Network Security

* Explain Network Security with its issues.

=> Network Security is a process of protected the network from the outside or unauthorized access to the network.

Network Security is used to protect data from unauthorized access, loss and modification.

The aims of Network Security is provideing confidentiality and accessibility of the data and network.

The Network Security is used to protect the weekness of a computer system.

=> Network Security Issues:

There are main five types of Network Security Issues.

(i) Distributed Denial of Service
(ii) Ransomware

(iii) Vishing
(iv) Thread Hijacking
(v) Cloud-based malware

(i) Distributed Denial of Service Attack:

In this attack, Attacker Flood a networks with such a high volume of traffic, this activity can be shown system unavailable for users.

After this attack, Attacker can implement malware activity and modify the data of system.

(ii) Ransomware: This is one of most expensive cyber threats.

In this attack, Attacker can coruption or loss the data of computer system.

Attacker can exploiting unpatche computer workstations and perform large scale updates in computer system.

(iii) Vishing: Vishing is a most well known social engineering method.

Using the phone, Visher can employ the social engineering method to gain the authorized details.

In Vishing, Visher can use bypass 2FA Method for the pass the second layer of the authentication.

(iv) Thread Hijacking: In this attack, Attacker use the your own email id against you.

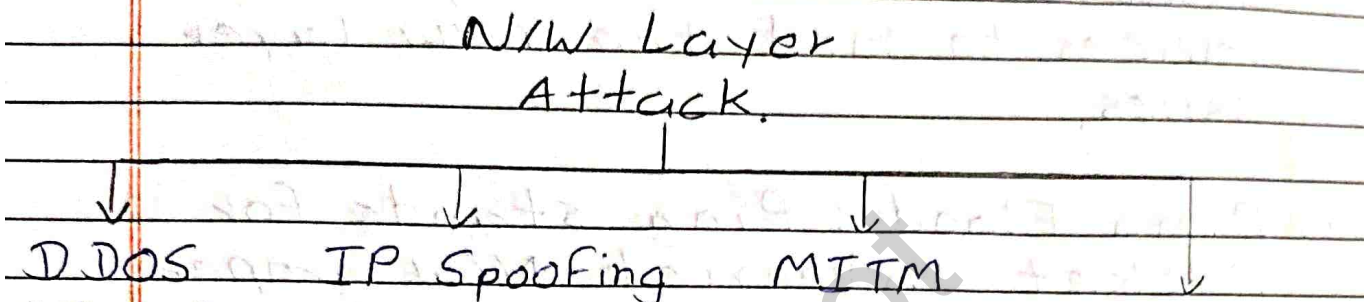
After using internal email id, attacker respond to an email thread with the malware attachment.

(v) Cloud-based Malware: For manage the data or store the data with more secure, we have to use 3rd party vendor.

In this method, Attacker figured out the ways to advantage of this system by using this vulnarablities in the system.

* Explain different types of Network Layer Attack.

=> There are main Four types of Network Layer Attack.



- Ping Flood
- Smarf Attack
- Ping Flood death

(a) DDOS: DDOS stands For Distributed Denial of Service which is extended From of DOS.

In this attack, Attacker needs more than one computer and internet connection For make N/w unavailable.

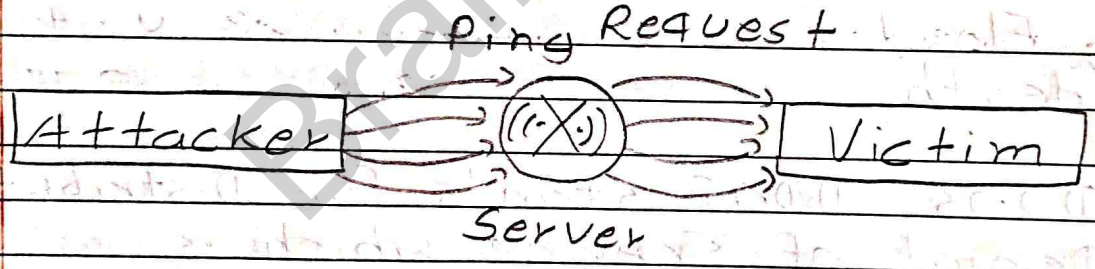
In this system, Attacker target a single system to execute the DOS attack.

