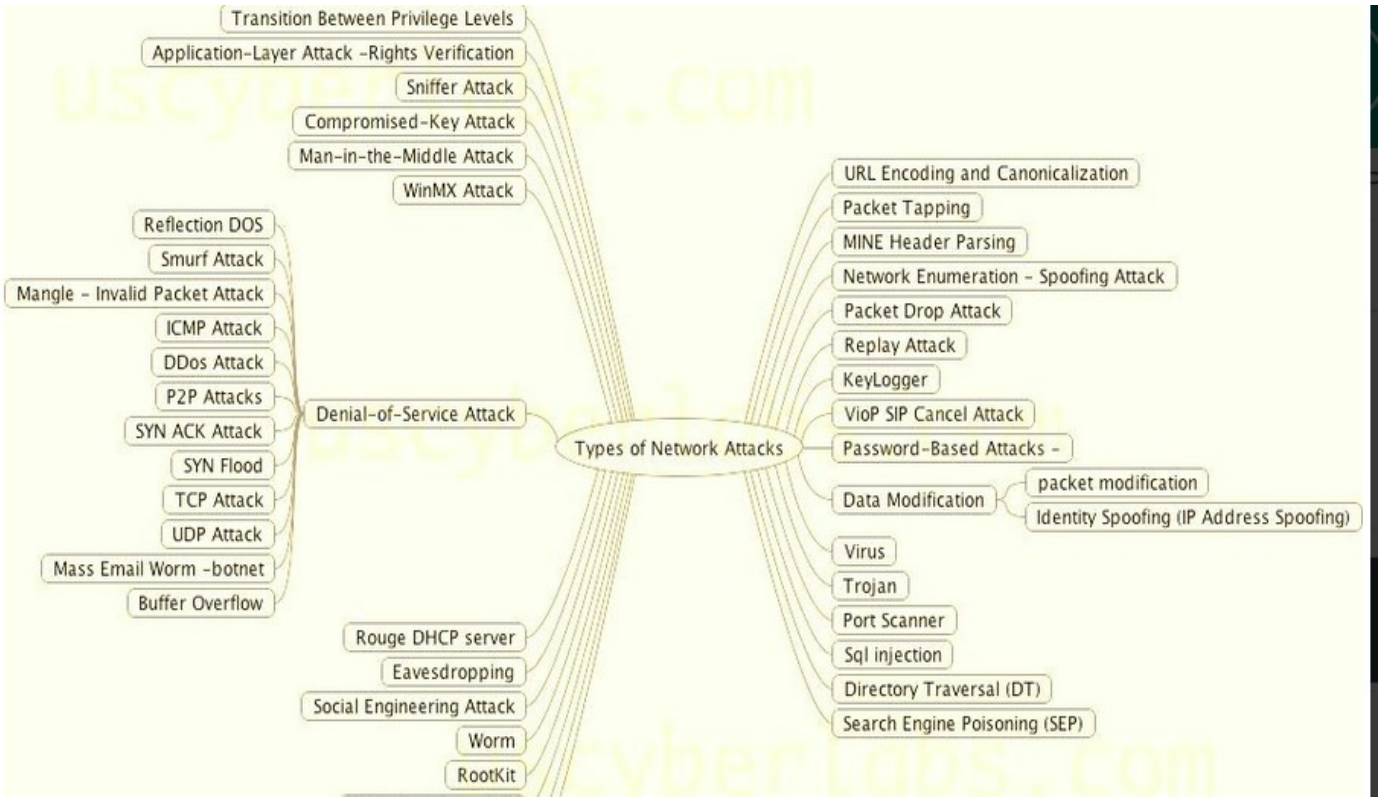
Network Security Threats :-

1. What is Network Security Threats.

Protecting the computer systems in the network from unwanted intrusions and unauthorized access. Security considers several kinds of threats. A threat may be an expressed or demonstrated intent to harm an asset or cause it to become unavailable.
The object of security is to protect valuable or sensitive organizational information while making it readily available. Attackers trying to harm a system or disrupt normal business operations exploit vulnerabilities by using various techniques, methods, and tools.

2. Types of Network Security Threats :



Some of the common security threats are :

- ➔ Malware: Malware is short for “malicious software. Malware as a term used to mean a “variety of forms of hostile, intrusive, or annoying software or program code.” Malware could be computer viruses, worms, Trojan horses, dishonest spyware, and malicious rootkits.

- ➔ Computer virus: A computer virus is a small piece of software that can spread from one infected computer to another. The virus could corrupt, steal, or delete data on your computer even erasing

everything on your hard drive. A virus could also use other programs like email program to spread itself to other computers.

- ➔ Rogue security software: A pop-up window that advertises a security update or alert which appears legitimate and asks to click on a link to install the “update” or “remove” unwanted malicious software that it has apparently detected. This could be rogue security software designed to lure people into clicking and downloading malicious software.

- ➔ Trojan horse: Users can infect their computers with Trojan horse software simply by downloading an application they thought was legitimate but was in fact malicious. Once inside the computer, a Trojan horse can do anything from record passwords by logging keystrokes (known as a keystroke logger) to hijacking your webcam to watch and record every move.

- ➔ Malicious spyware: Malicious spyware is used to describe the Trojan application that was created by cybercriminals to spy on their victims. keylogger software that records a victim’s every keystroke on his or her keyboard. The recorded information is periodically sent back to the originating cybercriminal over the Internet.

- ➔ Computer worm: A computer worm is a software program that can copy itself from one computer to another, without human interaction. Worms can replicate in great volume and with great speed. A worm can send copies of itself to every contact in your email address book and then send itself to all the contacts in your contacts’ address books.

