Page No.:
Date: / /

Assignment : UNIT - 3

Que: 1) What are Vulnerabilities and security threeed in network ?

Ans - Vulnerabilities and security threats are two important espect of network security Vulnerabilities refer to weekness or flaws in a system that can be exploited by an attackee to gain unauthorized access or cause damage to the system. security threat refer to the risks or potential actors that can exploit vulnerabilities and cause harm to be network or its assests.

Some common Vulnerabilities and security threads in network security include.

① Malware -
Malware is a type of software theat is cause harm to a system. it can includs viruses, woom, trojans and other type of malicious software that can steeal data, corrupt files or discrupt network operation.

② phising -
phishing is a social engineering attack that involves tricking user into providing sensitive information, such as username and password, by impersonating a legitimate entity.

Page No.:
Date: / /

③ Denial of service (DoS) -
Distributed Denial of service (DDoS) -
DoS and DDoS attack are designed to flood a network or service with traffic making it unavailable to users.

④ password attacks -
password attack involve attempting to guess or crack password to gain unauthorized access to a system or network.

⑤ Man-in-the Middle (MITM) attack -
MITM attack involve intercepting and manipulating communication between two parties, allowing the attacker to ~~the~~ eavesdrop on or modify the communications.

⑥ SQL injection attacks -
SQL Injection attack exploit vulnerabilities in web application to inject malicious code into a database, potentially allowing attacker to steal data or take control of the system.

⑦ Zero-day vulnerabilities -
zero day vulnerabilities are previously unknown vulnerabilities that are discovered and exploited by attacker

before they can be patched by the systems developers.

que:2) What is cryptography explain its compo

Ans-

Cryptography is the practice of secure communication in the presence of third parties of adversaries. It's involve the use of mathmatical algorithm and protocol to ensure confidentiality, integrity and authenticity of data. Cryptography has becomes an essential component of modern communication and plays critical roles in protecting sensitive information from unauthorized access.

The three main components of Cryptography

① Encryption -

Encryption is the process of transforming plaintext (human-readable data) into ciphertext (encrypted data) to protect its confidentiality. This is done using an encryption algorith and secret key. The encryption algorith takes the plaintext and the key as input and produces the ciphertext as output. The ciphetext can only be descrypted back into plaintext by someone who has the correct key

Page No.:
Date: / /

② Decryption -
Decryption is the reverse process of encryption, where the ciphertext is transformed back into plaintext using decryption algorithm and correct key. The decryption algorithm takes the ciphertext and produces the plaintext as output. only the person who has the correct key can decrypt the ciphertext and read the plaintext.

③ Hashing -
Hashing is a process of generate a fixed - length string of data from any input data, regardless of size. The output of a hashing algorithm is known as a hash or message digest. Hashing is used to ensure the integrity of data by detecting any changes to the original data. If the input data is changed the resulting hash will be different. Hashing is also used for digital signatures, where a hash of the of message is signed using a private key to authenticate the sender.

Page No.:
Date: / /

Que 3) Explain Asymmetric key encryption?

Ans -

Asymmetric key encryption, also known as public-key encryption, is a cryptographic technique that uses two different key for encryption and decryption. In contrast to symmetric key encryption where the same key is used for both encryption and decryption, assymetric key encryption uses a public key for encryption and a private key for decryption.

Here is how assymmetric key encryption -

① Key generation -
The user generates a key pair consisting of a public key and a private key. The public key is made available to anyone who needs to encrypt data while the private key is kept secret and only used by the owner to decrypt the data.

② Encryption -
To encryption message, the sender uses the recipient's public key to encrypt the message. only the receipt, who has the corresponding private key, can decrypt the message.

Date: / /

③ decryption -
To decrypt the encrypted message, the receipt uses there private key to decrypt the message. since the private key is kept secret, only the receipt can decrypt the message.

Asymmetric key encryption provides several advantage over symmetric key encryption. one advantage is that it eliminates the need for key exchange, which is required in symmetric key encryption. In symmetric key encryption the public key can be freely distributed without compromising the security of the encryption.

Que 3 4) Explain Symmetric key encryption and Explain Silent features.

Ans -

~~key generation~~ -
The symmetric key encryption is a cryptographic technique that uses the same key for both encryption and decryption of data. this means that the sender and the receiver of the message. Symmetric key encryption is faster and more efficient than asymmetric key encryption, making it ideal for

encrypting large amount of data.

Here is how symmetric key encryption works:

① Key generation -
The sender and Receiver agree on a secret key to use for encryption and decryption.

② Encryption -
The sender uses the secret key to encrypt the message. the encryption algorithm takes the plaintext message and the key as input and produces the ciphertext as output.

③ decryption -
The receiver uses the same secret key to decrypt the ciphertext and recovers the original plaintext message. the decryption algorithm takes the ciphertext and the secret key as input and produces the plaintext message as output.

The key features of symmetric encryption.

① Security -
The secret key used for encryption and decryption must be kept confident to maintain the security of the encryption

② Efficiency -
Symmetric key encryption is much faster and more efficient than asymmetric key encryption, making it ideal for encrypting large amount of data.

③ Scalability -
Symmetric key encryption is easily scalable, as the same key can be used to encrypt and decrypt message between multiple parties.

④ Simplicity -
Symmetric key encryption is simple and easy to implement, with relatively few computational resources required.

Ques 5) Explain conventional DES encryption standard.

Ans - The Data Encryption Standard (DES) is a symmetric encryption algorithm that was widely used for secure data communication in the 1970 and 1980. DES uses a block cipher, which means that it encrypt data in fixed-size blocks of 64-bits.

The conventional DES Encryption process involve the following steps.

① key generation -
A 64-bit secret key is generated by

applying a permutation to a 56-bit key.

② Initial permutation -
The plaintext is permuted using an initial permutation table to rearrange the bits.

③ key splitting -
The 64-bit key is split into two 28-bit halves, which are each used to generate 16- subkeys.

④ Round function -
DES uses 16 rounds of a complex function that involves several steps, including

- Expansion -
The 32-bit right half of the plaintext is expanded to 48 bit using an expension permutation.

- key Mixing -
The 48-bit expansion is XORed with a 48-bit subkey generated from the original key.

- Substitution -
The XORed result is split into eight 6 bit blocks, each of which is submitted with a different 4-bit value based on a predetermined substitution table.

• permutation -
The resulting 32-bit output of the 16th round is permuted using a fixed permutation.

⑤ Final permutation -
The output of the 16th round is permuted using a final permutation table to produce the ciphertext.

To decrypt the ciphertext, the process is simply reversed, using the same key but with the subkey applied in reverse order.