=> ICMP Attack : ~~IMP~~ ICMP Attack stands for Internet Control Message Protocol.

ICMP Attack is a type of N/W Layer protocol used by N/W devices to find the N/W layer issues.

(a) Ping Flood : Ping stands for Packet Internet N/W groper.

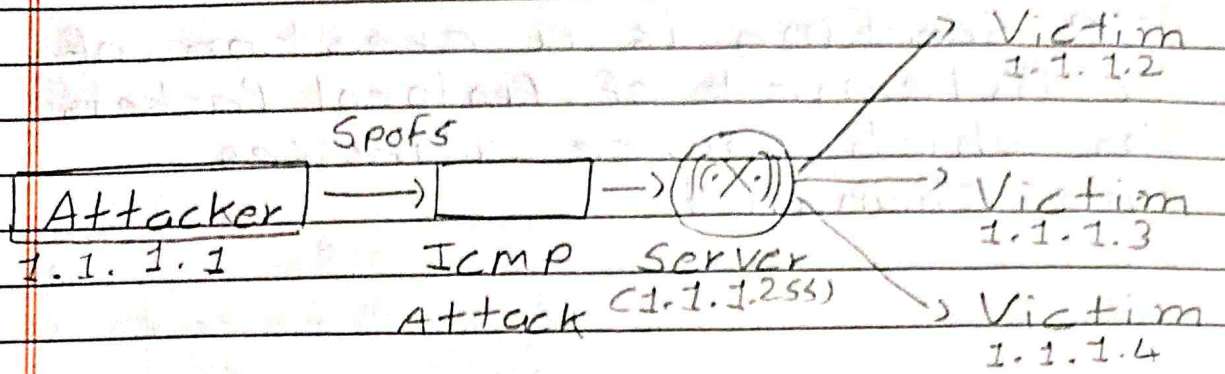
In this attacker sends a thousands or milions of ping requests to a server at a one time.



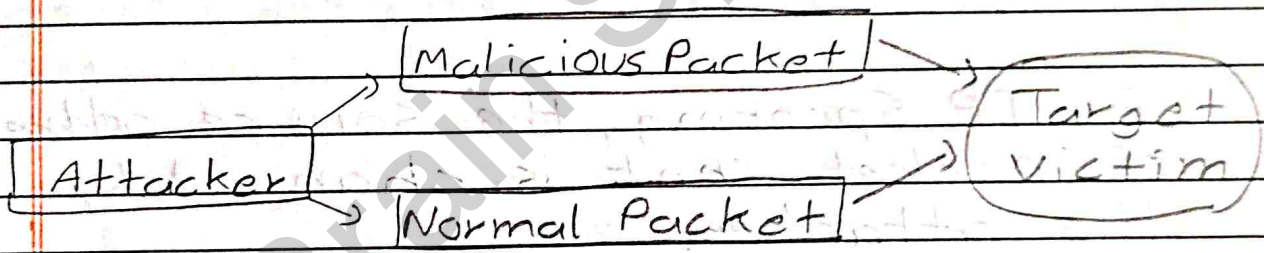
(b) Smarf Attack : In this attack, Attacker is use Ping.

In this attacker, sends out Ping requests to thousands of a Servers.

Attacker Spoofing the IP address in the ping requests for respones go to target.



(c) Ping of Death: In this attack, Attacker send a ping requests that size is larger than to allowable size of target.



B IP Spoofing:

In this Attack, Attacker is use the Fake IP Address for the attack.

Attacker is generates a fake IP address and send to the server then server send the IP Address to the victim.

IP Spoofing is a creation of a Internet of Protocol Packets in which source addresses are changed.

PC-PT	Requests → From: 192.168.1.15	Server-PT	Response → From: 192.168.1.2	Trusted-PC-PT

Attacker 192.168.1.2 192.168.1.15

In IP Spoofing, the source address of packet sent is changed by the attacker.

Due to the lot of traffic, the destination computer consider the packet is come from trusted computer and accepts it.

In IP Spoofing, the attacker sends many spoofed IP address to the server.

