SYN Flood Attack Linux

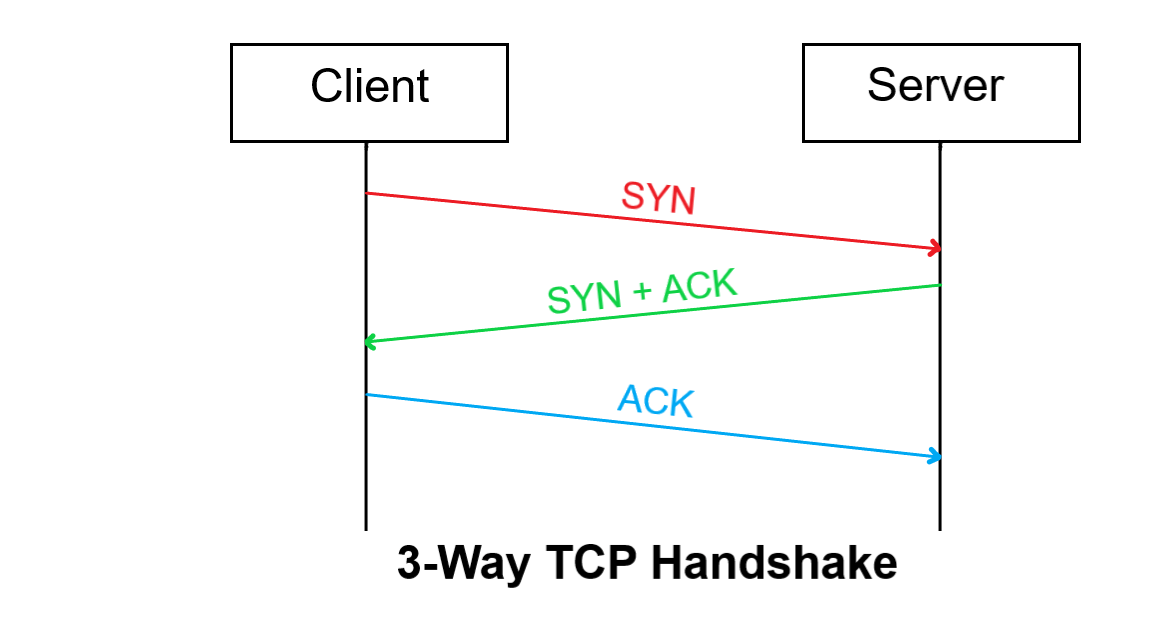
As businesses become more reliant on delivering services through the Internet, distributed denial of service (DDoS) assaults are becoming more widespread. The concept of SYN flood attacks is not new, and it has been around for ages. It was one of the techniques available to hackers even before the world wide web was born.

With time the system to protect from this attack became more well defined and better tested. This article will give you a few approaches to protecting yourself or your network from such an attack.

## What is an SYN flood attack?

An SYN flood (half-open attack) is a denial-of-service (DDoS) attack aiming to make the server unavailable to authorized traffic by consuming all available server resources.

An SYN flood works by not responding to the server with the expected ACK code after sending a synchronized packet (SYN) as part of the TCP three-way handshake. The server will wait for a response from the client, and if none comes, the connection times out.



Source: [thepythoncode.com](https://www.thepythoncode.com/article/syn-flooding-attack-using-scapy-in-python)

This can be exploited to cause the server to wait for incoming connections without closing them and therefore keep its internal connection table full, preventing it from receiving any more connections. The business will not be able to reply even to legitimate clients.