Министерство образования Республики Беларусь

Учреждение образования «Белорусский государственный университет   
информатики и радиоэлектроники»

Факультет компьютерных систем и сетей

Кафедра информатики

Дисциплина: Информационные сети. Основы безопасности

ОТЧЁТ

к лабораторной работе №4

на тему

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

Выполнил: студент гр.253504

Фроленко К.Ю.

Проверил: ассистент кафедры информатики Герчик А.В.

Минск 2025

СОДЕРЖАНИЕ

[ВВЕДЕНИЕ 3](#_Toc190686916)

[1 ФОРМУЛИРОВКА ЗАДАЧИ 4](#_Toc190686917)

[2 ПРИМЕР ВЫПОЛНЕНИЯ ПРОГРАММЫ 5](#_Toc190686918)

[ЗАКЛЮЧЕНИЕ 7](#_Toc190686919)

ВВЕДЕНИЕ

В современных распределённых системах обеспечение безопасности обмена данными является одной из ключевых задач. С ростом количества кибератак защита серверных приложений становится всё более актуальной. В данной работе разработано серверное приложение, способное не только устанавливать защищённое соединение с клиентами посредством специального механизма handshake, но и эффективно противостоять различным видам атак. Программа предназначена для демонстрации базовых принципов защиты, применяемых для фильтрации подозрительных соединений и предотвращения атак типа ACK Flood, Slowloris и SYN Flood.

В работе подробно рассматриваются этапы установления защищённого соединения: от генерации уникального токена сервером до проверки корректности ответа от клиента. Дополнительно реализованы механизмы обнаружения аномальной активности, позволяющие своевременно разрывать соединения с клиентами, пытающимися перегрузить сервер или использовать уязвимости в процедуре handshake. Такая архитектура позволяет повысить надёжность работы приложения и снизить риск несанкционированного доступа.

Также следует отметить, что выбранный подход демонстрирует возможности простых методов защиты, которые могут быть использованы в реальных приложениях для повышения устойчивости серверной инфраструктуры к кибератакам. Программа служит хорошей иллюстрацией того, как можно объединить проверку подлинности и мониторинг активности для создания защищённого сервера.

1 ФОРМУЛИРОВКА ЗАДАЧИ

Цель работы состоит в разработке серверного приложения, которое обеспечивает установление защищённого соединения с клиентами посредством механизма handshake и реализует защитные меры для противодействия сетевым атакам.

Задача включает в себя следующие основные аспекты:

1 **Установление защищённого соединения.** При каждом новом подключении сервер генерирует уникальный токен и отправляет его клиенту в виде сообщения CHALLENGE. Клиент должен корректно ответить, отправив соответствующее сообщение RESPONSE с полученным токеном. При совпадении токенов соединение считается успешно установленным, и клиент получает доступ к дальнейшему функционалу сервера.

2 **Обнаружение аномальной активности.** Приложение должно отслеживать поведение клиентов на предмет подозрительной активности. Если клиент отправляет слишком большое количество команд ACK за короткий период времени (ACK Flood), если передача данных замедляется до уровня, приводящего к истечению таймаута (Slowloris), или если наблюдается массовое создание незавершённых handshake (SYN Flood), сервер должен немедленно разорвать соединение.

3 **Защита от атак.** Встроенные в сервер защитные механизмы позволят обнаруживать и блокировать атаки на ранней стадии, предотвращая возможное истощение ресурсов системы. Это достигается за счёт ограничения количества незавершённых соединений, контроля времени отклика клиента и анализа количества отправляемых команд.

Таким образом, итоговое решение должно обеспечить корректное установление защищённого соединения с клиентом, а также демонстрировать эффективность реализованных защитных механизмов при попытках проведения атак.

2 ПРИМЕР ВЫПОЛНЕНИЯ ПРОГРАММЫ

В данной главе представлена практическая демонстрация работы серверного приложения. Описаны ключевые этапы его функционирования, а также проиллюстрированы результаты тестирования защитных механизмов. При запуске серверного приложения в консоли выводятся отладочные сообщения, информирующие о каждом этапе работы. После старта сервер начинает ожидать входящих подключений.

