Министерство высшего образования и науки Российской Федерации

Федеральное государственное автономное образовательное учреждение высшего образования

«Санкт-Петербургский политехнический университет Петра Великого»

—

Институт кибербезопасности и защиты информации

**ЛАБОРАТОРНАЯ РАБОТА №14**

**Защита от угроз нарушения безопасности типа «Отказ в обслуживании»**

по дисциплине «Основы информационной безопасности»

Выполнил

студент гр. 4851003/10002 Лобов Е.А.

Преподаватель. Зубков Е.А.

Санкт-Петербург

2022

## **ПОСТАНОВКА ЗАДАЧИ**

Задачей данной лабораторной работы является изучение механизма реализации компьютерной угрозы типа «отказ в обслуживании», ознакомление со способами защиты от такого рода угроз.

Для достижения этих целей необходимо:

1. Изучить интерфейс и основные функции генераторов пакетов Nemesis, Colasoft Packet Builder, PACKETH, ostinato.
2. Смоделировать атаку SYN-flood на виртуальный сервер.
3. Смоделировать атаку ICMP-flood на виртуальный сервер.
4. Организовать элементы защиты от SYN-flood и ICMP-flood атак.

## **ХОД РАБОТЫ**

### **Анализ основных функций генератора пакетов**

Colasoft Packet Builder: по умолчанию поддерживает только протоколы Ethernet, ARP, IP, TCP, UDP, на основе которых с помощью встроенного редактора можно создавать пользовательские пакеты. Данная программа представлена редактором декодирования, который позволяет редактировать определенные значения поля протоколов. В дополнение к составлению пакетов ColasoftPacketBuilder также поддерживает сохранение пакетных файлов и отправку пакетов по сети. (см. Рисунок 1)

