* Asymmetric
* Symmetric
* Substitution
* Transposition
Substitution

https://en.wikipedia.org/wiki/Atbash

Atbash is a monoalphabetic substitution cipher originally used to encrypt the Hebrew alphabet. It can be modified for use with any known writing system with a standard collating order.

NEW QUESTION 118

The Clipper chip is notable in the history of cryptography for many reasons. First, it was designed for civilian used secure phones. Secondly, it was designed to use a very specific symmetric cipher. Which one of the following was originally designed to provide built-in cryptography for the Clipper chip?
* Blowfish
* Twofish
* Skipjack
* Serpent
Skipjack

https://en.wikipedia.org/wiki/Clipper_chip

The Clipper chip was a chipset that was developed and promoted by the United States National Security Agency (NSA) as an encryption device that secured &#8220;voice and data messages&#8221; with a built-in backdoor that was intended to &#8220;allow Federal, State, and local law enforcement officials the ability to decode intercepted voice and data transmissions.&#8221;. It was intended to be adopted by telecommunications companies for voice transmission. Introduced in 1993, it was entirely defunct by 1996.

he Clipper chip used a data encryption algorithm called Skipjack to transmit information and the Diffie-Hellman key exchange-algorithm to distribute the cryptokeys between the peers. Skipjack was invented by the National Security Agency of the U.S. Government; this algorithm was initially classified SECRET, which prevented it from being subjected to peer review from the encryption research community. The government did state that it used an 80-bit key, that the algorithm was symmetric, and that it was similar to the DES algorithm. The Skipjack algorithm was declassified and published by the NSA on June 24, 1998. The initial cost of the chips was said to be $16 (unprogrammed) or $26 (programmed), with its logic designed by Mykotronx, and fabricated by VLSI Technology, Inc (see the VLSI logo on the image on this page).

NEW QUESTION 119

The most common way steganography is accomplished is via which one of the following?
* rsb
* Isb
* msb
* asb
lbs

https://en.wikipedia.org/wiki/Bit_numbering#:~:text=In%20computing%2C%20the%20least%20significant,number%20is%20even%20or%20odd.

The least significant bit (LSB) is the bit position in a binary integer giving the units value, that is, determining whether the number is even or odd. The LSB is sometimes referred to as the low-order bit or right-most bit, due to the convention in positional notation of writing less significant digits further to the right. It is analogous to the least significant digit of a decimal integer, which is the digit in the ones (right-most) position.

NEW QUESTION 120

Which one of the following is an authentication method that sends the username and password in cleartext?
* PAP
* CHAP
* Kerberos
* SPAP
PAP

https://en.wikipedia.org/wiki/Password_Authentication_Protocol

Password Authentication Protocol (PAP) is a password-based authentication protocol used by Point to Point Protocol (PPP) to validate users. Almost all network operating system remote servers support PAP. PAP is specified in RFC 1334.

PAP is considered a weak authentication scheme (weak schemes are simple and have lighter computational overhead but are much more vulnerable to attack; while weak schemes may have limited application in some constrained environments, they are avoided in general). Among PAP&#8217;s deficiencies is the fact that it transmits unencrypted passwords (i.e. in plain-text) over the network. PAP is therefore used only as a last resort when the remote server does not support a stronger scheme such as CHAP or EAP.

Incorrect answers:

SPAP &#8211; Shiva Password Authentication Protocol, PAP with encryption for the usernames/passwords that are transmitted.

CHAP &#8211; calculates a hash, shares the hash with the client system, the hash is periodically validated to ensure nothing has changed.

Kerberos &#8211; computer-network authentication protocol that works on the basis of tickets to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner. Its designers aimed it primarily at a client-server model and it provides mutual authentication-both the user and the server verify each other&#8217;s identity. Kerberos protocol messages are protected against eavesdropping and replay attacks.

Kerberos builds on symmetric key cryptography and requires a trusted third party, and optionally may use public-key cryptography during certain phases of authentication.

NEW QUESTION 121

Which of the following is a cryptographic protocol that allows two parties to establish a shared key over an insecure channel?
* Elliptic Curve
* NMD5
* RSA
* Diffie-Hellman

Diffie-Hellman

https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange

Diffie-Hellman key exchange is a method of securely exchanging cryptographic keys over a public channel and was one of the first public-key protocols as originally conceptualized by Ralph Merkle and named after Whitfield Diffie and Martin Hellman. DH is one of the earliest practical examples of public key exchange implemented within the field of cryptography.

