212-81 Q&As

EC-Council Certified Encryption Specialist (ECES)

Pass EC-COUNCIL 212-81 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/212-81.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

QUESTION 1

Which of the following is the standard for digital certificates?

A. RFC 2298

B. X.509

C. CRL

D. CA

Correct Answer: B

https://en.wikipedia.org/wiki/X.509

X.509 is a standard defining the format of public key certificates. X.509 certificates are used in many Internet protocols, including TLS/SSL, which is the basis for HTTPS, the secure protocol for browsing the web. They are also used in offline applications, like electronic signatures. An X.509 certificate contains a public key and an identity (a hostname, or an organization, or an individual), and is either signed by a certificate authority or self-signed. When a certificate is signed by a trusted certificate authority, or validated by other means, someone holding that certificate can rely on the public key it contains to establish secure communications with another party, or validate documents digitally signed by the corresponding private key.

QUESTION 2

A real time protocol for verifying certificates (and a newer method than CRL).

A. Online Certificate Status Protocol (OCSP)

B. Server-based Certificate Validation Protocol (SCVP)

C. Public Key Infrastructure (PKI)

D. Registration Authority (RA)

Correct Answer: A

Online Certificate Status Protocol (OCSP)

https://en.wikipedia.org/wiki/Online_Certificate_Status_Protocol The Online Certificate Status Protocol (OCSP) is an Internet protocol used for obtaining the revocation status of an X.509 digital certificate. It is described in RFC 6960 and is on

the Internet standards track. It was created as an alternative to certificate revocation lists (CRL), specifically addressing certain problems associated with using CRLs in a public key infrastructure (PKI).

QUESTION 3

How can rainbow tables be defeated?

A. Lockout accounts under brute force password cracking attempts

B. All uppercase character passwords

C. Use of non-dictionary words

D. Password salting

Correct Answer: D

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 "salt . password" 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.

QUESTION 4

Which one of the following terms describes two numbers that have no common factors?

A. Coprime

B. Fermat\\'s number

C. Euler\\'s totient

D. Convergent

Correct Answer: A

Coprime https://en.wikipedia.org/wiki/Coprime_integers In number theory, two integers a and b are said to be relatively prime, mutually prime, or coprime if the only positive integer (factor) that divides both of them is 1. Consequently, any prime number that divides one of a or b does not divide the other. This is equivalent to their greatest common divisor (gcd) being 1.

QUESTION 5

Which of the following was a multi alphabet cipher widely used from the 16th century to the early 20th century?

A. Atbash

B. Caesar

C. Scytale

D. Vigenere

Correct Answer: D