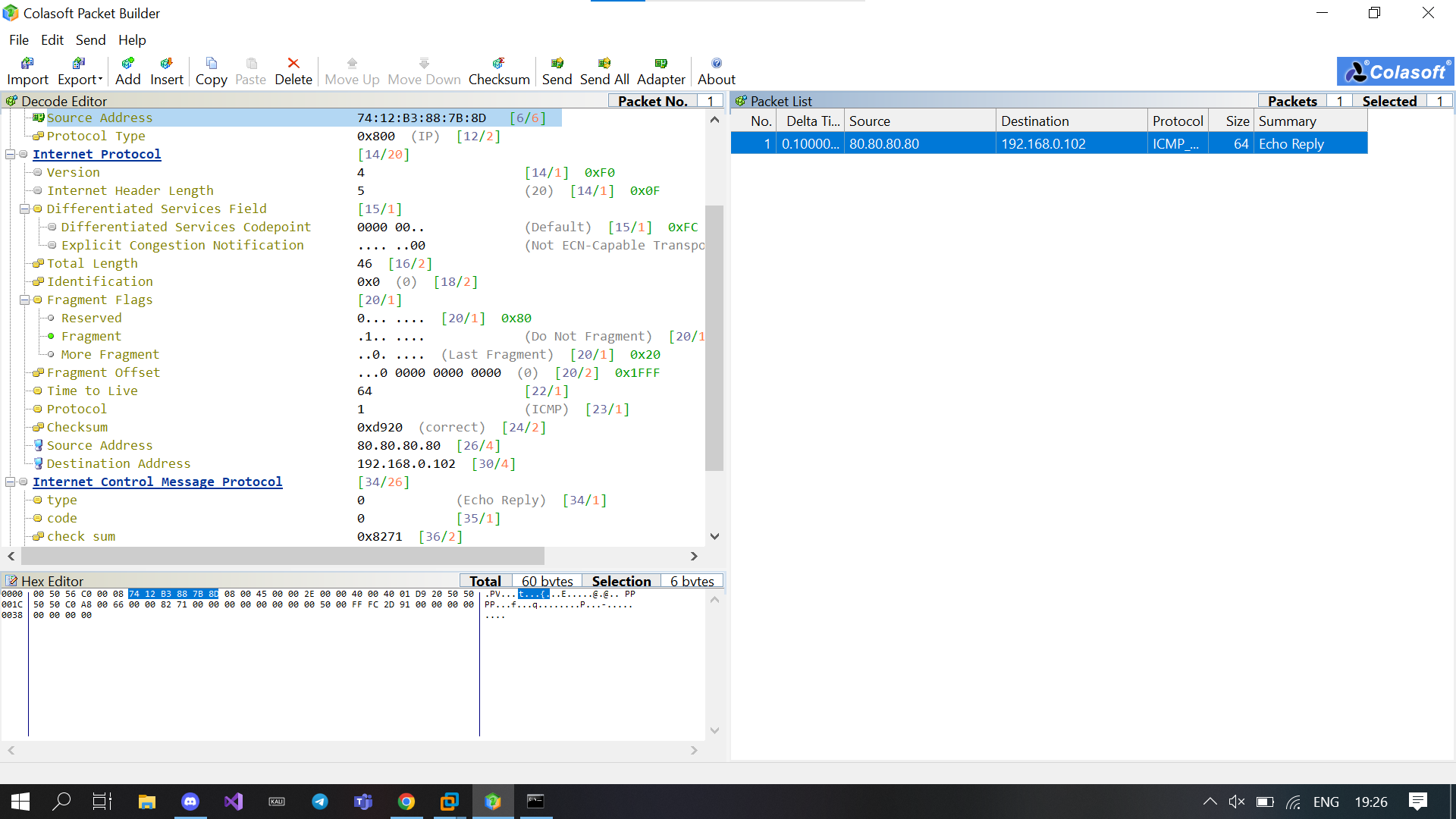


Рисунок 1 – Интерфейс Colasoft Packet Builder.

С помощью данной программы были смоделированы атаки на web-сервер Apache, установленный на виртуальную машину (ОС - Ubuntu).

### **2. Моделирование SYN-flood атаки**

Механизм данной атаки заключаются в следующем: при проведении SYN-flood атакующий компьютер непрерывно посылает сообщение с запросами на установку соединения. В пакете указывается несуществующий