При корректном выполнении процедуры handshake клиент получает сообщение **HANDSHAKE SUCCESS**, после чего сервер отправляет приветственное сообщение с перечнем доступных команд (например, PING, ACK, quit). Результаты успешного соединения можно увидеть **на рисунке 1.**

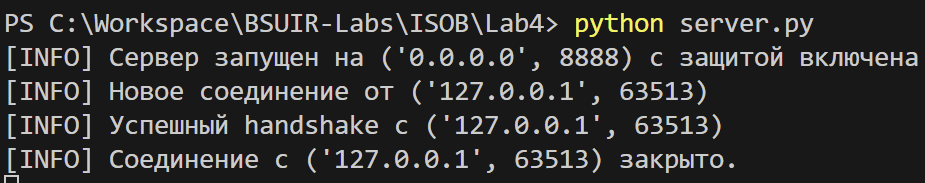


Рисунок 1 – Пример успешного соединения с сервером

На данном скриншоте из консоли показано, как клиент успешно проходит процедуру handshake: сервер отправляет сообщение **CHALLENGE**, клиент отвечает корректным сообщением **RESPONSE**, и сервер выводит сообщение **HANDSHAKE SUCCESS,** подтверждая установление защищённого соединения.

При моделировании ACK Flood атаки клиент за короткий промежуток времени отправляет множество команд **ACK**. Сервер, обнаружив превышение порога (ACK\_THRESHOLD), фиксирует аномалию и немедленно разрывает соединение. Результаты работы защитного механизма продемонстрированы на **рисунке 2.**

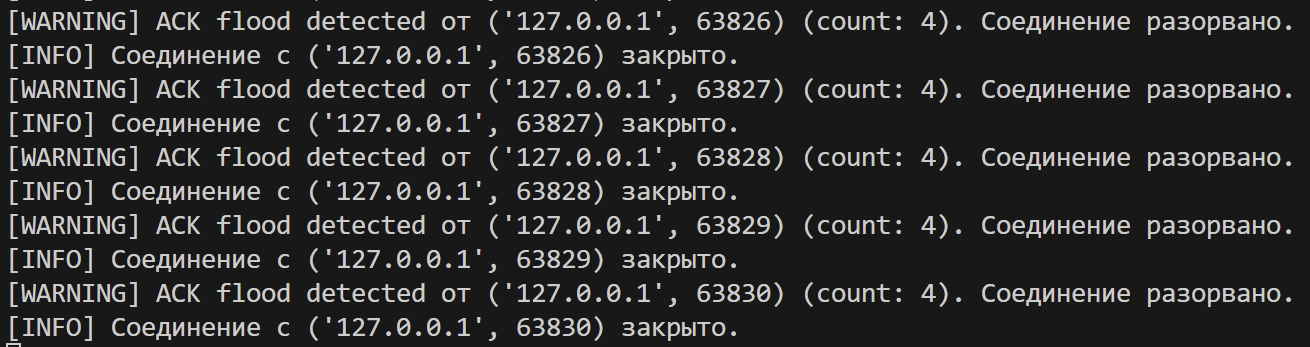


Рисунок 2 – Сценарий ACK Flood атаки

На данном скриншоте виден вывод отладочных сообщений, свидетельствующий о том, что сервер обнаружил избыточное количество команд **ACK** и принял решение разорвать соединение.

