Министерство образования Республики Беларусь

Учреждение образования

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет компьютерных систем и сетей

Кафедра информатики

Дисциплина: Информационные сети. Основы безопасности

ОТЧЕТ

к лабораторной работе №4

на тему

**АТАКИ ПРИ УСТАНОВКЕ TCP-СОЕДИНЕНИЯ И ПРОТОКОЛОВ ПРИКЛАДНОГО УРОВНЯ**

Выполнил:

студент гр. 253504

Носкович П.Н.

Проверил:

Герчик А.В.

Минск 2025

СОДЕРЖАНИЕ

[Введенеие 3](#_Toc157436533)

[1 Краткие теоретические сведения 4](#_Toc157436534)

[2 Результат выполнения программы 9](#_Toc157436535)

[Приложение А 13](#_Toc157436537)

# ВВЕДЕНИЕ

Цель данной лабораторной работы заключается в изучении теоретических сведений по работе адресации в сети *Internet*, физического, канального и транспортного уровней, а также разработке программы, реализующее атаки на протокол при установке *TCP*-соединения. В интерфейсе приложения необходимо продемонстрировать передаваемые данные, исходные данные протокола и проверки каждой из сторон.

# 1 КРАТКИЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

Стек протоколов *TCP/IP (Transmission Control Protocol/Internet Protocol,* протокол управления передачей/протокол интернета) – сетевая модель, описывающая процесс передачи цифровых данных. модель *TCP/IP* разделена на уровни, как и *OSI*, но отличие двух моделей в количестве уровней. Документами, определяющими сертификацию модели, являются *RFC1122* и *RFC1123*. Эти стандарты описывают четыре уровня абстракции модели *TCP/IP*: прикладной, транспортный, межсетевой и канальный (см. рисунок 1.1).

