1. Министерство образования и науки Российской Федерации
2. Санкт-Петербургский Политехнический Университет Петра Великого
3. —
4. **Институт компьютерных наук и кибербезопасности**

**ЛАБОРАТОРНАЯ РАБОТА № 14**

1. «Защита от угроз нарушения безопасности типа “Отказ в обслуживании”»
2. по дисциплине «Основы информационной безопасности»
3. Выполнил
4. студент гр. 5131001/30003 Шевчук Н.Е.

1. Руководитель
2. асс. преподавателя Орел Е.М.

Санкт-Петербург

2024

[1. Цель работы 3](#_Toc164757736)

[2. Формулировка задания 3](#_Toc164757737)

[3. Теоретическая справка 3](#_Toc164757738)

[3. Генераторы пакетов 5](#_Toc164757739)

[4. Ход работы 6](#_Toc164757740)

[5.1. Моделирование SYN-flood атаки 8](#_Toc164757741)

[5.2. Моделирование ICMP-flood атаки 10](#_Toc164757742)

[5.3. Защита от SYN-flood атаки 11](#_Toc164757743)

[5.4. Защита от ICMP-flood атаки 12](#_Toc164757744)

[6. Результаты работы 13](#_Toc164757745)

[7. Вывод 13](#_Toc164757746)

[8. Ответы на контрольные вопросы 13](#_Toc164757747)

# 1. Цель работы

Изучить механизм реализации компьютерной угрозы типа “отказ в обслуживании” и ознакомиться со способами защиты от такого вида угроз.

# 2. Формулировка задания

1. Смоделировать SYN-flood и ICMP-flood атаки на виртуальный сервер. Описать механизм смоделированной атаки и оценить количество запросов, время между запросами, скорость поступления запросов.
2. Организовать элементы защиты от SYN-flood и ICMP-flood. Сравнить результаты атак этого и предыдущего пунктов.

# 3. Теоретическая справка

Компьютерные угрозы типа “отказ в обслуживании” (Denial-of-service, DoS) – класс угроз, направленных на вычислительную систему, целью которых является препятствование возможности легального пользователя получить доступ к работающей системе из-за множества обращений, которые генерируются злоумышленником.

DoS-атаки возможны по нескольким причинам, связанным с ограниченностью вычислительных и информационных ресурсов: например, с ограниченной пропускной способностью каналов связи, ограниченной производительностью сетевого оборудования и серверов, которые не в состоянии обрабатывать огромное число одновременно поступающих запросов ("шквал запросов").

В настоящее время вычислительные мощности нападающей стороны практически не ограничены (например, используются бот-сети, высокопроизводительные вычислительные системы), поэтому мощность DoS-атак также значительно возросла: они стали распределенными и интеллектуальными.

Рассмотрим обобщенный сценарий реализации DoS-атаки.

Информация в сети передается пакетами. Структура пакета включает в себя адрес отправителя, адрес получателя, порт отправителя и порт получателя, а также другие служебные данные. Пакеты могут быть фрагментированы, то есть один пакет может быть разбит на несколько частей. Информация о фрагментации добавляется к служебной, чтобы компьютер получателя мог собрать фрагменты в пакет.

Наиболее распространены три типа сетевых пакетов:

* *TCP пакет* - тип пакета, надежного при передаче, поскольку компьютер получателя отправляет уведомление о получении пакета. Если уведомление не получено, пакет посылается повторно. В данном случае потеря информации исключается. Недостаток использования ТСР-пакетов - замедление передачи по причине пересылки уведомлений;
* UDP-пакет - тип пакета, не предусматривающего уведомлений о его получении, следовательно, допускающий потери информации;
* IСМР-пакет - тип пакета, предназначенного для служебных задач (например, для диагностики сети, выполнения ping) и не используемого для передачи информации.

DoS-атаки основаны на идее флуда (flood), то есть "затопления" жертвы огромным количеством пакетов.

Рассмотрим пример флуда с помощью ТСР-пакета. Перед началом обмена данными протокол ТСР устанавливает соединение методом трехэтапного подтверждения. Флаг SYN обозначает начало запроса на установку соединения. Флаг АСК обозначает подтверждение о получении пакета. Флаг FIN предназначен для разрыва соединения после завершения передачи. Метод трехэтапного подтверждения установки соединения заключается в простом обмене пакетами.