Incorrect answers:

Elliptic Curve &#8211; Asymmetric Key Algorithm, provides encryption, digital signatures, key exchange, based on the idea of using points on a curve to define the public/private key, used in wireless devices and smart cards. The security of the Elliptic Curve cryptography is based on the fact that finding the discrete logarithm of a random elliptic curve element with respect to a publicly known base point is difficult to the point of being impractical to do so. (y2 = x3 + Ax + B) &#8211; Developed by Victor Miller and Neil Koblitz in 1985 MD5 &#8211; hash function &#8211; Created by Ronald Rivest. Replaced MD4. 128 bit output size, 512 bit block size, 32 bit word size, 64 rounds. Infamously compromised by Flame malware in 2012. Not collision resistant &#8211; Not Reversible &#8211; RFC 1321 RSA &#8211; is a public-key cryptosystem that is widely used for secure data transmission.

NEW QUESTION 122

A technique used to increase the security of block ciphers. It consists of steps that combine the data with portions of the key (most commonly using a simple XOR) before the first round and after the last round of encryption.
* Whitening
* Key Exchange
* Key Schedule
* Key Clustering

Whitening

https://en.wikipedia.org/wiki/Key_whitening

In cryptography, key whitening is a technique intended to increase the security of an iterated block cipher. It consists of steps that combine the data with portions of the key.

The most common form of key whitening is xor-encrypt-xor &#8212; using a simple XOR before the first round and after the last round of encryption.

The first block cipher to use a form of key whitening is DES-X, which simply uses two extra 64-bit keys for whitening, beyond the normal 56-bit key of DES. This is intended to increase the complexity of a brute force attack, increasing the effective size of the key without major changes in the algorithm. DES-X&#8217;s inventor, Ron Rivest, named the technique whitening.

Incorrect answers:

Key Clustering &#8211; different encryption keys generated the same ciphertext from the same plaintext message.

Key Schedule &#8211; an algorithm for the key that calculates the subkeys for each round that the encryption goes through.

Key Exchange &#8211; a method in cryptography by which cryptographic keys are exchanged between two parties, allowing use of a cryptographic algorithm.

NEW QUESTION 123

A _______ refers to a situation where two different inputs yield the same output.
* Convergence
* Collision
* Transposition
* Substitution
Collision

https://en.wikipedia.org/wiki/Collision_(computer_science)

A collision or clash is a situation that occurs when two distinct pieces of data have the same hash value, checksum, fingerprint, or cryptographic digest.

NEW QUESTION 124

What is the solution to the equation 8 mod 3?
* 1
* 4
* 3
* 2
2

https://en.wikipedia.org/wiki/Modulo_operation

The modulo operation returns the remainder or signed remainder of a division, after one number is divided by another (called the modulus of the operation).

Given two positive numbers a and n, a modulo n (abbreviated as a mod n) is the remainder of the Euclidean division of a by n, where a is the dividend and n is the divisor. The modulo operation is to be distinguished from the symbol mod, which refers to the modulus (or divisor) one is operating from.

For example, the expression &#8220;5 mod 2&#8221; would evaluate to 1, because 5 divided by 2 has a quotient of 2 and a remainder of 1, while &#8220;9 mod 3&#8221; would evaluate to 0, because the division of 9 by 3 has a quotient of 3 and a remainder of 0; there is nothing to subtract from 9 after multiplying 3 times 3.

NEW QUESTION 125

Algorithm that was chosen for the Data Encryption Standard, which was altered and renamed Data Encryption Algorithm.
* Blowfish
* Rijndael
* Lucifer
* El Gamal
Lucifer

https://en.wikipedia.org/wiki/Lucifer_(cipher)

Lucifer was a direct precursor to the Data Encryption Standard. One version, alternatively named DTD-1.

NEW QUESTION 126

Original, unencrypted information is referred to as ____.
* text
* plaintext
* ciphertext
* cleartext
plaintext

https://en.wikipedia.org/wiki/Plaintext

In cryptography, plaintext usually means unencrypted information pending input into cryptographic algorithms, usually encryption algorithms. Cleartext usually refers to data that is transmitted or stored unencrypted (&#8220;in clear&#8221;).

NEW QUESTION 127

Ahlen is using a set of pre-calculated hashes to attempt to derive the passwords from a Windows SAM file. What is a set of pre-calculated hashes used to derive a hashed password called?
* Hash matrix
* Rainbow table
* Password table
* Hash table
Rainbow table

https://en.wikipedia.org/wiki/Rainbow_table

A rainbow table is a precomputed table for caching the output of cryptographic hash functions, usually for cracking password hashes. Tables are usually used in recovering a key derivation function (or credit card numbers, etc.) up to a certain length consisting of a limited set of characters. It is a practical example of a space-time tradeoff, using less computer processing time and more storage than a brute-force attack which calculates a hash on every attempt, but more processing time and less storage than a simple key derivation function with one entry per hash. Use of a key derivation that employs a salt makes this attack infeasible.