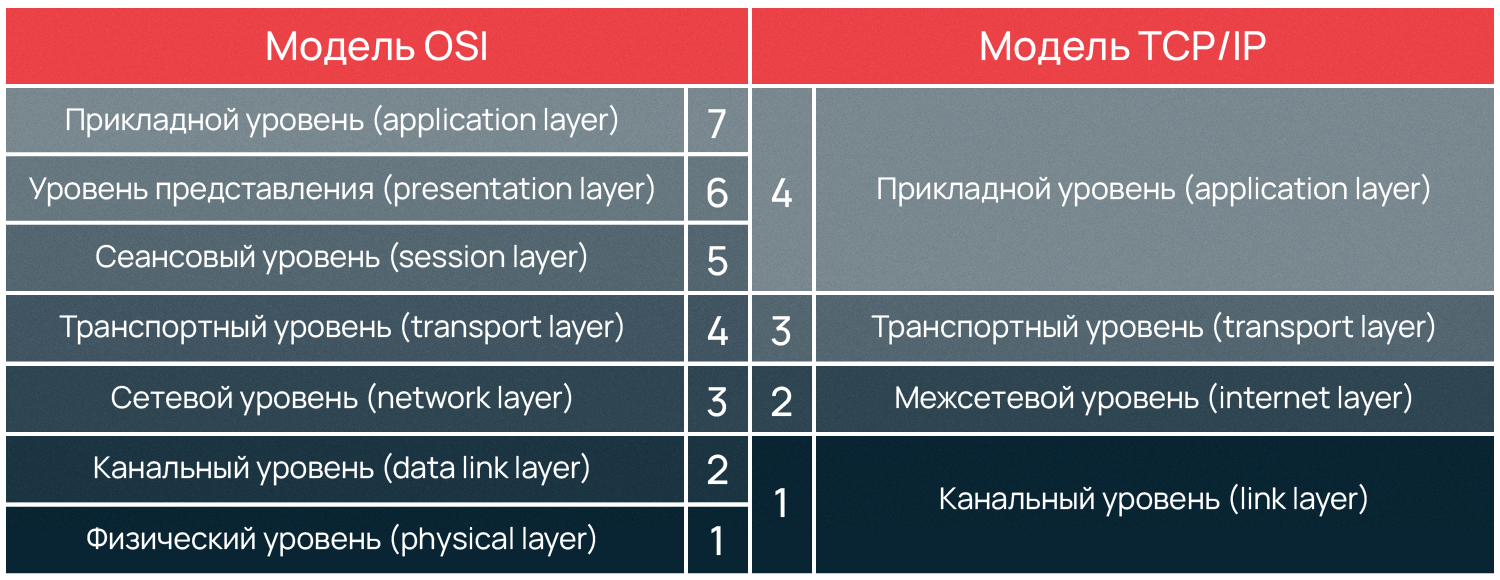


Рисунок 1.1 – Сравнение модели *OSI* и *TCP/IP*

Предназначение канального уровня – дать описание тому, как происходит обмен информацией на уровне сетевых устройств, определить, как информация будет передаваться от одного устройства к другому. Информация здесь кодируется, делится на пакеты и отправляется по нужному каналу, т. е. среде передачи. Этот уровень также вычисляет максимальное расстояние, на которое пакеты возможно передать, частоту сигнала, задержку ответа и т. д. Все это – физические свойства среды передачи информации. На канальном уровне самым распространенным протоколом является *Ethernet.*

Глобальная сеть интернет состоит из множества локальных сетей, взаимодействующих между собой. Межсетевой уровень используется, чтобы описать обеспечение такого взаимодействия. Межсетевое взаимодействие – это основной принцип построения интернета. Локальные сети по всему миру объединены в глобальную, а передачу данных между этими сетями осуществляют магистральные и пограничные маршрутизаторы. Именно на межсетевом уровне функционирует протокол *IP*, позволивший объединить разные сети в глобальную. Как и протокол *TCP*, он дал название модели.

Постоянные резиденты транспортного уровня — протоколы *TCP* и *UDP*, они занимаются доставкой информации.

*TCP* (протокол управления передачей) – надежный, он обеспечивает передачу информации, проверяя дошла ли она, насколько полным является объем полученной информации и т. д. *TCP* дает возможность двум конечным устройствам производить обмен пакетами через предварительно установленное соединение. Он предоставляет услугу для приложений, повторно запрашивает потерянную информацию, устраняет дублирующие пакеты, регулируя загруженность сети. *TCP* гарантирует получение и сборку информации у адресата в правильном порядке.

В заголовке *TCP* содержатся следующие основные поля:

– *Source port* (16 бит): порт источника. Порт хоста, от которого исходит запрос.

– *Destination port* (16 бит): порт назначения. Порт хоста, куда направляется запрос.

– *Sequence number*, *SYN* (32 бита): порядковый номер. Позволяет контролировать порядок сообщений. Каждая конечная точка (как порт источника, так и порт назначения) будут поддерживать свой уникальный порядковый номер для отправляемых сообщений. При установлении соединения *TCP* (используется сообщение с установленным флагом *SYN*) в качестве изначального порядкового номера будет сгенерировано случайное число.

– *Acknowledgement number*, *ACK* (32 бита): номер подтверждения. Когда сообщение содержит флаг *ACK*, то значение в номере подтверждения должно соответствовать следующему порядковому номеру (*SYN*), которое отправитель сообщения с флагом *ACK* ожидает получить от передающей системы. Таким образом, отправка одного номера подтверждения способна подтвердить получение всех байтов с информацией, полученных до этого.

– *ACK* (1 бит). Устанавливается, когда пакет содержит значение номера подтверждения в поле подтверждения. Все пакеты после стартового пакета *SYN* будут иметь установленный флаг *ACK*.

– *RST* (1 бит): сброс данного соединения. Отправкой пакета *RST* одна из сторон сообщает о немедленном разрыве соединения. При этом соединение обрывается, а буфер очищается. Самые распространенные причины отправки пакета с установленным флагом *RST* — ответ на пакет, полученный для закрытого сокета; пользователь сам прервал соединение (например, закрыв браузер, не дожидаясь ответа); соединение не было нормально закрыто, но находится в неактивном состоянии некоторое время.

– *SYN* (1 бит). Начинает соединение и синхронизирует порядковые номера. Первый пакет, отправленный с каждой стороны, должен в обязательном порядке иметь установленным этот флаг.

– *FIN* (1 бит). Одна из конечных точек отправляет пакет с установленным флагом *FIN* для другой конечной точки, чтобы сообщить, что все пакеты были отправлены, и соединение пора завершить.