Предположим, что в первом пакете с запросом на установку соединения, пришедшим от узла А, указан неверный IР-адрес. В таком случае подтверждение от узла В не вернется к узлу А. Узел В, не дождавшись ответа в заданный временной промежуток, должен освободить память, выделяемую для поддержания соединения. Указанная особенность используется для DoS-атаки SYN-flood.

При проведении SYN-flood, атакующий компьютер непрерывно посылает сообщение с запросами на установку соединения. В пакете указывается несуществующий Р-адрес. Атакуемый узел создает новые динамические структуры данных и запускает таймер для каждой новой попытки соединения до тех пор, пока не исчерпает свои ресурсы. После этого атакуемый компьютер перестает отвечать на попытки подключения.

Принцип атаки ICMP-flood схож с SYN-flood, но атакуемый компьютер "забрасывается" пакетами типа ІСМР. Поскольку система должна ответить на такой пакет, это приводит к созданию большого количество ответных пакетов, и, как следствие, к снижению пропускной способности канала.

# Генераторы пакетов

Ниже изложены основные функции некоторых генераторов пакетов:

* + *“Nemesis”* – это утилита для создания и внедрения сетевых пакетов (ARP, DNS, ETHERNET, ICMP, IP, OSPF, RIP, TCP, UPD). Данная программа хорошо подходит для тестирования сетевых систем обнаружения вторжений, брандмауэров, стеков IP.
  + *“Colasoft Packet Builder”* – программа, которая позволяет создавать пользовательские сетевые пакеты (ETHERNET, APR, IP, TCP, UPD), а также изменить параметры в редакторе декодера, шестнадцатеричном редакторе или редакторе ASCII для создания пакетов. Программа поддерживает сохранение пакетов и их отправку в сеть. Данная программа позволяет очень гибко настраивать параметры пакетов. Также программа обладает отзывчивым и понятным интерфейсом.
  + *“PACKETH”* – инструмент для создания пакетов GUI и CLI для ETHERNET, позволяющий создавать и отправлять любой возможный пакет или последовательность пакетов по каналу Ethernet.
  + *“Ostinato”* – универсальный обработчик пакетов и генератор трафика с интуитивно понятным графическим интерфейсом, позволяющий создавать и отправлять пакеты различных протоколов, изменять любое значение, отправлять трафик с требуемой скоростью, выбирать размер трафика, а также отправлять несколько потоков трафика – последовательно и вместе.

# Ход работы

Для реализации DoS-атаки необходимо создать виртуальный сервер, который будет атакован. Для этого на систему виртуальной машины устанавливается сервер Apache. Кроме того, на атакуемую ЭВМ устанавливается программа “Wireshark” для анализа трафика. Она является инструментом для захвата и анализа сетевого трафика для большинства известных протоколов.