IP-адрес. Атакуемый узел создаёт новые динамические структуры данных и запускает таймер для каждой новой попытки соединения до тех пор, пока не исчерпает свои ресурсы. Поле этого атакуемый компьютер перестаёт отвечать на попытки подключения.

Моделирование атаки было начато с изучения конфигурации сети, в частности требовалось узнать IP-адрес, на который будут посылаться пакеты.

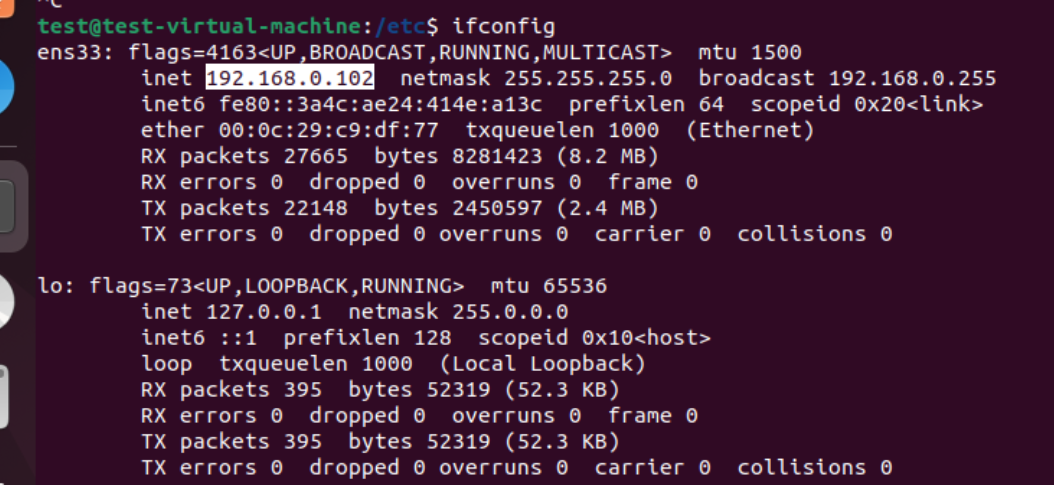
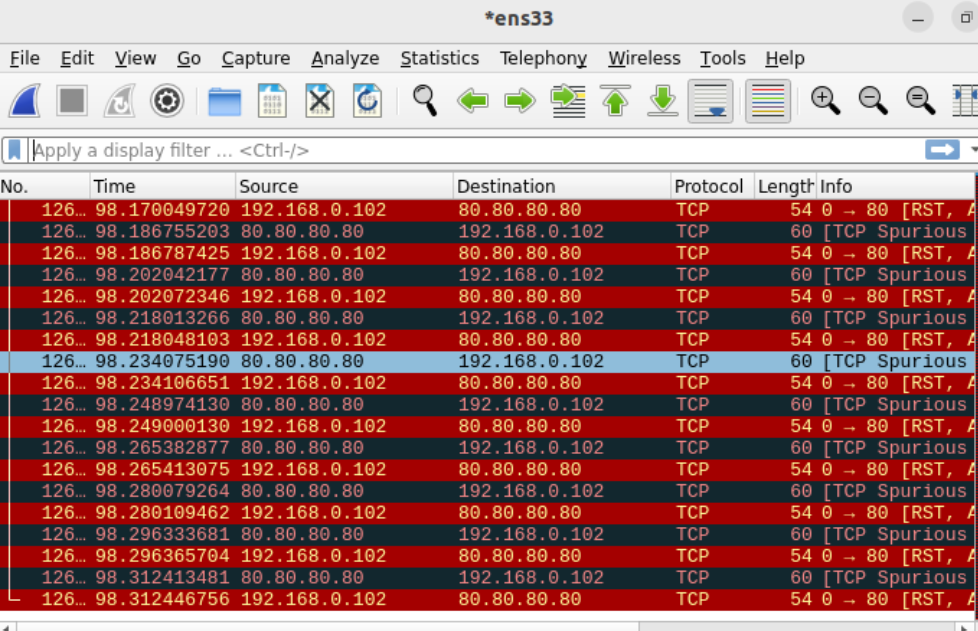


