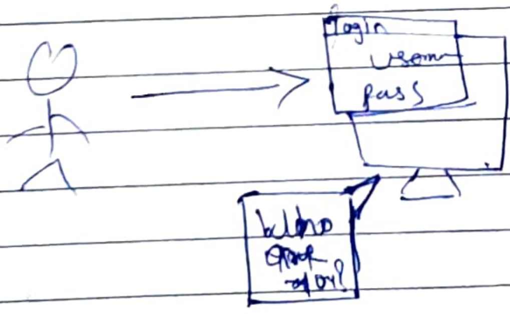
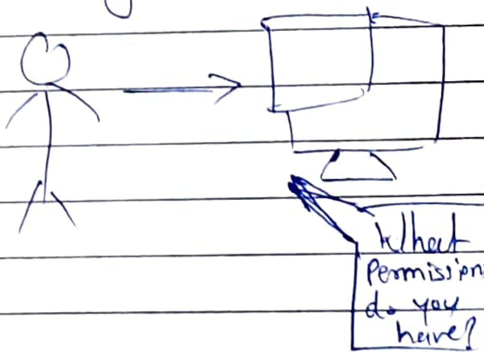
Authentication & Authorization

Authentication	Authorization
• Here, identity of ~~pause~~ users are checked for providing the access to system.	• Here, person's or user's authorities are checked for accessing the resources
• Users are verified	• Users are validated
• It is done before authorization process.	• It is done after authentication process
• needs user's login details.	• Needs user's privillege or security levels.
• It determines whether person is user or not	• It determines What permission does the user have?
• Authentication credentials can be changed in part as and when required by user	• Autherization permission can not be changed by user as these are granted by owner of the system & only owner can change it.





([illegible] of (users, unauthorised users & devices
out of private networks)

4 Network Access Control

It is a security soln that uses a set of protocols to keep unauthorized users and devices out of private networks or give restricted access to the devices which are compliant with network security policies.

(which device have control of your network
which device can authenticate your network
& " can authorise within your ")

(Without NAC if anybody connects to your environment then it is harmful for environment)

It handles network management & security that implements security policy, compliance and management of access control to a network.

Components of NAC :-

(1) Restricted area - It restricts access to the network by user authentication & authorization Control.

(2) Network Boundary protection : It monitors & controls the connectivity of network with external networks.

Types of NAC :- (1) Preadmission
(2) Post admission

* SHA 15 (Secure Hash Algo)

1. Plain text message 1024 bits
2. output bits - 512 bits
3. No of rounds - 80
4. Each round will produce a word [illegible]
5. K constant each round (hexa decimal format)
6. Buffer (stores result)

↓

o/p of one block → i/p to next block

* Kerberos :—

Kerberos provides a centralized authentication server whose fun' is to authenticate users to servers and servers to users.

In kerberos authentication server & databased used for client authentication.

It runs as third-party trusted server known as the key distribution center (KDC)

Main Components of Kerberos —

1. Authentication server performs the initial authentication & ticket or ticket Granting service

2. Database - Authentication server verifies the access right of users in DB

3. Ticket Granting Server :— Ticket Granting Server issues the ticket for the server

→ Provides two or more verification factors for user

Multi Factor Authentication (MFA)?

Multi factor Authentication is an authentication method that requires the user to provide two or more verification factors to gain access to resource such as an appln, online acc, or VPN.

~~Transf~~

Transport-Level Security

- **Web Security Considerations :—**
  - update s/w
  - Beware of SQL injection
  - Cross site scripting (xss)
  - error messages
  - Data validation
  - Password

- **Secure Socket layer (SSL)**

Provides security to the data that is transferred betn web browser & server. SSL encrypts the link betn a web server and a browser which ensure that all data passed betn them remain private & free from attack.

(SSL are protocol for establishing authenticated & & encrypted links betn networked computers)

- TLS - Transport Layer Security
  - designed to provide security at transport layer.
  - It was derived from SSL
  - It ensures no third party may evaesdrop or tampers with any message.

- HTTPS - Hypertext transfer Protocol Secure
  - Secure version of HTTP
  - mainly used for providing security to the data sent bet^n website & web browser.
  - widely used on internet & used for secure comm^n
  - Also called as HTTPS over SSL coz HTTPS comm^n protocols are encrypted using SSL.

- SSH - Secure Shell or Secure Socket Shell.
  - Cryptographic network protocol that is used for transferring encrypted data over network.

It allows you to connect to a server or multiple servers, without having you to remember or enter your pass for each system that is login remotely from one system in to another

~~- IPSec - IP Security~~

~~- used to encrypt applⁿ layer data~~
~~It is protocol used to setup encryption connection betⁿ devices~~

- IPSec - IP Security
  - used to encrypt applⁿ layer data
  - It is a group of protocol that are used to setup encrypted connⁿ betⁿ devices together

Intro to Security Attacks

- **Vulnerability** – Weakness that can be exploited by cybercriminals to gain unauthorized access to comp system.

  (It is a weakness in information system, system processes or internal controls of organization)

- **Threat** :– Malicious act that seeks to damage data or other assests, misuse them.

- **Threat Modeling** :– It is a method of optimizing network security by locating vulnerabilities, identifying objectives, & developing countermeasures to either prevent or mitigate the effects of cyber attacks against the system.

- **Risk** :– Probability of loss resulting from cyber attack or data breach on your organization.

- **Attack** :- When there is unauthorized System or network access by third party it is called as Attack.

- **Types of Attacks** -
  1. Malware Attack
  2. phishing Attack
  3. Password
  4. Man in the middle attack
  5. DoS

- **Countr measures** :- It is process that can prevent Comp from effects of Pr
  It is an action, process, device or system that can prevent, or mitigate the effects of threats to a computer.