– *Window size* (16 бит): размер окна приема. В нем указывается количество байт данных, считая от последнего номера подтверждения, которые готов принять отправитель данного пакета. Другими словами, отправитель данного пакета в этом поле сообщает другой стороне, каким доступным на данный момент размером буфера приема данных он располагает.

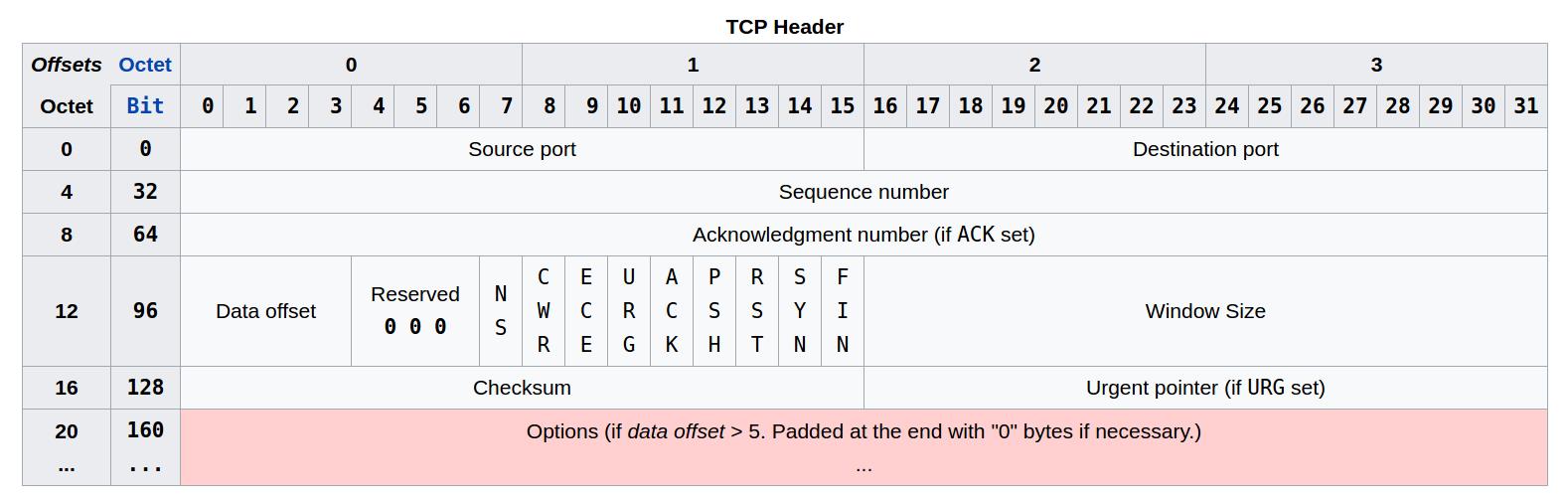


Рисунок 1.2 – Заголовок *TCP*

Перед тем, как данные могут быть переданы между двумя узлами, в *TCP*, в отличие от *UDP*, предусмотрена стадия установки соединения. Также после того, как все данные были переданы, наступает стадия завершения соединения. Таким образом, осуществление каждого *TCP*-соединения можно условно разделить на три фазы: инициализация соединения, загрузка данных, завершение соединения.

Установка соединения осуществляется с помощью, так называемого трехстороннего рукопожатия *TCP* (см. рисунок 1.3). Инициатором соединения может выступать любая сторона.

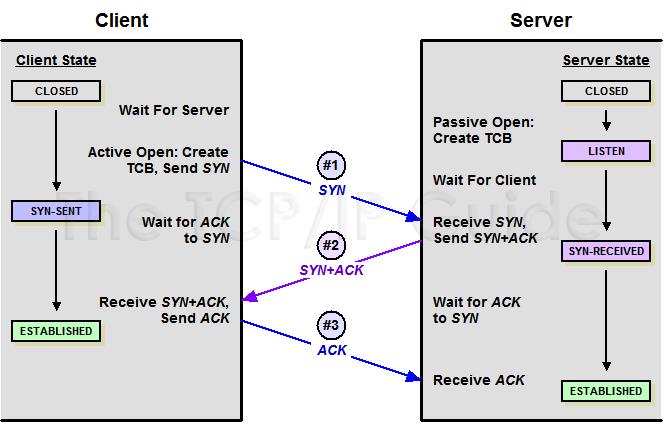


Рисунок 1.3 – Трехстороннее рукопожатие *TCP*

После инициализации соединения полезная нагрузка будет перемещаться в обоих направлениях *TCP*-соединения. Все пакеты в обязательном порядке будут содержать установленный флаг *ACK*. Другие флаги, такие как, например, *PSH* или *URG*, могут быть, а могут и не быть установленными.