Рисунок 2 – Выявление IP-адреса для атаки.

На полученный 80-й порт действующего IP-адреса отправлялись пакеты с несуществующими IP-адресами источника, портом источника 1.2.3.1 (случайное число) и с установленным флагом SYN. На Рисунке 3 видно, что пакеты успешно доходили до сервера, после чего происходила неудачная попытка отправки ответного пакета на несуществующие IP-адреса. Количество запросов и время между ними задавалось в генераторе пакетов.

* Рисунок 3 – SYN-flood атака с позиции атакуемой машины.

### **3. Моделирование ICMP-flood атаки**

При ICMP-flood на узел жертвы отправляется эхо-запрос, который требуется обработать и отправить эхо-ответ, при этом необходимо будет задействовать большие ресурсы по сравнению с обычным пакетом, хотя сам запрос по объему небольшой. В результате при относительно небольшом трафике можно добиться перегрузки по количеству пакетов.

Для моделирования ICMP-flood атаки в исходном генераторе с пакетом TCP была проведена замена номера протокола на 1, тем самым был получен ICMP-пакет. Далее была произведена отправка таких пакетов с интервалом в 100 мс

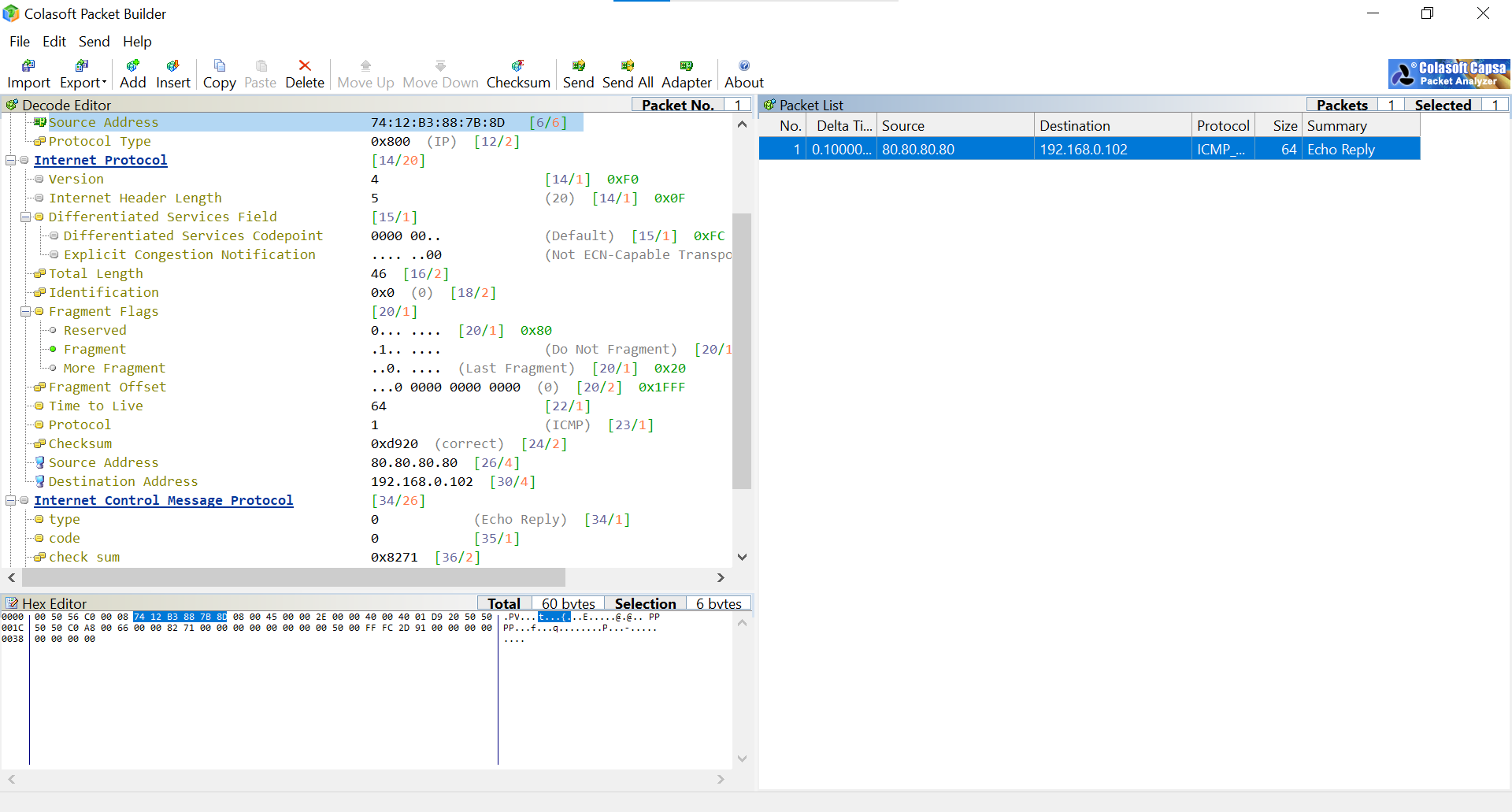


Рисунок 4 – Параметры ICMP пакета.

