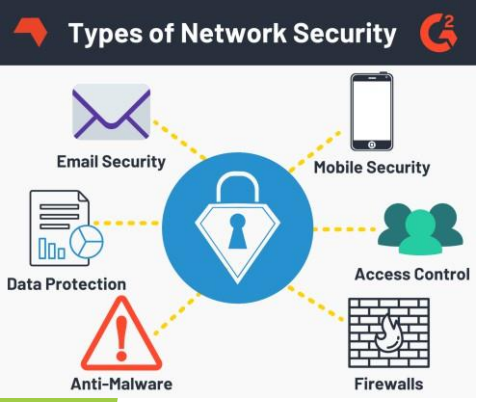
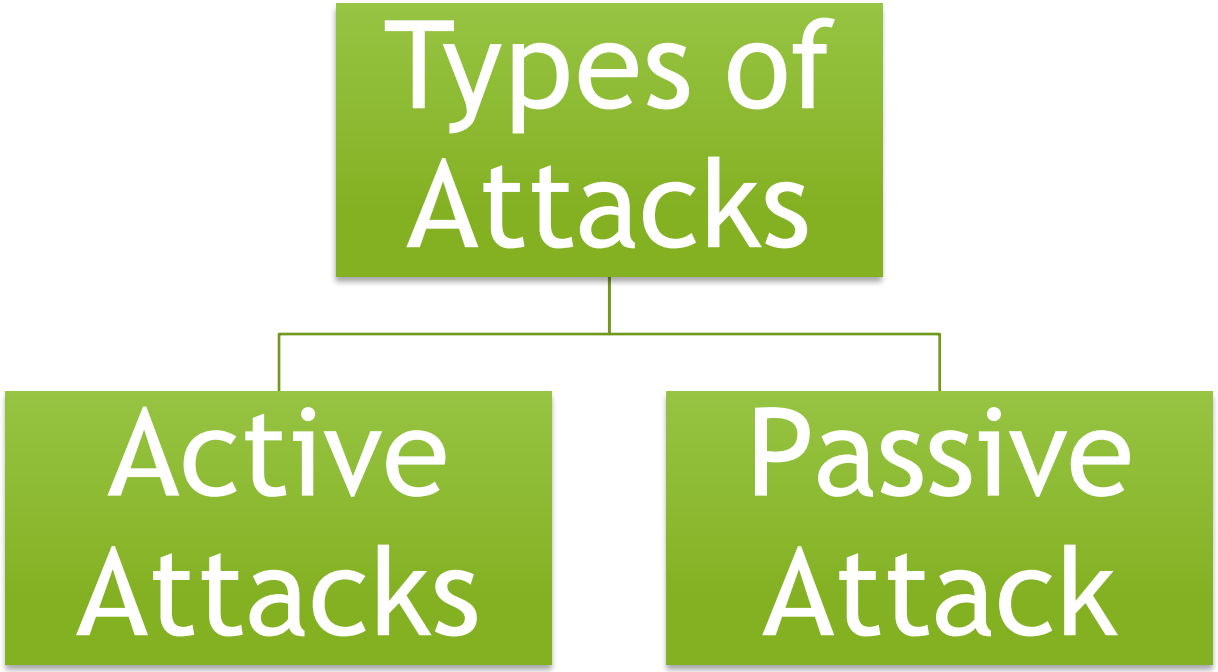
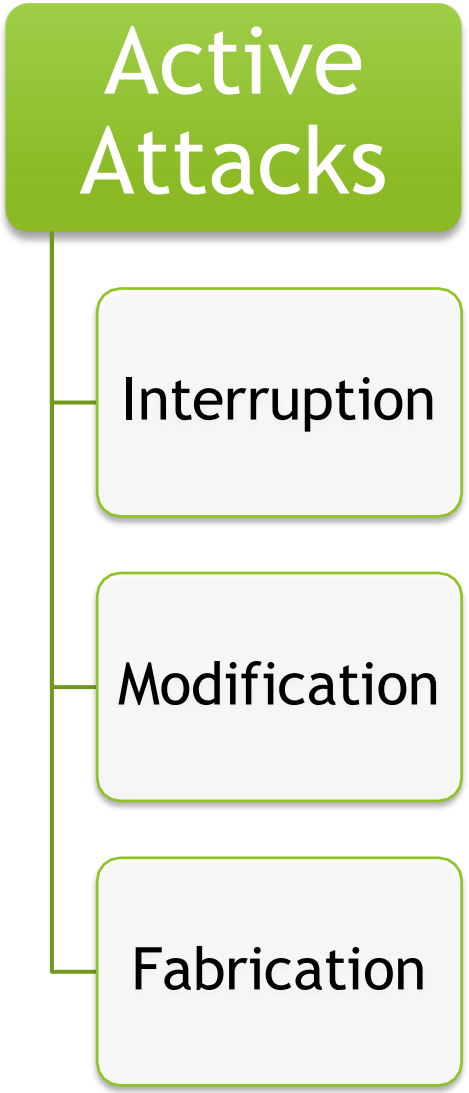


NIS
(Network and Information Security)
&
SIC
(Security In Computing)

Attack:- Attack is a path or way by which hacker can gain access to computer system without your prior knowledge



Active Attack:- In active attacks, the contents of the original message are modified in some way. These attacks cannot be prevented easily



Active Attacks

Interruption

- It causes when an unauthorized user pretends to be another user

Modification

- It contains replay attack and alterations. A user captures a sequence of event and re-sends it. Alteration involves some modification/changes to the original message.

