ECCouncil

EC0-350

Ethical Hacking and Countermeasures

Answer: E

Explanation:
This is a buffer overflow with it’s payload in hex format.

QUESTION: 467
StackGuard (as used by Immunix), ssp/ProPolice (as used by OpenBSD), and Microsoft's /GS option use _____ defense against buffer overflow attacks.

A. Canary
B. Hex editing
C. Format checking
D. Non-executing stack

Answer: A

Explanation:
Canaries or canary words are known values that are placed between a buffer and control data on the stack to monitor buffer overflows. When the buffer overflows, it will clobber the canary, making the overflow evident. This is a reference to the historic practice of using canaries in coal mines, since they would be affected by toxic gases earlier than the miners, thus providing a biological warning system.

QUESTION: 468
Symmetric encryption algorithms are known to be fast but present great challenges on the key management side. Asymmetric encryption algorithms are slow but allow communication with a remote host without having to transfer a key out of band or in person. If we combine the strength of both crypto systems where we use the symmetric algorithm to encrypt the bulk of the data and then use the asymmetric encryption system to encrypt the symmetric key, what would this type of usage be known as?

A. Symmetric system
B. Combined system
C. Hybrid system
D. Asymmetric system

Answer: C

Explanation:

Because of the complexity of the underlying problems, most public-key algorithms involve operations such as modular multiplication and exponentiation, which are much more computationally expensive than the techniques used in most block ciphers, especially with typical key sizes. As a result, public-key cryptosystems are commonly "hybrid" systems, in which a fast symmetric-key encryption algorithm is used for the message itself, while the relevant symmetric key is sent with the message, but encrypted using a public-key algorithm. Similarly, hybrid signature schemes are often used, in which a cryptographic hash function is computed, and only the resulting hash is digitally signed.

QUESTION: 469

Steven the hacker realizes that the network administrator of XYZ is using syskey to protect organization resources in the Windows 2000 Server. Syskey independently encrypts the hashes so that physical access to the server, tapes, or ERDs is only first step to cracking the passwords. Steven must break through the encryption used by syskey before he can attempt to brute force dictionary attacks on the hashes. Steven runs a program called “SysCracker” targeting the Windows 2000 Server machine in attempting to crack the hash used by Syskey. He needs to configure the encryption level before he can launch attach. How many bits does Syskey use for encryption?

A. 40 bit
B. 64 bit
C. 256 bit
D. 128 bit

Answer: D

Explanation:

SYSKEY is a utility that encrypts the hashed password information in a SAM database using a 128-bit encryption key.

QUESTION: 470

In the context of using PKI, when Sven wishes to send a secret message to Bob, he looks up Bob’s public key in a directory, uses it to encrypt the message before sending it off. Bob then uses his private key to decrypt the message and reads it. No one listening on can decrypt the message. Anyone can send an encrypted message to Bob but only Bob can read it. Thus, although many people may know Bob’s public key and use it to verify Bob’s signature, they cannot discover Bob’s private key and use it to forge digital signatures. What does this principle refer to?

A. Irreversibility

B. Non-repudiation
C. Symmetry
D. Asymmetry

Answer: D

Explanation:
PKI uses asymmetric key pair encryption. One key of the pair is the only way to decrypt data encrypted with the other.

QUESTION: 471
What is SYSKEY # of bits used for encryption?

A. 40
B. 64
C. 128
D. 256

Answer: C
Explanation:
System Key hotfix is an optional feature which allows stronger encryption of SAM. Strong encryption protects private account information by encrypting the password data using a 128-bit cryptographically random key, known as a password encryption key.

QUESTION: 472
Which of the following is NOT true of cryptography?

A. Science of protecting information by encoding it into an unreadable format
B. Method of storing and transmitting data in a form that only those it is intended for can read and process
C. Most (if not all) algorithms can be broken by both technical and non-technical means
D. An effective way of protecting sensitive information in storage but not in transit

Answer: D

Explanation:
Cryptography will protect data in both storage and in transit.

QUESTION: 473

Which of the following best describes session key creation in SSL?

A. It is created by the server after verifying theuser's identity
B. It is created by the server upon connection by the client
C. It is created by the client from the server's public key
D. It is created by the client after verifying the server's identity

Answer: D

Explanation:

An SSL session always begins with an exchange of messages called the SSL handshake. The handshake allows the server to authenticate itself to the client using public-key techniques, then allows the client and the server to cooperate in the creation of symmetric keys used for rapid encryption, decryption, and tamper detection during the session that follows. Optionally, the handshake also allows the client to authenticate itself to the server.

QUESTION: 474

How many bits encryption does SHA-1 use?

A. 64 bits
B. 128 bits
C. 160 bits
D. 256 bits

Answer: C

Explanation:

SHA-1 (as well as SHA-0) produces a 160-bit digest from a message with a maximum length of 264 - 1 bits, and is based on principles similar to those used by Professor Ronald L. Rivest of MIT in the design of the MD4 and MD5 message digest algorithms.

QUESTION: 475

There is some dispute between two network administrators at your company. Your boss asks you to come and meet with the administrators to set the record straight. Which of these are true about PKI and encryption? Select the best answers.

A. PKI provides data with encryption, compression, and restorability.
B. Public-key encryption was invented in 1976 by Whitfield Diffie and Martin Hellman.
C. When it comes to eCommerce, as long as you have authenticity, and authenticity, you do not need encryption.
D. RSA is a type of encryption.

Answer: B, D

Explanation:
PKI provides confidentiality, integrity, and authenticity of the messages exchanged between these two types of systems. The 3rd party provides the public key and the receiver verifies the message with a combination of the private and public key. Public-key encryption WAS invented in 1976 by Whitfield Diffie and Martin Hellman. The famous hashing algorithm Diffie- Hellman was named after them. The RSA Algorithm is created by the RSA Security company that also has created other widely used encryption algorithms.

QUESTION: 476
A client has approached you with a penetration test requirements. They are concerned with the possibility of external threat, and have invested considerable resources in protecting their Internet exposure. However, their main concern is the possibility of an employee elevating his/her privileges and gaining access to information outside of their respective department. What kind of penetration test would you recommend that would best address the client’s concern?

A. A Black Box test
B. A Black Hat test
C. A Grey Box test
D. A Grey Hat test
E. A White Box test
F. A White Hat test

Answer: C

QUESTION: 477
In which of the following should be performed first in any penetration test?

A. System identification
B. Intrusion Detection System testing
C. Passive information gathering

D. Firewall testing

Answer: C

QUESTION: 478
Vulnerability mapping occurs after which phase of a penetration test?

A. Host scanning
B. Passive information gathering
C. Analysis of host scanning
D. Network level discovery

Answer: C

Explanation:
The order should be Passive information gathering, Network level discovery, Host scanning and Analysis of host scanning.