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.253505 Сенько Н. С.

Проверил: ассистент кафедры информатики
Герчик А.В.

Минск 2025

СОДЕРЖАНИЕ

1 ЦЕЛЬ РАБОТЫ

Цель данной работы — исследовать и применить на практике методы защиты сервера от наиболее распространённых атак на этапе установления TCP-соединения.

В ходе исследования были рассмотрены методы противодействия таким атакам, как SYN Flood, ACK Flood и Slowloris. Для этого были использованы механизмы ограничения полузакрытых соединений, токены для подтверждения рукопожатия и мониторинг активности клиента.

В результате был создан сервер на базе asyncio, который способен эффективно защищаться от различных типов атак. Защита включает в себя ограничение количества полузакрытых соединений, чтобы предотвратить исчерпание ресурсов сервера во время SYN Flood атак. Также используется случайный токен для проверки клиента при установлении соединения, что затрудняет проведение автоматизированных атак. Кроме того, контролируется частота отправки ACK-сообщений с разрывом соединения при подозрительной активности.

Дополнительно реализован таймаут ожидания данных, который позволяет прерывать соединение при длительной неактивности клиента. Это снижает риск успешной Slowloris-атаки.

Разработанная система позволяет исследовать поведение сервера при различных сценариях атак, оценить эффективность внедрённых механизмов защиты и продемонстрировать важность комплексного подхода к обеспечению безопасности сетевых приложений.

2 ХОД РАБОТЫ

Ход работы начинается с запуска сервера в двух режимах: защищенном и уязвимом. В защищенном режиме включены механизмы обнаружения и предотвращения атак, тогда как в уязвимом режиме эти защиты отключены, что позволяет наглядно продемонстрировать разницу в поведении сервера под нагрузкой.

Сначала проводится тест на *SYN Flood* атаку. В уязвимом режиме сервер принимает все запросы на соединение и становится неспособным обрабатывать при их большом количестве. В защищенном режиме сервер отслеживает количество таких соединений и отклоняет новые попытки подключения при превышении лимита, фиксируя возможную атаку в логе, который вывел информацию, что он перегружен.

Затем имитируется атака *ACK Flood*. В уязвимом режиме сервер продолжает принимать и обрабатывать бесконечные *ACK*-сообщения, что приводит к исчерпанию ресурсов. В защищенном режиме сервер отслеживает частоту отправки *ACK* в определенном временном окне и разрывает соединение при превышении допустимого порога, регистрируя факт обнаружения атаки.

Последний этап – демонстрация Slowloris атаки. В уязвимом режиме сервер остается заблокированным из-за множества частично отправленных запросов, которые занимают соединения на длительное время. В защищенном режиме установлен таймаут ожидания данных, что позволяет серверу автоматически разрывать неактивные соединения и продолжать обработку новых запросов.

Таким образом, в ходе экспериментов наглядно показывается, как включенные механизмы защиты позволяют серверу устойчиво работать даже при попытках атак, в то время как без защиты сервер становится уязвимым к перегрузкам и отказу в обслуживании.

ЗАКЛЮЧЕНИЕ

В ходе лабораторной работы были исследованы и внедрены методы защиты сервера от распространённых сетевых атак на этапе установления TCP-соединения.

В процессе разработки были созданы механизмы, которые ограничивают полузакрытые соединения, подтверждают рукопожатие с использованием случайного токена, обнаруживают аномальную частоту ACK-сообщений и устанавливают таймаут ожидания данных.

Эксперименты показали, что в уязвимом режиме сервер легко подвергается атакам SYN Flood, ACK Flood и Slowloris, быстро теряя доступность из-за исчерпания ресурсов. В защищённом режиме сервер успешно обнаруживает и блокирует атаки, сохраняя работоспособность и регистрируя инциденты в журнале.

Результаты работы подтверждают важность внедрения многоуровневой защиты в сетевых приложениях для обеспечения устойчивости к атакам и поддержания стабильной работы сервиса. Реализация предложенных защитных механизмов значительно снижает риск отказа в обслуживании и повышает общую безопасность системы.