Fabrication

- It is an attempt to prevent authorized users from accessing some services. E.g. Denial of Service (DoS) attacks.

Passive Attack:- Passive attacks are those, where attacker aims to obtain information that is in transit.

In passive attack, attacker does not involve any modifications to the contents of an original message. So, the passive attacks are hard to detect

Passive Attacks

Release of Message Contents

- Release of message contents means a confidential message should be accessed by authorized user otherwise a message is released against our wishes

Traffic Analysis

- Traffic analysis is a passive attacker may try to find out similarities between encodes message for some clues regarding communication and this analysis is knows as traffic analysis

Denial of Service (DoS) Attack

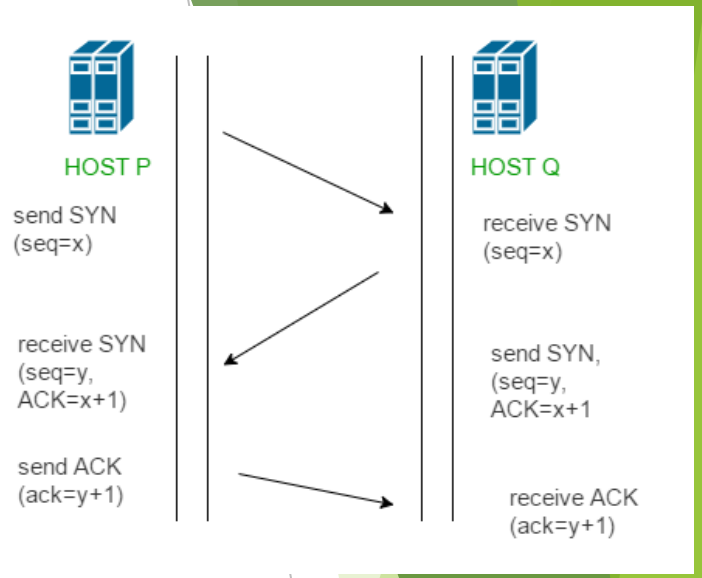
- DoS attack is a type of attack which can exploit a know vulnerability in a specific application or OS, or may attack features or weaknesses in particular protocols or services.
- Using this attack, attacker attempts to deny unauthorized access to specific information or to the computer system or network itself.
- Aim of this attack is to simply prevent access to the target system, or the attack can be used in combination with other actions in order to gain unauthorized access to a computer or network. E.g:- SYN Flooding attack and POD attack.
- DoS attacks are conducted using a single attacking system.

SYN Flooding Attack

- SYN Flooding attack, used to prevent the services to the system. It takes the advantage of trusted relationship and TCP/IP networks design. This attack uses TCP/IP three-ways handshake for connection between two systems.
- Now what exactly is THREE WAY HANDSHAKE