NEW QUESTION 128

In relationship to hashing, the term _____refers to random bits that are used as one of the inputs to the hash. Essentially the ______ is intermixed with the message that is to be hashed
* Vector
* Salt
* Stream
* IV
Salt

https://en.wikipedia.org/wiki/Salt_(cryptography)

A salt is random data that is used as an additional input to a one-way function that hashes data, a password or passphrase. Salts are used to safeguard passwords in storage. Historically a password was stored in plaintext on a system, but over time additional safeguards were developed to protect a user&#8217;s password against being read from the system. A salt is one of those methods.

Incorrect answers:

Vector &#8211; Wrong!

IV &#8211; an initialization vector or starting variable (SV) is a fixed-size input to a cryptographic primitive that is typically required to be random or pseudorandom. Randomization is crucial for encryption schemes to achieve semantic security, a property whereby repeated usage of the scheme under the same key does not allow an attacker to infer relationships between segments of the encrypted message. For block ciphers, the use of an IV is described by the modes of operation. Randomization is also required for other primitives, such as universal hash functions and message authentication codes based thereon.

Stream &#8211; A stream cipher is a symmetric key cipher where plaintext digits are combined with a pseudorandom cipher digit stream (keystream). In a stream cipher, each plaintext digit is encrypted one at a time with the corresponding digit of the keystream, to give a digit of the ciphertext stream. Since encryption of each digit is dependent on the current state of the cipher, it is also known as state cipher. In practice, a digit is typically a bit and the combining operation is an exclusive-or (XOR).

NEW QUESTION 129

Cryptographic hashes are often used for message integrity and password storage. It is important to understand the common properties of all cryptographic hashes. What is not true about a hash?
* Few collisions
* Reversible
* Variable length input
* Fixed length output
Reversible

https://en.wikipedia.org/wiki/Hash_function

Hash functions are not reversible.

Incorrect answers:

Fixed length output and Variable length input. Hash function receive variable length input and produce fixed length output Few collisions. Every hash function with more inputs than outputs will necessarily have collisions

NEW QUESTION 130

How can rainbow tables be defeated?
* Lockout accounts under brute force password cracking attempts
* All uppercase character passwords
* Use of non-dictionary words
* Password salting
Password salting

https://en.wikipedia.org/wiki/Salt_(cryptography)#Benefits

Salts also combat the use of hash tables and rainbow tables for cracking passwords. A hash table is a large list of pre-computed hashes for commonly used passwords. For a password file without salts, an attacker can go through each entry and look up the hashed password in the hash table or rainbow table. If the look-up is considerably faster than the hash function (which it often is), this will considerably speed up cracking the file. However, if the password file is salted, then the hash table or rainbow table would have to contain &#8220;salt . password&#8221; pre-hashed. If the salt is long enough and sufficiently random, this is very unlikely. Unsalted passwords chosen by humans tend to be vulnerable to dictionary attacks since they have to be both short and meaningful enough to be memorized. Even a small dictionary (or its hashed equivalent, a hash table) is significant help cracking the most commonly used passwords. Since salts do not have to be memorized by humans they can make the size of the rainbow table required for a successful attack prohibitively large without placing a burden on the users.

NEW QUESTION 131

In 2007, this wireless security algorithm was rendered useless by capturing packets and discovering the passkey in a matter of seconds. This security flaw led to a network invasion of TJ Maxx and data theft through a technique known as wardriving.

Which Algorithm is this referring to?
* Wired Equivalent Privacy (WEP)
* Wi-Fi Protected Access 2 (WPA2)
* Wi-Fi Protected Access (WPA)
* Temporal Key Integrity Protocol (TKIP)
Wired Equivalent Privacy (WEP)

https://en.wikipedia.org/wiki/Wired_Equivalent_Privacy#Weak_security

In 2007, Erik Tews, Andrei Pychkine, and Ralf-Philipp Weinmann were able to extend Klein&#8217;s 2005 attack and optimize it for usage against WEP. With the new attack it is possible to recover a 104-bit WEP key with probability 50% using only 40,000 captured packets. For 60,000 available data packets, the success probability is about 80% and for 85,000 data packets about 95%. Using active techniques like deauth and ARP re-injection, 40,000 packets can be captured in less than one minute under good conditions. The actual computation takes about 3 seconds and 3 MB of main memory on a Pentium-M 1.7 GHz and can additionally be optimized for devices with slower CPUs. The same attack can be used for 40-bit keys with an even higher success probability.

NEW QUESTION 132

A _____ is a function is not reversible.
* Stream cipher
* Asymmetric cipher
* Hash
* Block Cipher

Hash

https://en.wikipedia.org/wiki/Hash_function

Hash functions are irreversible. This is actually required for them to fulfill their function of determining whether someone possesses an uncorrupted copy of the hashed data. This brings susceptibility to brute force attacks, which are quite powerful these days, particularly against MD5.