При нормальном завершении *TCP*-соединения в большинстве случаев инициализируется процедура, называемая двухсторонним рукопожатием, в ходе которой каждая сторона закрывает свой конец виртуального канала и освобождает все задействованные ресурсы (см. рисунок 1.4). Обычно эта фаза начинается с того, что один из задействованных процессов приложения сигнализирует своему уровню *TCP*, что сеанс связи больше не нужен. Со стороны этого устройства отправляется сообщение с установленным флагом *FIN* (отметим, что этот пакет не обязательно должен быть пустым, он также может содержать полезную нагрузку), чтобы сообщить другому устройству о своем желании завершить открытое соединение. Затем получение этого сообщения подтверждается (сообщение от отвечающего устройства с установленным флагом *ACK*, говорящем о получении сообщения *FIN*). Когда отвечающее устройство готово, оно также отправляет сообщение с установленным флагом *FIN*, и, после получения в ответ подтверждающего получение сообщения с установленным флагом *ACK* или ожидания определенного периода времени, предусмотренного для получения *ACK*, сеанс полностью закрывается.

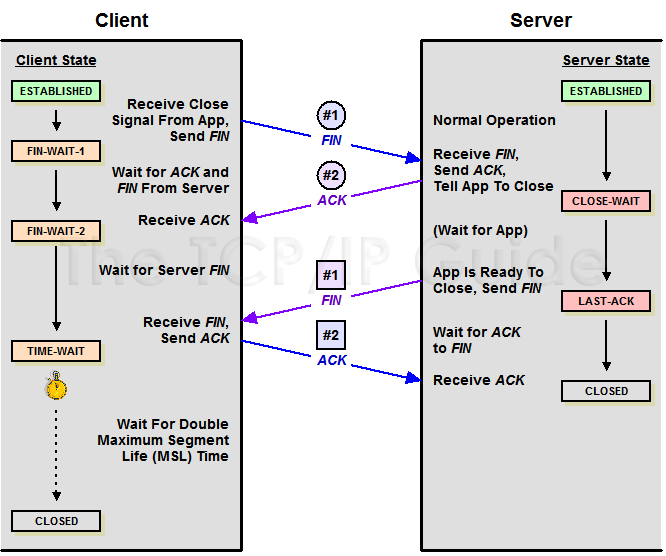


Рисунок 1.4 – Завершение *TCP*-соединения

# 2 РЕЗУЛЬТАТ ВЫПОЛНЕНИЯ ПРОГРАММЫ

В качестве атак на *TCP*-протокол были выбраны атака *TCP reset* вслепую и *SYN Flood*.

Если атакующий имеет возможность перехвата трафика, которым обмениваются его жертвы, то может считывать порядковые и подтверждающие номера *TCP*-пакетов жертв. Он может использовать эту информацию для того, чтобы выбирать, какие порядковые номера давать своим фальшивым сегментам *RST*. Однако если атакующий не может перехватывать трафик жертв, то не будет знать, какие порядковые номера вставлять. Но он всё равно может передавать любое количество сегментов *RST* с любым количеством разных порядковых номеров, надеясь, что один из них окажется верным. Такая атака называется атакой *TCP reset* вслепую. В первоначальной версии протокола *TCP* атакующему достаточно было только подобрать порядковый номер *RST* в пределах *TCP*-окна получателя. Это слишком упрощало успешные атаки вслепую, так как для почти гарантированного успеха атакующему достаточно было просто отправить несколько десятков тысяч сегментов. Чтобы противостоять этому, правило, заставлявшее получателя принимать сегмент *RST*, заменили на строгий критерий. Благодаря новым правилам для осуществления атак *TCP reset* вслепую нужно отправлять миллионы сегментов, что делает их практически нереализуемыми.

