Assignment : UNIT-4

Page No.:
Date : / /

Que 1) What are firewalls, explain packet filter? Types of firewalls.

Ans -

Firewalls -

Firewalls are security devices used to protect a computer network from unauthorized access and malicious attacks. A firewall act as a barrier between a trusted internal network and an untrusted external network, such as the internet. Firewalls can be implemented as hardware or software solution and work by monitoring and controlling the traffic and flows between these network

Que 2

Ans -

packet filter -

packet filter is one of the most comman type of firewalls. packet filtering is a technique that examines each packet of data that passes through the firewall and compares it is a set of predefined rules. these rules dicate which packets are allowed to pass through the firewall and which are blocked.

packet filtering work by examining the header information of each packet which contains information such as source and destination IP address

Page No.:
Date: / /

the protocal being used (such as TCP or UDP) and the source and destination ports. Based on these criteria, the firewall can decide whether to allow the packet to pass through or to block it.

packet filtering can be block traffic based on specific IP address or ranges specific protocol or ports or specific combination of these factors

Que 12) what is RSA diffie hellman public key system.

Ans -

RSA and Diffie-Hellman are two different public key encryption system used for secure communication over public network. RSA was developed by Ron Rivest, Adi shamir. Both system are widely used in modern cryptography and provide different approaches to solving the problem of secure communication.

The RSA public key system is based on the mathematical properties of large prime number. Each user generates a public and private key pair, with the public key shared and other and

only the recipient with the corresponding private key can decrypt the message.

The security of the RSA system relies Deffin-Hellman is a key exchange protocol that is used to establish a shared secret key between two parties over an insecure network. It enables two parties to exchange information in a way that is secure even if an attacker is listening to the communication. Alice and bob both generate a public-private key pair and exchange their public key with each other. they then use each other's public key and their public key with each other. this shared secret key can be used symmetric encryption to protect subsequent communition between the two parties.

The combination of RSA and diffi-Hellman is often used in practice to establish a secure communication channel. RSA is used to securely exchange the public keys exchange, which is then establishes a shared secret key for symmetric encryption of the communication. this combination of techniques is widely used to secure internet communication including online transaction, email, and messaging application.

Date: / /

Ques 3) What is HASH function and SHA?

Ans :-

HASH function -

A HASH function is a mathematical function that takes in input data of any size and produces a fixed-size output, known as hash or message. The output of hash function is typically a unique representation of the input data, such that even a small change in the input data will produce a ~~drastic~~ drastically different output.

SHA -

SHA or secure hash algorithm, is a family of cryptographic hash function developed by the national security Agency (NSA) in the United state. the most widely used SHA function in SHA-256. which produces a 256-bit message digest. other version of ~~SHA~~ SHA, such as SHA-1 and SHA3 are also in use.

SHA-256 is commonly used in digital signature algorithm, password storage and other security application where data integrity and authenticity are important. it is also used in blockchain technology. where it is used to generate a

Page No.:
Date: / /

a unique and immutable fingerprint of a block of data

Que: 4) What intrusion technique and how intrusion are detected ?

Ans -

Intrusion Techniques -

A Network intrusion is any unauthorized activity on a computer network.

The following attack vectors

i) Asymmetric Routing -

in this method, the attacker attempt to utilize more than one route to the targeted network device.

The data to have the overall attack evade detection by having a significant portion of the offending packet bypass certain network segment and their network intrusion sensors.

ii) Buffer overflow Attacks -

The approach attempt to overwrite specific section of computer memory within a network, replacing normal data in those memory location with a set of command that will later

Date: / /

be executed as part of the attack.

iii) Comman Gateway Interface scripts -
The CGI provide easy opening such as " backtracking through which attackee can accesss supposedly secure network System files.
when system fail to include input verification or check for backtrack charectees a coveet CGI spript can easily add the directory label ---
or pipe 'I' charectee to any file path name and thereby access files that should not be available via web.

iv) Traffic flooding -
An ingenious method of network intrusion simply tergets network intrusion detection system by creating traffic load too heavy for the System to adequetely screen. the attackee can sometime execute an undetected attack and even trigger an undetected 'fail-open- codition.

v) Trojans -
They instigate Dos attack erase Stored data as open channel to peemits system control by outside attackee trojans can be introduced

online archeives and file resposiitories

Intrusion Detection -
An intrusion detection is a system that monitors network traffic for suspicious activity is discovered

classification of Intrusion Detection -

① Signature based method -
Signature based intrusion detection detects the attacks on the basis of the specific pattern such as number of bytes or number of 1's or 0's in in the network basis.
It also detects on the basis of the already known malicious intruction sequence that is used by the malware

② Anomoly - based method -
In anamoly based IDS there is use of machine learning to create a trustful activity model and anything coming is compared with that model and it is declared suspicious if it is not found in model.

Ques 5) Explain key management in details -

Ans - key management define as managing cryptographic keys within a cryptosystem

It can manage with generating exchanging saving, using and replacing key as required at the user level.

A key management system will also contain key servers, user process and protocols; including cryptographic protocal design.

The Security of the cryptosystem is based upon succesful key management.

proper management provide a key stays security throughout its lifecycle, from generation and use to saving and deletion.

How ~~much~~ key management works -

most cryptographic keys follows a lifecycle which involves.

① the generation of a key is the first step in ensuring that key is secure

If the key is generated with a weak encryption algorithm, then attack could easily discover the value of the encryption key.

(ii) the next step of the key lifecycle is ensuring the safe distribution of the key. key should be distributed to the required users via a secure connection.

(iii) After distribution, it is used for cryptographic operation.

(iv) once a keys cryptoperiod or time period passes, the key must be rotated.

(v) when the key of an encrypted set of data expires, the key is retired and replaced with a new key.

(vi) first the data is decrypted by the old key and then encrypted by the new key.