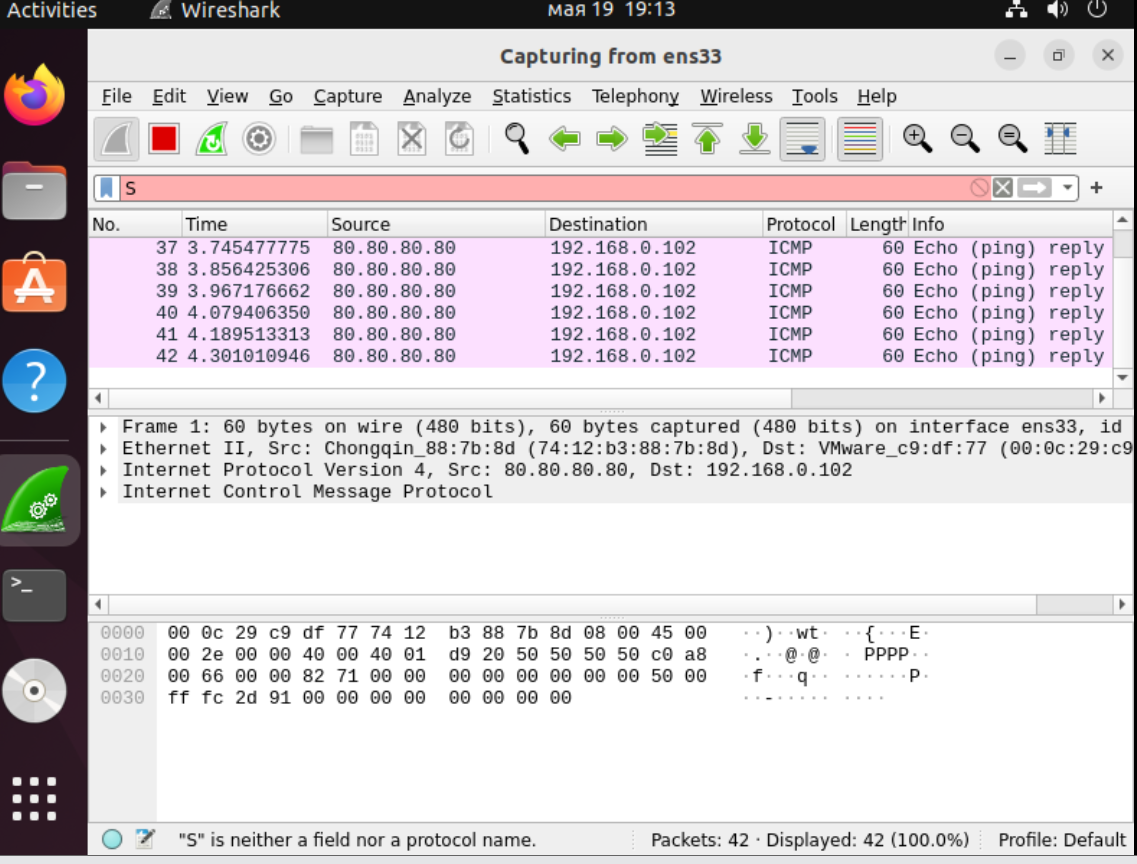
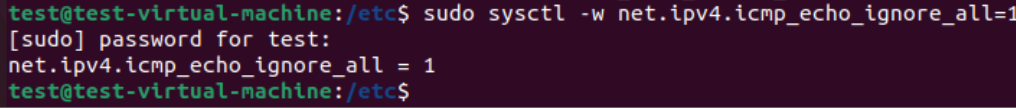


Рисунок 5 – Данные из Wireshark.

### **4. Организация элементов защиты от атак**

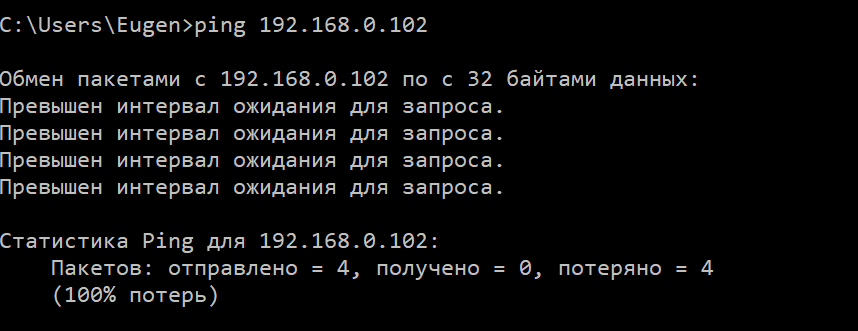
Для защиты от ICMP-flood необходимо отключать ответы на запросы ICMP echo:

sysctl -w net.ipv4.icmp\_echo\_ignore\_all=1 .



С помощью правил межсетевого экрана это можно реализовать следующим образом

iptables –A INPUT –p icmp –j DROP --icmp-type 8 .