Атака *SYN Flood* реализуется следующим образом. Клиент генерирует *SYN*-пакет, запрашивая новую сессию у сервера. Поскольку *TCP*-сессия открыта (алгоритм «трехэтапного рукопожатия *TCP*» исполнен), хост будет отслеживать и обрабатывать каждую пользовательскую сессию, пока она не будет закрыта. Во время *SYN Flood* атакуемый сервер с большой скоростью получает поддельные SYN-запросы, содержащие поддельный *IP*-адрес источника. *SYN Flood* поражает сервер, занимая всю память таблицы соединений, обычно используемую для хранения и обработки входящих пакетов. Это вызывает критическое падение производительности и, как итог, отказ в работе сервера.

На рисунке 2.1 представлен корректный результат работы программы, если хакер не атакует соединение.

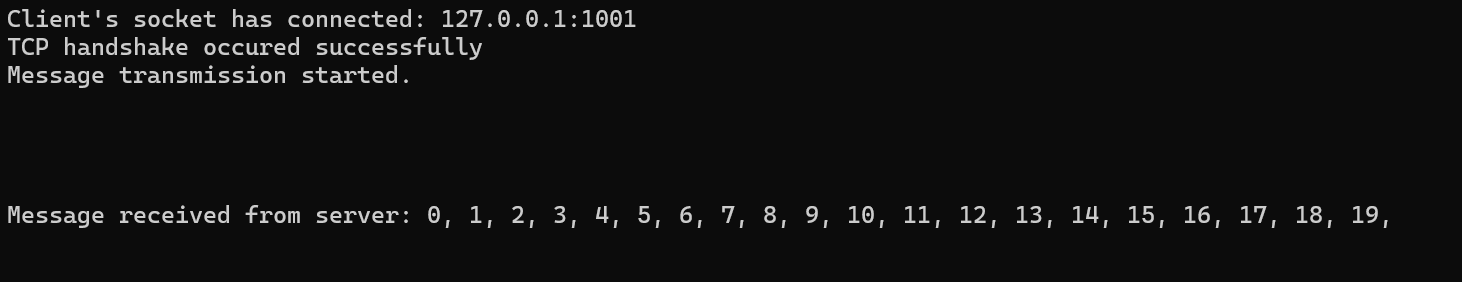


Рисунок 2.1 – Корректный результат программы

На рисунке 2.2 представлен результат программы, когда хакер реализует атаку *TCP* *reset*. Соответственно, хакер отправил пакет с установленным флагом *RST* и измененными портами, чтоб сервер разорвал соединение с клиентом.