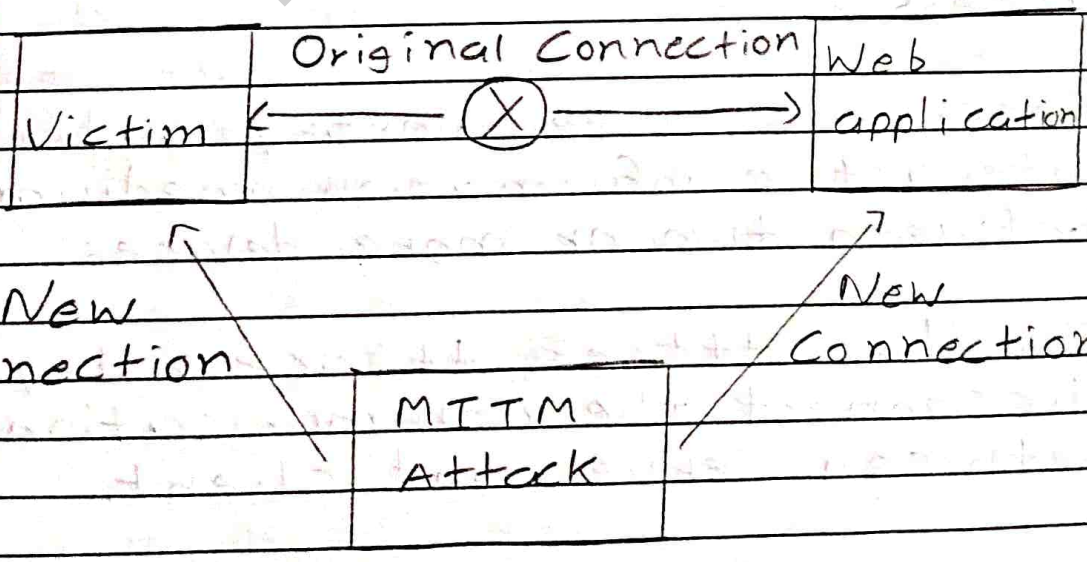
Attacker generate many fake IP address and spoofed into the server.

c MITM Attack: MITM Attack stands For Man-in-the-Middle.

MITM is a type of attack in which unauthorized third party try to manipulate data.

In this Attack, some third party arrange some kind of meeting between the two party by a manipulates both party and achieve access to the data that the two people trying to deliver to each other.

It occurs when some third party between you and other party monitoring and controlling your communication.



In the attack, Attacker can re-route the data exchange path.

When computer are communicating at low level of the Network Layer then computer might know the whom they are exchanging the data.

D Hijacking Attack:

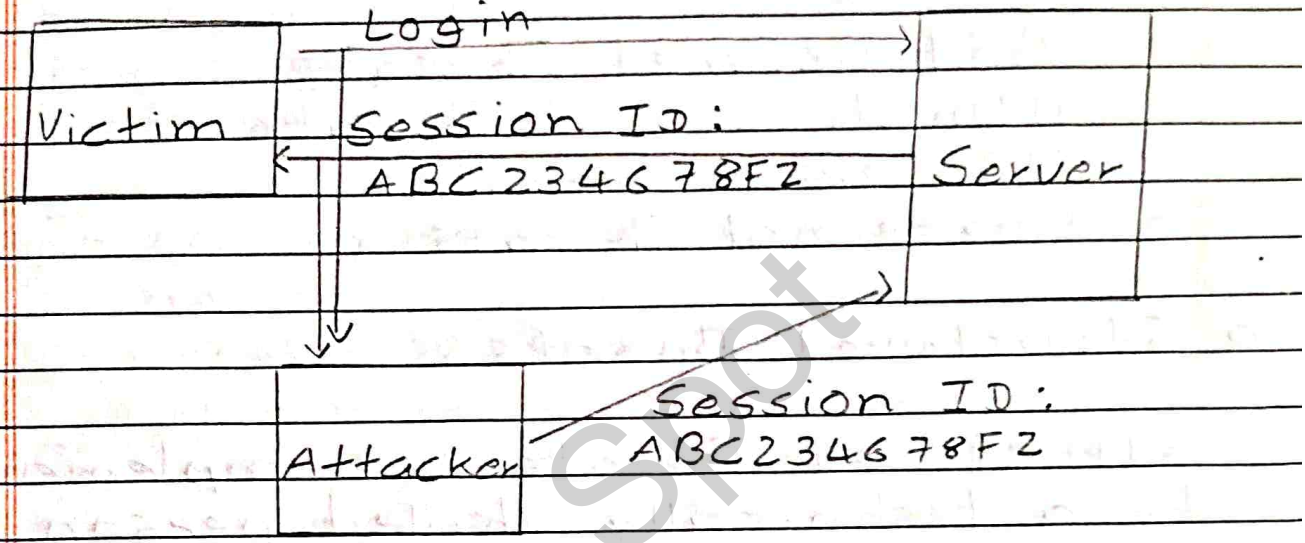
In this attack, Attacker disrupt a session between client and server while both communicating with eachother.