- ➔ Botnet: A botnet is a group of computers connected to the Internet that have been compromised by a hacker using a computer virus or Trojan horse. An individual computer in the group is known as a “zombie“ computer.

- ➔ Spam: Spam in the security context is primarily used to describe email spam unwanted messages in your email inbox. Spam, or electronic junk mail, is a nuisance as it can clutter your mailbox as well as potentially take up space on your mail server.

- ➔ Phishing: Phishing scams are fraudulent attempts by cybercriminals to obtain private information. Phishing scams often appear in the guise of email messages designed to appear as though they are from legitimate sources.

- ➔ Rootkit: A rootkit is a collection of tools that are used to obtain administrator level access to a computer or a network of computers. A rootkit could be installed on computer by a cybercriminal exploiting a vulnerability or security hole in a legitimate application on PC and may contain spyware that monitors and records keystrokes.

Some of the network security threats are :

- ➔ Viruses, worms, and Trojan horses.
- ➔ Spy-ware and adware.
- ➔ Zero-day attacks, also called zero-hour attacks.
- ➔ Hacker attacks.
- ➔ Denial of service attacks.
- ➔ Data interception and theft.
- ➔ Identity theft.

3. Configuration Weakness.

Many network devices have default settings that emphasize performance or ease of installation without regard for security issues. Installation without adequate attention to correcting these settings could create serious potential problems.
Some common configuration issues include the following :

- ➔ Ineffective access control lists failing to block intended traffic.
- ➔ Default, missing, or old passwords.
- ➔ Unneeded ports or services left active.
- ➔ User IDs and passwords exchanged in clear text.
- ➔ Weak or unprotected remote access through the Internet or dial-up services.
- ➔ Outdated Server Application or Software.

4. Steps for Securing Network :

- ➔ Divide the network into segments for efficient network management.

- ➔ Filter Internet access by blocking port1433 and port 1434 or use any firewall software to implement such type of filters.

- ➔ Block all unwanted ports for any chance of being misused; keep open the required communication ports only to data transfer.

- ➔ Monitor open ports, Port 80 is the most commonly used port for http access.

- ➔ Keep all systems updated including server operating systems files and latest patches. These important updates and patches keep the system secure from vulnerabilities.
- ➔ In windows platform, keep client system's automatic update option enabled, so that when ever updates are released clients machines download and installed them and secure them to the maximum level, do the same for server operating system but do monitor to update server OS.

- ➔ IT managers can also use powerful authentication techniques to keep the network secure from security threats.

5. General Flow of attack.

The types of attacks on the security of a computer system or network are best characterized by viewing the function of thecomputer system as providing information. In general, there is a flow of information from a source, such as a file or a region of main memory, to a destination, such as another file or a user.

- ➔ **Normal Flow :**

1) Normal Flow

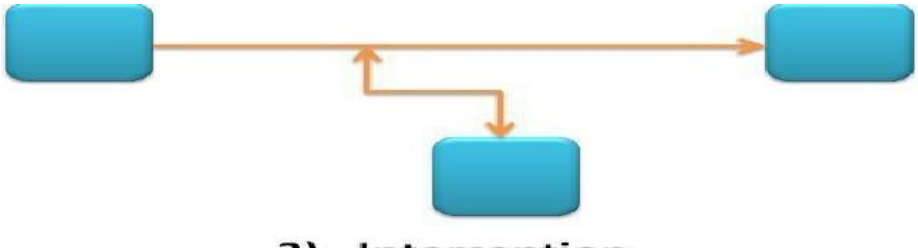
- ➔ **Interruption :**

An asset of the system is destroyed or becomes unavailable or unusable. This is attack availability.

2) Interruption

- ➔ **Interception :**

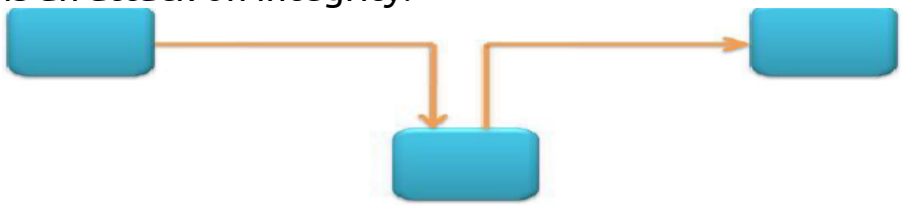
An unauthorized party gains access to an asset. This is an attack on confidentiality, the unauthorized party could be a person, a program or a computer.



3) Interception

➔ **Modification :**

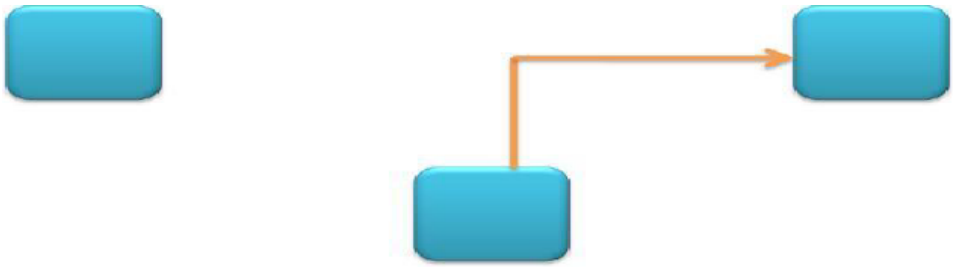
An unauthorized party not only gains access to but tampers with the asset. This is an attack on integrity.



4) Modification

➔ **Fabrication :**

An unauthorized party inserts counterfeit objects into the system. This is an attack on authenticity.



5) Fabrication