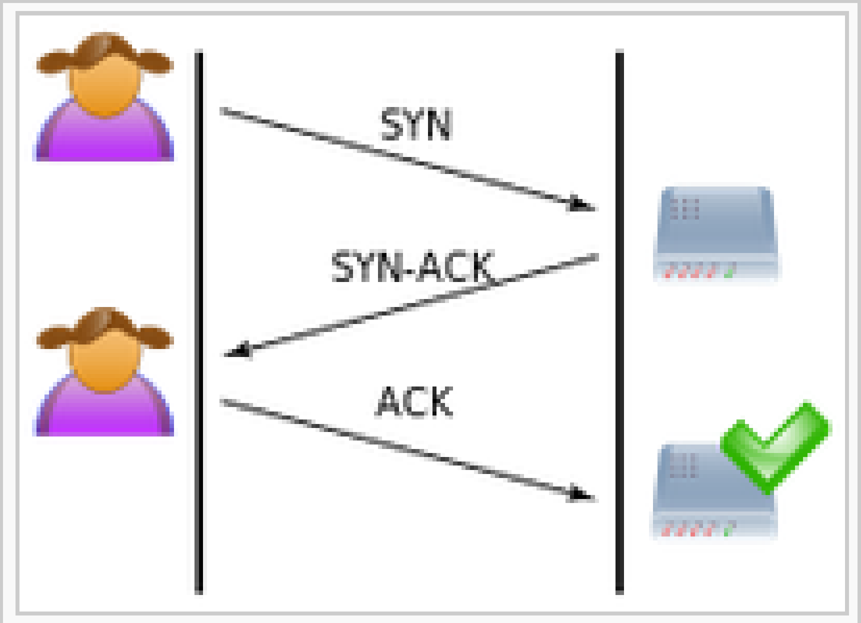
Some Add-on's we Must Know :

Most common way to perform DOS ?
Perform TCP SYN flood.



A normal connection between
a user (Tanu) and a server(Manu).