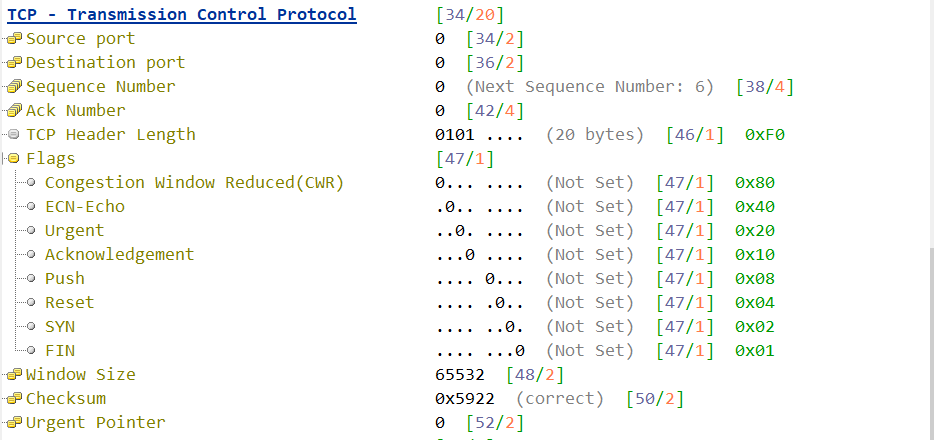
## **ВЫВОДЫ**

В ходе данной работы были изучены механизмы реализаций компьютерных угроз типа «отказ в обслуживании», были приобретены базовые навыки защиты от такого рода угроз.

На практике изучены и смоделированы DoS-атаки типов SYN-flood и ICMP-flood, приводящие к отказу в обслуживании сервера, либо к снижению его пропускной способности. Настройки сервера были изменены таким образом, чтобы он имел простую защиту от подобных атак.

# Ответы на вопросы

**Transmission Control Protocol** (TCP, протокол управления передачей) — один из основных протоколов передачи данных интернета. Предназначен для управления передачей данных интернета. Пакеты в TCP называются *сегментами***.**

****

Порты источника и назначения.

**Sequence number** (32 бита) — измеряется в байтах, и каждый переданный байт полезных данных (payload) увеличивает это значение на 1.

Если установлен флаг SYN (идёт установление сессии), то поле содержит изначальный порядковый номер — ISN (Initial Sequence Number). В целях безопасности это значение генерируется случайным образом и может быть равно от 0 до 232−1 (4294967295). Первый байт полезных данных в устанавливающейся сессии будет иметь номер ISN+1.

В противном случае, если SYN не установлен, первый байт данных, передаваемый в данном пакете, имеет этот порядковый номер.

**Acknowledgment Number (ACK SN)** (32 бита) — если установлен флаг ACK, то это поле содержит порядковый номер октета, который отправитель данного сегмента желает получить. Это означает, что все предыдущие октеты (с номерами от ISN+1 до ACK-1 включительно) были успешно получены.

Каждая сторона подсчитывает свой Sequence number для переданных данных и отдельно Acknowledgement number для полученных данных. Sequence number каждой из сторон соответствует Acknowledgement number другой стороны.

Длина заголовка (Data offset) занимает 4 бита и указывает значение длины заголовка, измеренное в 32-битовых словах. Минимальный размер составляет 20 байт (пять 32-битовых слов), а максимальный — 60 байт (пятнадцать 32-битовых слов). Длина заголовка определяет смещение полезных данных относительно начала сегмента. Например, Data offset равное 11112 говорит о том, что заголовок занимает пятнадцать 32-битных слова (15 строк\*32 бита в каждой строке/8 бит = 60 байт).

Это поле содержит 9 битовых флагов:

* **NS** (ECN-nonce)
* **CWR**
* **ECE** (ECN-Echo)

Флаги относящиеся к защитному механизму ECN-nonce, обеспечивающему защиту от сокрытия пакетов TCP.

* **URG** — поле *«Указатель важности»* .Когда узел отправляет сегмент с URG флагом, то узел-получатель принимает его на отдельном канале.
* **ACK** — поле *«Номер подтверждения»* задействовано .
* **PSH** — инструктирует получателя протолкнуть данные, накопившиеся в приемном буфере, в приложение пользователя. API для установки PSH флага нет. Обычно он устанавливается ядром, когда оно очищает буфер. Дело в том, что когда узел отправляет информацию, TCP сохраняет её в буфере и не передает её сразу другому узлу, ожидая, захочет ли узел-отправитель передать ещё. Такая же схема работает и у узла-получателя. Когда он получает информацию, TCP сохраняет её в буфере, чтобы не тревожить приложение из-за каждого байта полученной информации. Если узел отправляет сегмент с PSH флагом, это значит, что он отправил все, что было нужно.
* **RST** — оборвать соединения, сбросить буфер (очистка буфера)
* **SYN** — синхронизация номеров последовательности
* **FIN** — флаг, будучи установлен, указывает на завершение соединения