312-50V12 Q&As

Certified Ethical Hacker Exam (CEHv12)

QUESTION 1

Which of the following is the primary objective of a rootkit?

A. It opens a port to provide an unauthorized service

B. It creates a buffer overflow

C. It replaces legitimate programs

D. It provides an undocumented opening in a program

Correct Answer: C

QUESTION 2

What is the most common method to exploit the "Bash Bug" or "Shellshock" vulnerability?

A. SYN Flood

B. SSH

C. Through Web servers utilizing CGI (Common Gateway Interface) to send a malformed environment variable to a vulnerable Web server

D. Manipulate format strings in text fields

Correct Answer: C

QUESTION 3

A hacker is an intelligent individual with excellent computer skills and the ability to explore a computer\\'s software and hardware without the owner\\'s permission. Their intention can either be to simply gain knowledge or to illegally make changes.

Which of the following class of hacker refers to an individual who works both offensively and defensively at various times?

A. White Hat

B. Suicide Hacker

C. Gray Hat

D. Black Hat

Correct Answer: C

QUESTION 4

BitLocker encryption has been implemented for all the Windows-based computers in an organization. You are concerned that someone might lose their cryptographic key. Therefore, a mechanism was implemented to recover the keys from Active Directory. What is this mechanism called in cryptography?

A. Key archival

B. Key escrow.

C. Certificate rollover

D. Key renewal

Correct Answer: B

QUESTION 5

John wants to send Marie an email that includes sensitive information, and he does not trust the network that he is connected to. Marie gives him the idea of using PGP. What should John do to communicate correctly using this type of encryption?

A. Use his own public key to encrypt the message.

B. Use Marie\\'s public key to encrypt the message.

C. Use his own private key to encrypt the message.

D. Use Marie\\'s private key to encrypt the message.

Correct Answer: B

When a user encrypts plaintext with PGP, PGP first compresses the plaintext. The session key works with a very secure, fast conventional encryption algorithm to encrypt the plaintext; the result is ciphertext. Once the data is encrypted, the session key is then encrypted to the recipient\\'s public key

https://en.wikipedia.org/wiki/Pretty_Good_Privacy Pretty Good Privacy (PGP) is an encryption program that provides cryptographic privacy and authentication for data communication. PGP is used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications. PGP encryption uses a serial combination of hashing, data compression, symmetric-key cryptography, and finally public-key cryptography; each step uses one of several supported algorithms. Each public key is bound to a username or an email address.

https://en.wikipedia.org/wiki/Public-key_cryptography Public key encryption uses two different keys. One key is used to encrypt the information and the other is used to decrypt the information. Sometimes this is referred to as asymmetric encryption because two keys are required to make the system and/or process work securely. One key is known as the public key and should be shared by the owner with anyone who will be securely communicating with the key owner. However, the owner\\'s secret key is not to be shared and considered a private key. If the private key is shared with unauthorized recipients, the encryption mechanisms protecting the information must be considered compromised.