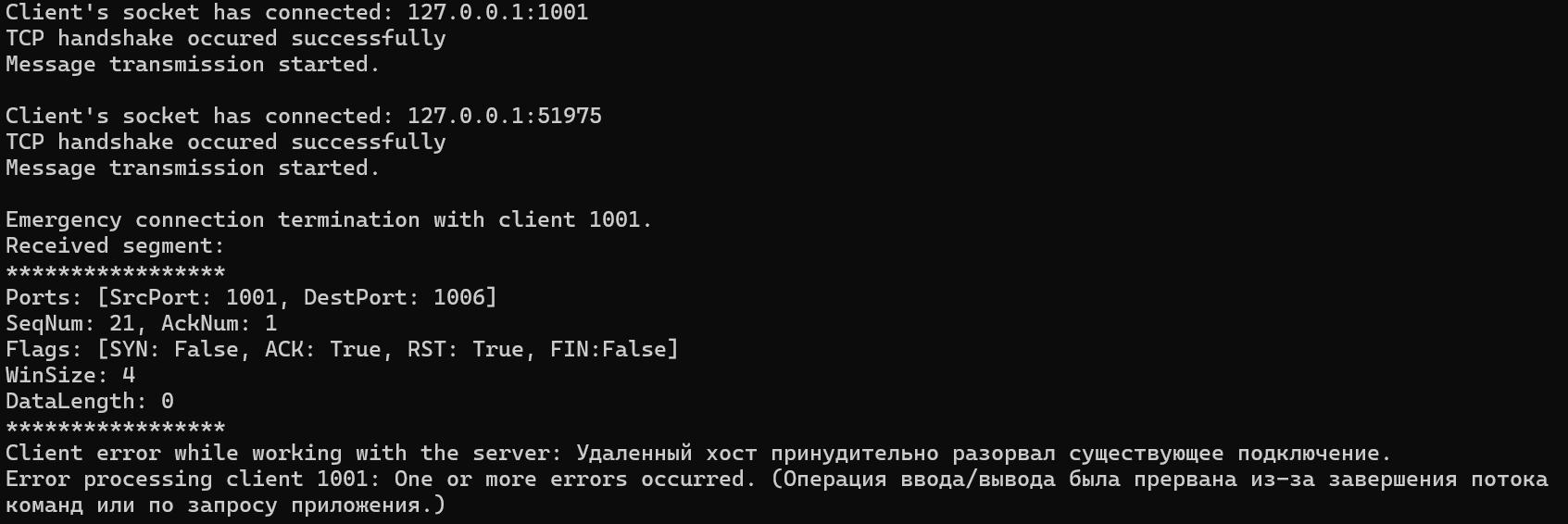


Рисунок 2.2 – Атака *TCP reset*

На рисунке 2.3 представлен результат программы, когда хакер реализует атаку *TCP reset*. Соответственно, хакер параллельно отправляет несколько запросов с флагом *SYN*, но не подтверждает дальнейшего подключения. Т. к. у сервера установлено максимальное время ожидания ответа, то по истечению этого времени сервер разрывает соединение.

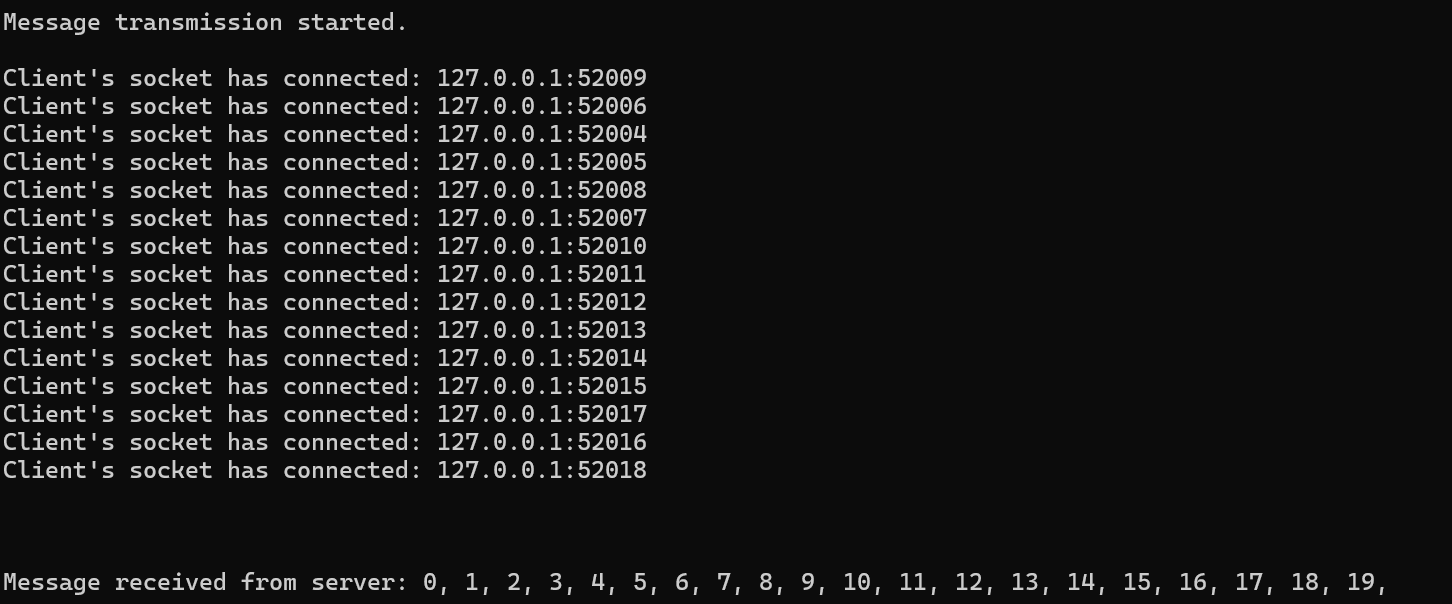


Рисунок 2.3 – Результат атаки *SYN Flood*

# ПРИЛОЖЕНИЕ А

**(обязательное)**

**Исходный код программы**

NetworkSegment.cs

namespace Lab3

{

public class NetworkSegment