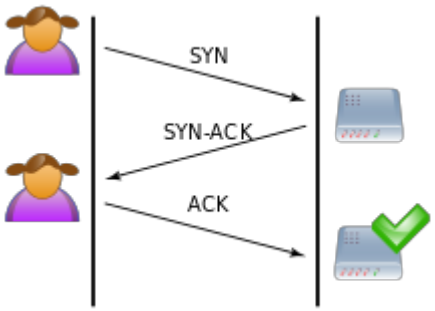
WIKIPEDIA

SYN flood

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.[1][2]



A normal connection between a user (Alice) and a server. The three-way handshake is correctly performed.

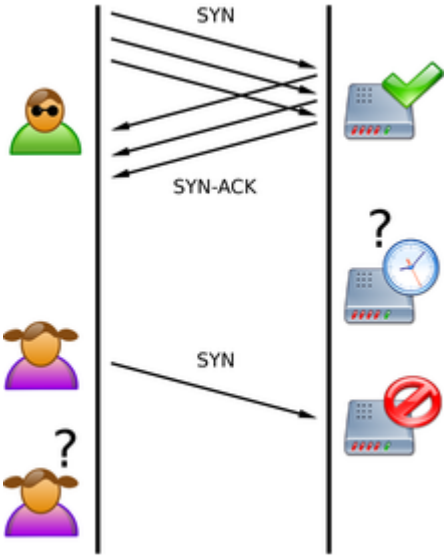
Contents

Technical details

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:

1. The client requests a connection by sending a SYN (*synchronize*) message to the server.
2. The server *acknowledges* this request by sending SYN–ACK back to the client.
3. 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.



SYN Flood. The attacker (Mallory) sends several packets but does not send the "ACK" back to the server. The connections are hence half-opened and consuming server resources. Alice, a legitimate user, tries to connect but the server refuses to open a connection resulting in a denial of service.

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. However, in an attack, the *half-open connections* created by the malicious client bind resources on the server and may eventually exceed the resources available on the server. At that point, the server cannot connect to any

clients, whether legitimate or otherwise. This effectively denies service to legitimate clients. Some systems may also malfunction or crash when other operating system functions are starved of resources in this way.

Countermeasures

There are a number of well-known countermeasures listed in RFC 4987 including:

1. Filtering
2. Increasing Backlog
3. Reducing SYN-RECEIVED Timer
4. Recycling the Oldest Half-Open TCP
5. SYN Cache
6. SYN cookies
7. Hybrid Approaches
8. Firewalls and Proxies

See also

- Denial-of-service attack
- Fraggle attack
- Internet Control Message Protocol
- IP address spoofing
- Ping flood
- Smurf attack
- UDP flood attack

References

1. TCP SYN Flooding and IP Spoofing Attacks (https://www.cert.org/historical/advisories/CA-1996-21.cfm), 1996 Advisory, Software Engineering Institute, Carnegie-Mellon University
2. New York's Panix Service Is Crippled by Hacker Attack (https://partners.nytimes.com/library/cyber/week/0914panix.html), New York Times, September 14, 1996

External links

- Official CERT advisory on SYN Attacks (http://www.cert.org/advisories/CA-1996-21.html)