Using the IP Address, Attacker tack over the trusted client access.

Session is a temporary and interactive information medium between two or more devices.

In this Attack, Attacker try to disconnect the communication between server and client.

After that create a new session with server pretending to be the trusted client.



After the create new connection attacker can take that data which attacker want to from server.

Using Same Session ID Attacker access the server data as a Victim or User.

* Explain Types of Comman Threats.

=> There are Main Four types of Comman Threats.

a) Structured Threats
b) Unstructured Threats
c) Internal Threats
d) External Threats

a Structured Threats:

Structured Threats are implemented by a technically skilled person who is trying to gain access to the network.

These people are know the all types of vulnerabilities of the system.

These people are know how to implement all the types of system vulnerabilities.

They understand, develop and implement all the Hijacking Method.

These groups are often involves with the major type of fraud.

B Unstructured Threats:

Unstructured Threats are implement by non-technical person who try to gain access in your Network.

Inexperienced individual try to using the easily available hacking tooles or method.

These people does not do serious damage in the Network.

C External Threats:

Occurs when someone from outside your Network creates a security threats to your network.

This Threats are implemented by individuals or groups working outside of a group.

They does not have authorized access to the computer system or Network.

D Internal Threats:

Our
Occurs when someone from inside your Network creates a security threats to your Network.

This Types of threats are more common and dangerous.

Internal attacker initiated by someone who has authorized access to the Network.

* Explain Intruders in Security.

=> Intruders is one type of Attack, in which person enters in a network places without any permission.

It breach the privacy of user and aims at stealing the users detailes.

There are Three Types of Intruders

a) Masquerader
b) Misfeasor
c) Clandesine Users

a Masquerader:

These are not authorized to use the system but still explore user's privacy and information.

These person are ~~proce~~ processing method that given them control over the system network.

They are outsider, hence they don't have direct access to the system or Network.

B Misfeasor:

These are authorized to use the system but it is misuse the granted permission.

They take advantage of their permission and access given to them.

They are insider and they have direct access to the use of system or Network.

C Clandertine User:

These are supervision/admistrative control over the system and misuse the authoritative power.

The miscontrol of power is often done by supertative authorities for gain Financial advantages.

They can be outsider or insider and they have direct/indirect access to use the system or network.

* Explain Viruses with its Types.

=> Computer viruses are malicious software program or piece of code that infect the computer or whole systems.

Viruses can be spread through files data and using the insecure network.

Once it enters in your system, it can replicate or produce copies of program in system.

There are Seven types of Viruses

1 File Infector Viruses: This viruses are attach with the computer file, after that it can spread to other computer.

2 Boot Sector Viruses: This viruses are infect the system hard drive boot sector which can damage the whole operating system.

3 Macro Viruses: This viruses are small program to execute task which is written in document, when document is open, the viruses can execute its code.

4 Multipartite: This types of viruses can infect both file and hard drive boot sector.

5 Polymorphic: As much as it makes its root deeper in the system while infecting the device it change its code to make itself difficult to detect

6 Rootkit: It has ability so strong that it is nearly impossible to detect the its root in system.

7 Worms: They do not need any types of attachment to any files or program to spread themselves.

* Explain Worms with its Types.

=> Computer worms are a types of malicious software that can self-replicate and spread independently in other computer.

Worms does not need to attach themselves to existing files or programs.

Worms are exploit vulnerabilities in network protocals or operating system to spread.

