- Government enhanced collaboration on cyber defense

Unit-3 Assignment

1) What are different ways to Provide authentication discuss briefly

→ i) Password:- Based Authentication
User Provides a Secret Password known only to them this is simple but vulnerable to guessing and brute force attacks

Ex:- Login to gmail account by entering Email-ID and Password

(ii) Multi-factor Authentication (MFA):- It requires users to Prevent two or more authentication factors Password, OTP or Biometric even if one factor leaked unauthorized access is still prevented, advantage

Ex:- banking app Password and OTP both should be Provided

iii) Certificate based Authentication:- Uses digital certificate involved by a trusted certificate authority (CA) to verify identity

Ex:- Login, device Provides a client certificate before connecting to network

iv) Token-based Authentication:- Involves the use of security tokens which can be hardware devices or software that generate Unique

Ex:- RSA Secure to Token; Google Authentication APP Generate code

v) Biometric:- Authenticate user based on their unique biological characteristic difficult to replicate or steal
Eg:- Unlocking smartphone using fingerprint

vi) OTP:- Password that is valid for only one login transation Even if the hacker get the OTP it became after some time.
Ex:- When we have to login into Bank website we will recieve OTP via SMS

vii) Public Key Infrastructure:- Uses Public and Private Key along with digital certificate for authentication
Eg:- When we access a Server HTTP website the Server authenticate itself using a Public key Certificate

viii) Kerberos Authentication:- A Ticket based authentication Protocol that uses a Key Distribution Center (KDC) to Security authenticate users.

2) If a MAC uses a weak hash function how can an attacker exploit this?

→ Message Authentication Code (MAC) ensures message integrity and authentication using a hash function and a secret key

(i) Collision attack:- MD5 is vulnerable to collision attack, meaning an attacks can find two different messages that Produces the same hash output that Produce a Specific MAC Making it Possible to forge message

(ii) Length Extension Attack:- If the MAC implementation is Poor like appending the Key to Message attackers can Perform Length Extension attacks where they append extra data to the original messge and calucate a Valid MAC without knowing the Key

7) If any attacker replays an add message with a valid MAC how can this be Prevented?

This is called a Replay Attack

→ i) Time Stamps:- Contains a time stamp in each message The reciever checks if the time stamp is recent

(ii) Number Used Once:- Attach a Unique random number with each message. The reciever Keeps track of already seen nonce to reject · replays

iii) Sequence Number:- Use incremental sequence number with each message. The reciever only manage with a higher sequence number than before.

iv) Session Tokens:- for session short-lived tokens that expire after a short time after single use

?) How does the Publickey distribution Problem?

by allowing two Parties to securly generate a share secret key over an insecure communication channel without actually transmitting the key

In traditional encryption system

→ No need to distribute public keys in advance

→ It avoids the risk of interception during key exchange

5. why does Kerberous use two tickes (TGT? Service ticket?

→ TGT (Ticket Granting Ticket):- To authenticate the user once & get access to the ticket granting server

→ Service Ticket to access each specific service securely

This two Ticket system

1) Enhances security never reaches service

2) Reduce Password exposure

3) Suppots scalability efficiency allowing multiple service using a model

9