**SYN-флуд** — одна из разновидностей сетевых атак типа отказ от обслуживания, которая заключается в отправке большого количества SYN-запросов (запросов на подключение по протоколу TCP) в достаточно короткий срок (RFC 4987).

Согласно процессу «трёхкратного рукопожатия» TCP, клиент посылает пакет с установленным флагом SYN (*synchronize*). В ответ на него сервер должен ответить комбинацией флагов SYN+ACK (*acknowledges*). После этого клиент должен ответить пакетом с флагом ACK, после чего соединение считается установленным.

Принцип атаки заключается в том, что злоумышленник, посылая SYN-запросы, переполняет на сервере (цели атаки) очередь на подключения. При этом он игнорирует SYN+ACK пакеты цели, не высылая ответные пакеты, либо подделывает заголовок пакета таким образом, что ответный SYN+ACK отправляется на несуществующий адрес. В очереди подключений появляются так называемые полуоткрытые соединения ([англ.](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) *half-open connection*), ожидающие подтверждения от клиента. По истечении определенного тайм-аута эти подключения отбрасываются. Задача злоумышленника заключается в том, чтобы поддерживать очередь заполненной таким образом, чтобы не допустить новых подключений. Из-за этого клиенты, не являющиеся злоумышленниками, не могут установить связь, либо устанавливают её с существенными задержками.

Используя эти фильтры, мы должны иметь возможность обнаруживать различные сканирования сетевого обнаружения, **тесты ping** и другие вещи, которые обычно выполняются **на этапе исследования (обнаружение активов)**

Если мы видим множество этих ARP-запросов, запрашивающих множество **разных IP-адресов** за короткий период времени, вполне вероятно, что кто-то пытается обнаружить **действующие IP-адреса** в нашей сети с помощью **ARP-сканирования**

**TCP ping** обычно использует **порт 7 (эхо).** Если мы видим, что больше этого трафика направляется на множество разных IP-адресов, это означает, что кто-то, вероятно, выполняет проверку связи TCP, чтобы **найти активные хосты в сети (например, запустив nmap -sn -PS / -PA <subnet>).**

i am a team programmer, my task was to write a code that will send tcp packets to a specific port. also create a website and connect it to the docker file to check the code itself. The goal of the project is to drop the site so that it does not respond to requests