При моделировании Slowloris атаки клиент намеренно замедляет передачу ответа на **CHALLENGE**, отправляя данные по одному символу с большими интервалами. В результате истекает таймаут, и сервер завершает процедуру handshake. Результаты данного сценария можно увидеть **на рисунке 3.**

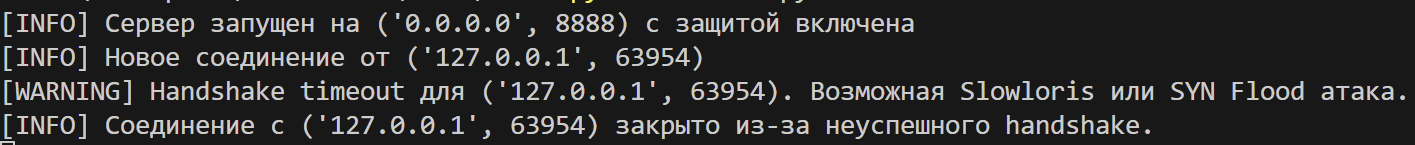


Рисунок 3 – Сценарий Slowloris атаки

Этот скриншот иллюстрирует, как истекает таймаут соединения из-за замедленной передачи данных. Сервер фиксирует превышение времени ожидания и завершает handshake, предотвращая возможность проведения атаки.

При моделировании SYN Flood атаки происходит массовое создание незавершённых handshake. Ограничение на количество таких соединений (MAX\_HALF\_OPEN\_CONNECTIONS) позволяет серверу обнаружить атаку и отклонить новые подключения. Вывод отладочных сообщений свидетельствует о том, что сервер блокирует входящие соединения при превышении допустимого лимита на рисунке 4.

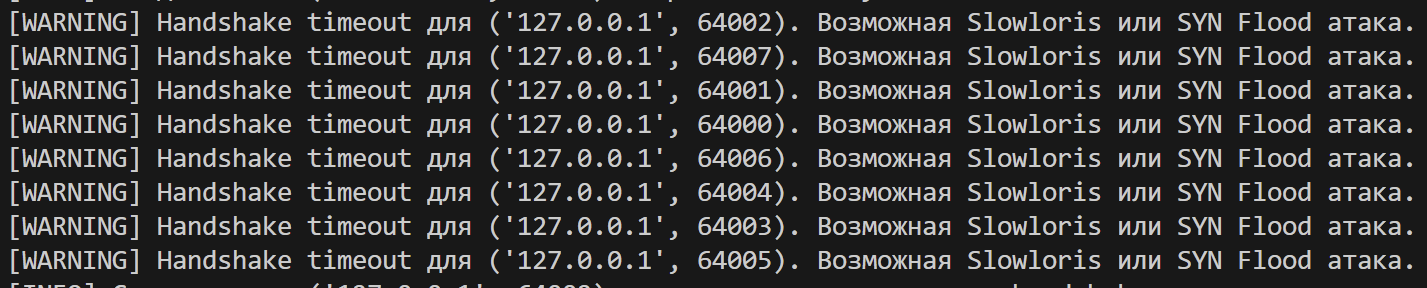


Рисунок 4 – Сценарий SYN Flood атаки

На данном скриншоте отображён вывод, подтверждающий, что сервер обнаружил чрезмерное количество незавершённых handshake и отказал в установлении новых соединений.

В результате тестирования было установлено, что при корректном поведении клиента сервер успешно устанавливает защищённое соединение и позволяет выполнять команды, а при обнаружении аномальной активности защитные механизмы срабатывают оперативно и без задержек.

# ЗАКЛЮЧЕНИЕ

В данной работе разработано серверное приложение, демонстрирующее возможность установления защищённого соединения с клиентом посредством механизма handshake и эффективной защиты от сетевых атак. Реализованная система успешно обеспечивает проверку подлинности клиента, генерируя уникальные токены и контролируя корректность его ответов. Дополнительно встроенные механизмы обнаружения атак типа ACK Flood, Slowloris и SYN Flood позволяют оперативно разрывать подозрительные соединения, что значительно повышает надёжность работы сервера.

Проведённое экспериментальное исследование показало, что при нормальной работе сервера клиенты получают доступ к функционалу, а попытки злоупотребления ресурсами приводят к немедленному разрыву соединения. Таким образом, предложенное решение демонстрирует практическую применимость простых, но эффективных методов защиты серверных приложений в условиях современных угроз.