- **Avoiding attacks** -
  1. keep s/w + systems fully up to date
  2. Backup your data
  3. keep your website clean
  4. Scan web site for vulnerabilities.

- Security Services :-

(1) Cyber Data Security
(2) Cyber security assessments
(3) Compromise Assessment Services
(4) Managed network Security Service

Protocol Vulnerabilities :-

* DOS - Denial of Service Attack

In this attack hacker makes the System or data unavailable to Someone who needs it.

4 ways to do DOS
(1) Browser Redirection
(2) closing Connection
(3) Destruction
(4) Resource exehaustion

In this attack computer Sends massive amount of traffic to victim's Computer & shut it down.

DOS is slower than DDOS

Can block easily

* DDOS - Distributed DOS

In this attacker tries to make a machine or n/w resource unavailable to user by sending massive traffic from diff. devices.

Basically DOS attacks are done from many different locations using many systems.

DDOS is faster than DOS

Difficult to block as multiple devices are sending packets from multiple locations.

* Session Hijacking :—

It is security attack on user sessions over protected network.

hacker takes control of user's browsing session to gain access to their personal info & pass.

- Ways of Session hijacking

① Cross Site Scripting (XSS Attack) —
attacker can also capture victims Session ID using XSS attack by using Javascript.

Attacker sends crafted link to the victim with malicious JS, when victim clicks on link JS will run & complete the instn made by attacker

② IP Spoofing —

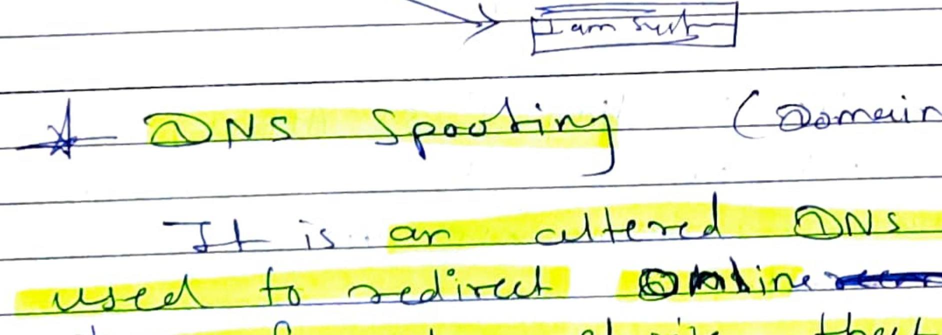
— Spoofing is pretending to be Someone else.

— In this attacker obtains IP address of the client & injects his own packets spoofed with IP address of client. into TCP session, so to fool the server that it is communi-cating with victim i.e original host.

* ARP Spoofing — Address Resolution Protocol spoofing

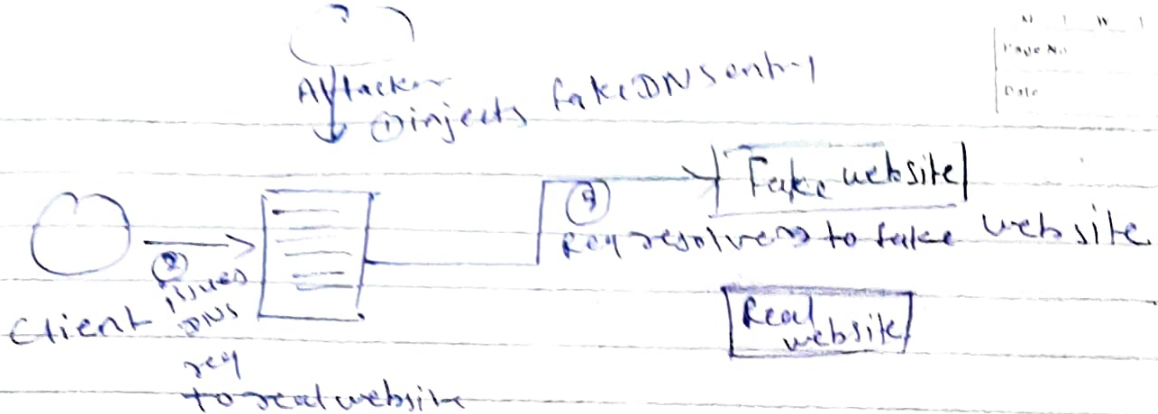
— It is MITM attack that allows attackers to intercept commⁿ betⁿ n/w device

— ARP spoofing attacker pretends to be both sides of n/w commⁿ channel.



* DNS Spoofing (Domain name System Spoofing)

It is an altered DNS records are used to redirect online ~~records~~ ~~a~~ traffic to a fraud website that resembles in intended destination.



* Buffer overflow attack

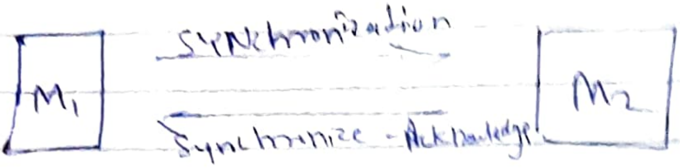
It happens when program tries to fill a block of memory with more than a buffer size. ~~to~~

Buffers are essentially the areas of storage that temporarily hold data while it is being transfered from loc to other.

* Ransomware —

It is a type of malicious S/w that threats to publish or block access to data or a comp system usually by encrypting it, until victim pays a ransom fee to attacker.

✱ SYN Flood Attack :



- In SYN Flood attack Acknowledgement does not happen.

- Type of DoS attack
- also known as half open attack

✱ SQL Injection : —

It is a code based vulnerability that allows an attacker to read & access sensitive data from DB

Attackers can by pass measures of appl^n & use SQL queries to modify, add, update or delete records in DB.