=> Works:

Computer worms are enter in the system using the systems weekness in networking protocal.

After a computer worm load and begain running on a newly infected system and spread to many other system.

There are Five types of Worms.

1 Email Worm: It is work by creating and sending the email message.

When a user open this email attachments or link then worms can activate and spread to the user's contacts list.

2 File sharing: This worms can sp spread through shared Foldar and spread through peer to peer File sharing network.

3 Cryptoworms: It is work by encrypting data on the victims system.

4 Internet Worms: This Worms is target popular website with the poor security.

It can infect the site.

5 Instant Message: They are marked by attachment or links which spread to the user contanct list

* Difference between Virues and Worms.

	Worms	Virues
1	It is spread using computer Network.	It is spread using the executable file.
2	It eat system Resources.	It can modify the information.
3	Less Harmful compare to virues.	More Harmful compare to worms
4	Can be detected by Antivirus and Firewall.	Antivirus provides protection against virues.
5	Wormes can be controlled by the remote.	Virues can't be controlled by the remote.
6	Execute via weekness of system.	Execute via executable file
7	Spread Faster.	Spread slower.

* Explain Firewall in Network Security

=> A Firewall is a fundamental component of network security that Filter the Incoming and outgoing Network Traffic.

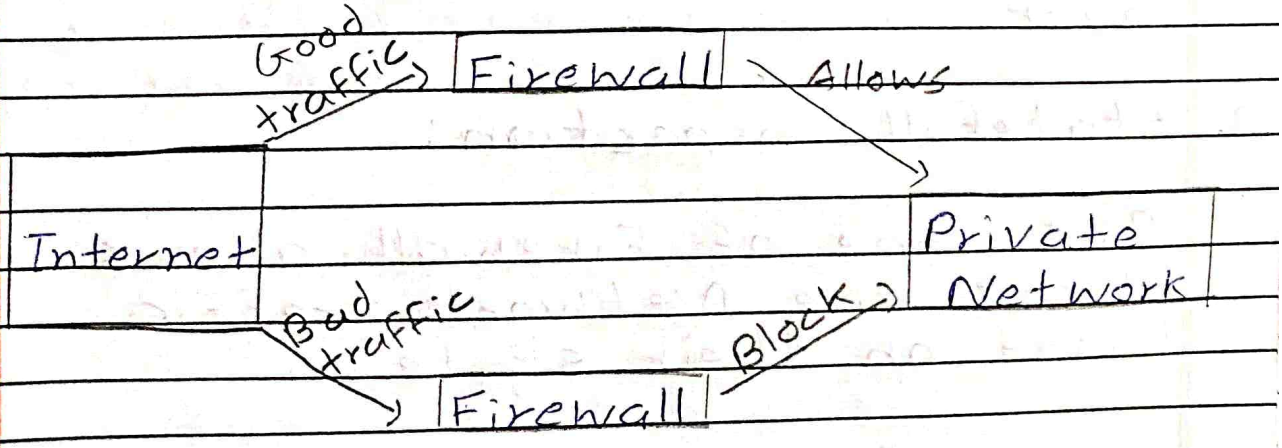
Firewall acts as a barries between a trusted internal network and untrusted external network.

=> Works:

Firewall Filters the Network traffic within a private Network.

It is analyses which traffic should be allowed or not.

Firewall work like entry point of your computer system which allow only trusted system.



There are main Six Types of Firewall.

1) Packet Filtering
2) Proxy Service
3) Statefull Inspection
4) Next Generation Firewall
5) UTM Firewall
6) Threat Focused NGFW

1 Packet Filtering:

Firewalls use packet filtering to inspect and control the flow of data packet based on predefined rules.

2 Proxy Service:

This Type of Firewall is used to inspect the network by filtering message at the application layer.

3 Statefull Inspection:

This Type of Firewall allows or blocks the Network traffic based on their state.

4 Next Generation Firewall:

The NGF is a deep packet inspection Firewall that adds application layer inspection.

5 UTM Firewall:

UTM Firewall refers to when multiple security Features or service are combined into a single device within your Network.

6 Threat Focused NGFW:

This Firewall provides advanced threat detection and mitigation with Network.