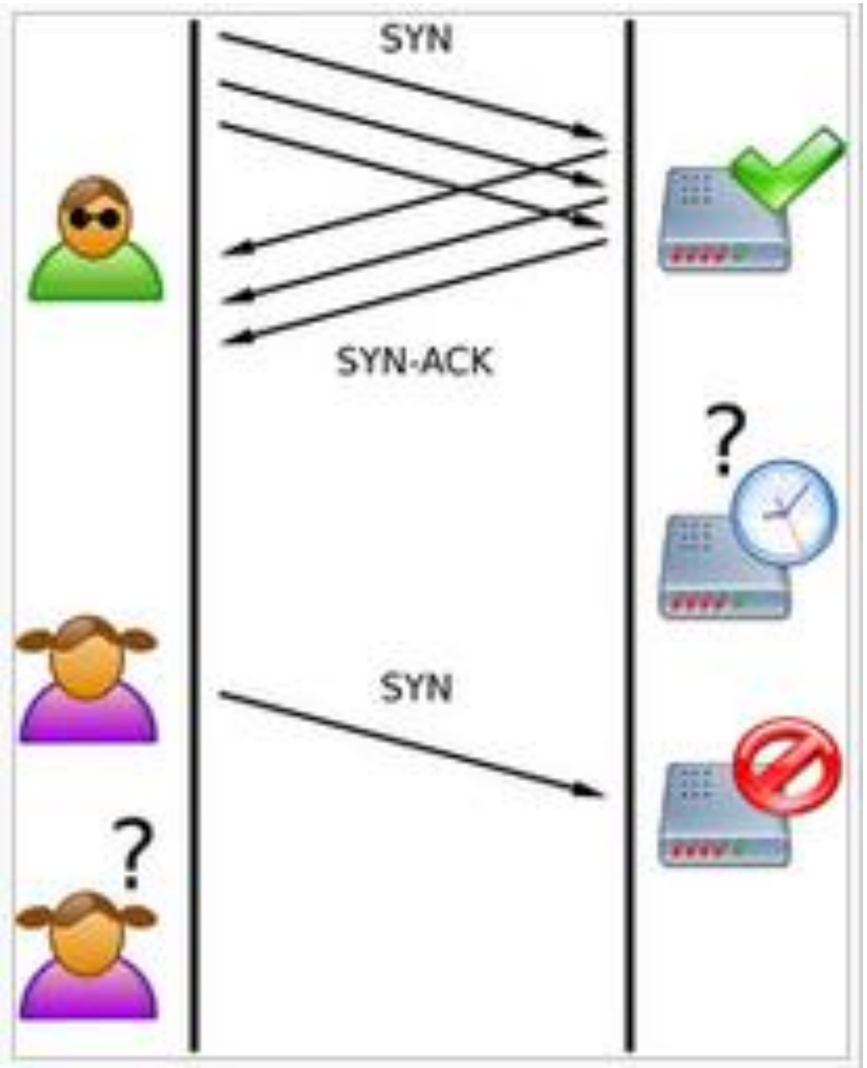
Three-way handshake

A SYN flood is a form of denial-of-service attack in which an attacker

✓ sends a succession of SYN requests to a target's system

✓in an attempt to consume enough server resources

✓to make the system unresponsive to legitimate traffic.



SYN Flood.

The attacker (Janu) sends several packets but does not send the "ACK" back to the server.

The connections are hence half-opened and consuming server resources.

Tanu, a legitimate user, tries to connect but the server refuses to open a connection resulting in a denial of service.

Brief about TCP Connection and SYN Flooding : (for self read)

- Normally when a client attempts to start a TCP connection to a server, the client and server exchange a series of messages which normally runs like this:
- The client requests a connection by sending a SYN (*synchronize*) message to the server.
- The server *acknowledges* this request by sending SYN-ACK back to the client.
- The client responds with an ACK, and the connection is established.
- This is called the TCP three-way handshake, and is the foundation for every connection established using the TCP protocol.

- A SYN flood attack works by not responding to the server with the expected ACK code. The malicious client can either simply not send the expected ACK, or by spoofing the source IP address in the SYN, causing the server to send the SYN-ACK to a falsified IP address - which will not send an ACK because it "knows" that it never sent a SYN.

- The server will wait for the acknowledgement for some time, as simple network congestion could also be the cause of the missing ACK, but in an attack increasingly large numbers of *half-open connections* will bind resources on the server until no new connections can be made, resulting in a denial of service to legitimate traffic. Some systems may also malfunction badly or even crash if other operating system functions are starved of resources in this way.

Brief about Virus

anatomy of a Virus : 3 parts:

1. Replicator

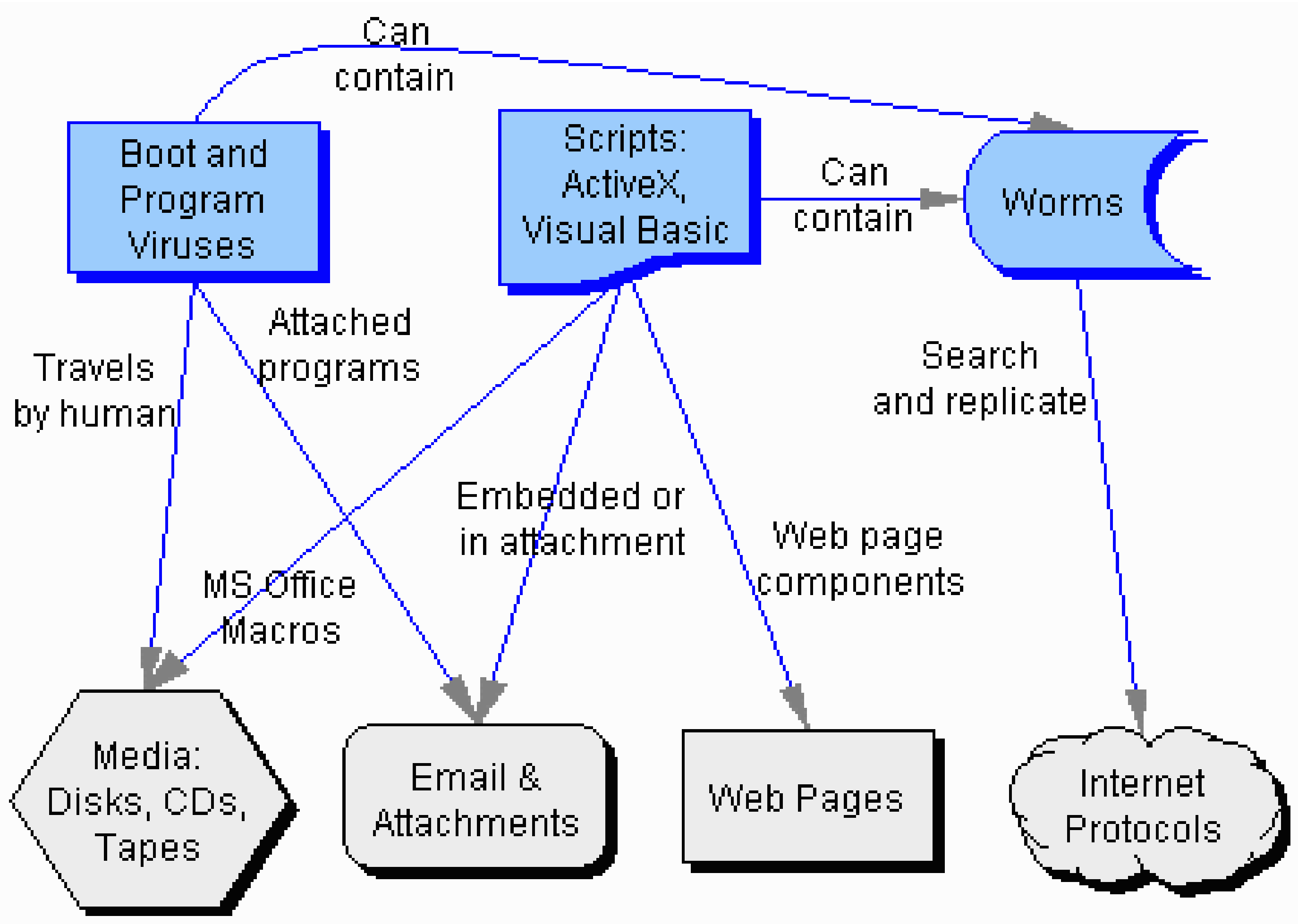
Replicates , thereby ensures survival

2. Concealer

3. Payload

Types of Virus :

1. Boot
2. Program
3. Multipartite
4. Stealth
5. Polymorphic
6. Macro
7. Active X



Types of Virus with Description :

Boot viruses:

These viruses infect floppy disk boot records or master boot records in hard disks. They replace the boot record program (which is responsible for loading the operating system in memory) copying it elsewhere on the disk or overwriting it. Boot viruses load into memory if the computer tries to read the disk while it is booting.

Examples: Form, Disk Killer, Michelangelo, and Stone virus

Program viruses:

These infect executable program files, such as those with extensions like .BIN, .COM, .EXE, .OVL, .DRV (driver) and .SYS (device driver). These programs are loaded in memory during execution, taking the virus with them. The virus becomes active in memory, making copies of itself and infecting files on disk.

Examples: Sunday, Cascade

Multipartite viruses:

A hybrid of Boot and Program viruses. They infect program files and when the infected program is executed, these viruses infect the boot record. When you boot the computer next time the virus from the boot record loads in memory and then starts infecting other program files on disk. **Examples: Invader, Flip, and Tequila**

Types of Virus with Description … contd….

Stealth viruses:

These viruses use certain techniques to avoid detection. They may either redirect the disk head to read another sector instead of the one in which they reside or they may alter the reading of the infected file's size shown in the directory listing. For instance, the Whale virus adds 9216 bytes to an infected file; then the virus subtracts the same number of bytes (9216) from the size given in the directory.

Examples: Frodo, Joshi, Whale

Polymorphic viruses:

A virus that can encrypt its code in different ways so that it appears differently in each infection. These viruses are more difficult to detect.

Examples: Involuntary, Stimulate, Cascade, Phoenix, Evil, Proud, Virus 101

Macro Viruses:

A macro virus is a new type of computer virus that infects the macros within a document or template. When you open a word processing or spreadsheet document, the macro virus is activated and it infects the Normal template (Normal.dot)-a general purpose file that stores default document formatting settings. Every document you open refers to the Normal template, and hence gets infected with the macro virus. Since this virus attaches itself to documents, the infection can spread if such documents are opened on other computers.

Examples: DMV, Nuclear, Word Concept.

Active X:

Java controls and ActiveX will soon be the scourge of computing. Most people do not know how to control there web browser to enable or disable the various functions like playing sound or video and so, by default, leave a nice big hole in the security by allowing applets free run into there machine. There has been a lot of commotion behind this and with the amount of power that JAVA imparts, things from the security angle seem a bit gloom.