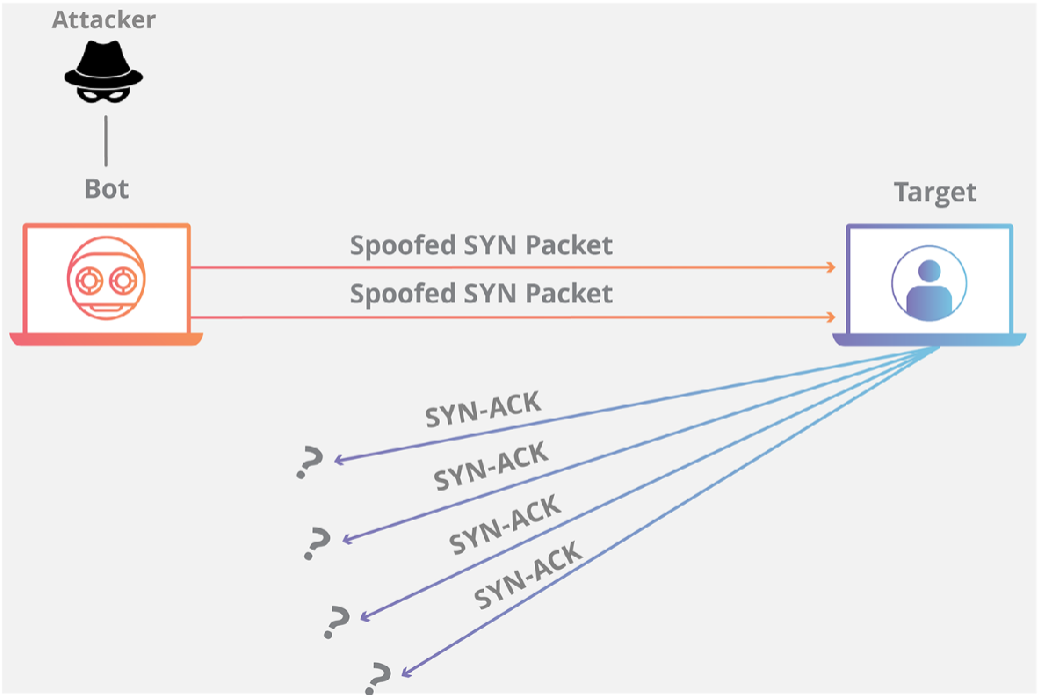
Three-way Handshake

- Step 1(SYN):- In first step, the clients want to establish a connection with a server, so it sends a segment with SYN which informs the server that the clients wants to start a communication and with that sequence number it starts the segments with
- Step 2(SYN + ACK):- Server responds to the client request with SYN-ACK signal bit set. Acknowledgement(ACK) signifies the response of the segment it received and SYN signifies with what sequence number it is likely to start the segments with
- Step 3(ACK):- In the final part client acknowledges the response of the server and they both establish a reliable connection with which they will start the actual data transfer.



SYN Flooding Attack

- In SYN Flooding Attack, the attacker sends a high volume of SYN packets to the targeted server, often with Spoofed IP Addresses.
- The server then responds to each one of the connection requests and leaves an open port ready to receive the response.
- While the server waits for the final ACK packet, which never arrives, the attacker continues to send more SYN packets. The arrival of each new SYN packet causes the server to temporarily maintain a new open port connection for a certain length of time, once all the available ports have been utilized the server is unable to function normally.

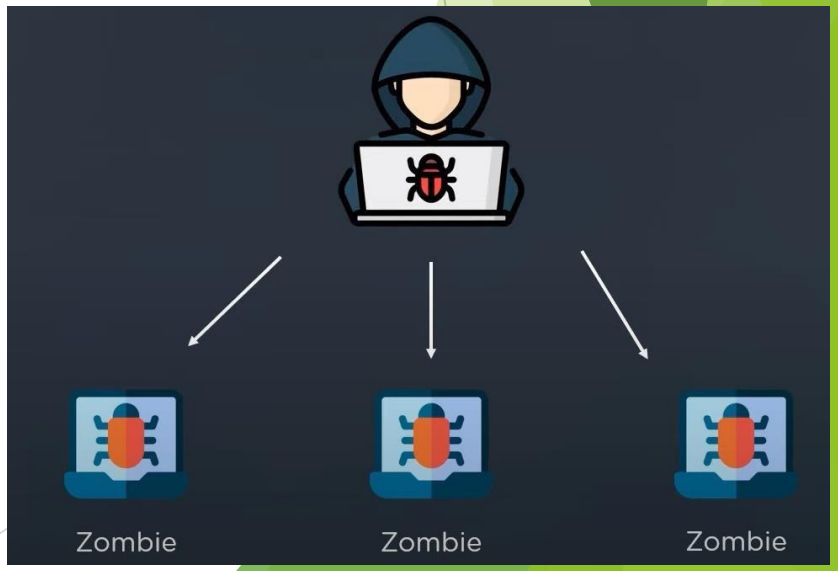


Ping-of-death (POD) attack

- Attacker sends an Internet Control Message Protocol (ICMP) “ping” packet equal to or exceeding 64 kB.
- This type of packet should not occur naturally.
- Certain systems were not able to handle such large size of packet, and the system would hang or crush.
- Attackers use ping commands to develop a ping of death command. They can write a simple loop that allows them to execute the ping command with packet sizes that exceed the 65,535-byte maximum level when the target machine attempts to put the fragments back together.

Distributed Denial of Service (DDoS)

- Denial of Service attack is using multiple attacking system which are known as **Distributed Denial of Service (DDoS) attack**
- Goal is to deny the use or access to specific service or system.
- In DDoS attack the method is used to deny a service by simply overwhelm the target with traffic from many different systems.
- This attack is a two-step process.
- In the first step, the attacker creates multiple botnet also called as Zombies.
- Attacker uses this zombies to attack on the targeted system whenever the attacker initiates it using malware infusion



Distributed Denial of Service (DDoS)

- Then these bots flood the target with continuous requests that causes the server system to crash.

Distributed Denial of Service (DDoS)

- One important thing of a DDoS attack is that with just a few messages to the agents, the attacker can have a flood of messages sent against the targeted system

- To stop or mitigate the effects of DoS and DDoS attack, one important precaution is to be taken that is apply the latest patches and upgrades to your system ad the application running on them

Thank you for Hearing with Patience