*apt install apache2*

*apt update*

*ufw app list*

*ufw allow 'Apache'*

*ufw enable*

*systemctl status apache2*

*add-apt-repository universe*

*apt install wireshark*

*apt update*

*dpkg-reconfigure wireshark-common*

*chmod +x /usr/bin/dumpcap*



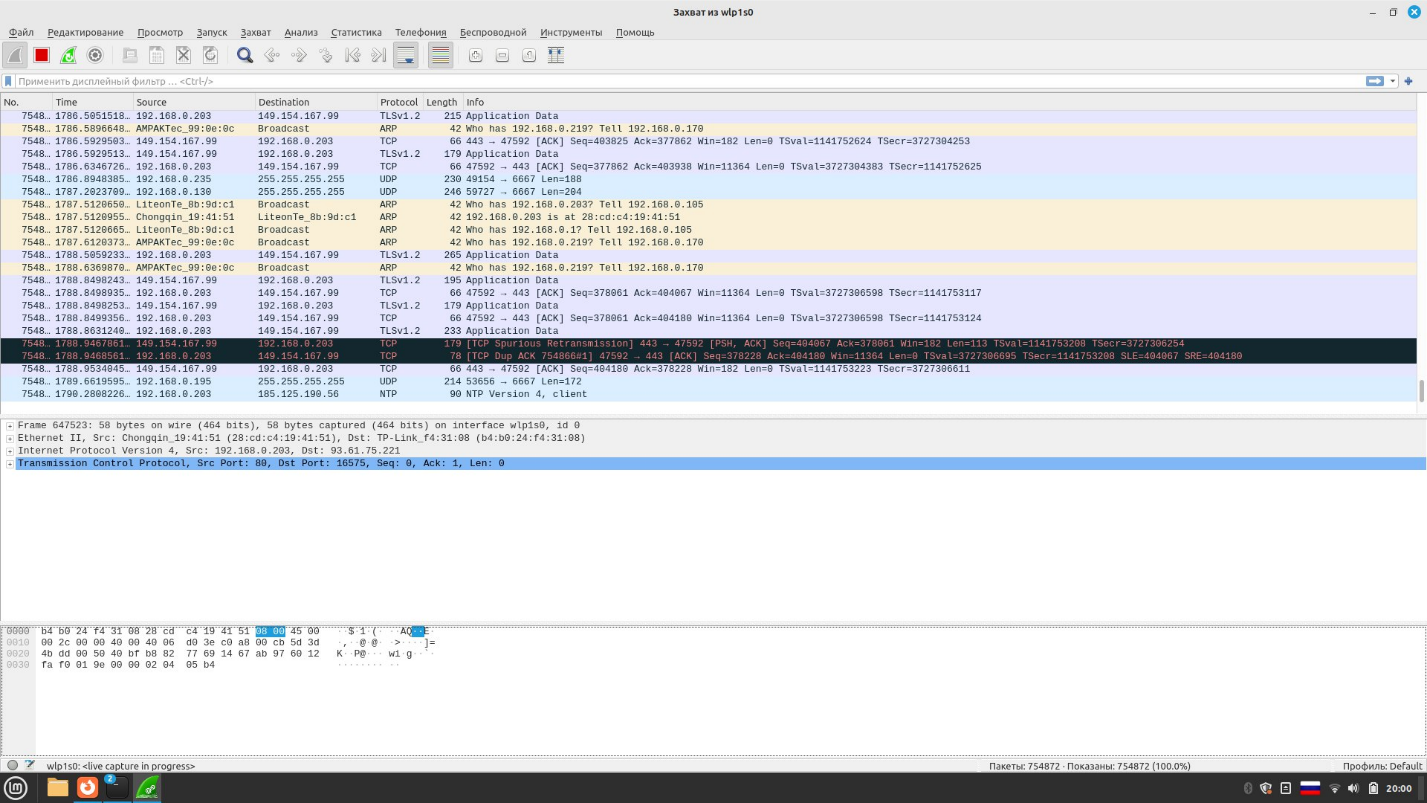
Рис.1. Сервер Apache

Рис.2. Окно Wireshark до начала атаки

На атакующую виртуальную машину был установлен генератор пакетов hping3.

*apt install hping3*

## Моделирование SYN-flood атаки



Рис.1 (реализация SYN-flood атаки).

Составляющие команды:

* -с 1500 - отправляем 15000 пакетов/сек;
* -d 120 – размер пакетов 120 байт (максимально возможный);
* -S – включен флаг SYN;
* -w 64 – размер TCP-окна имеет значение 64
* -p 80 – порт 80
* --flood – для максимально быстрой отправки пакетов;
* --rand-source - используется для генерирования поддельных IP-адресов, чтобы замаскировать реальный источник и избежать обнаружения

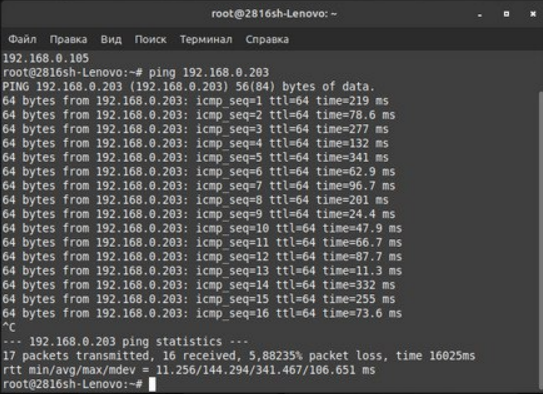
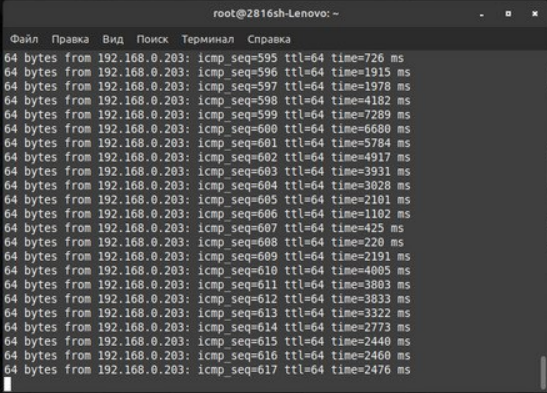
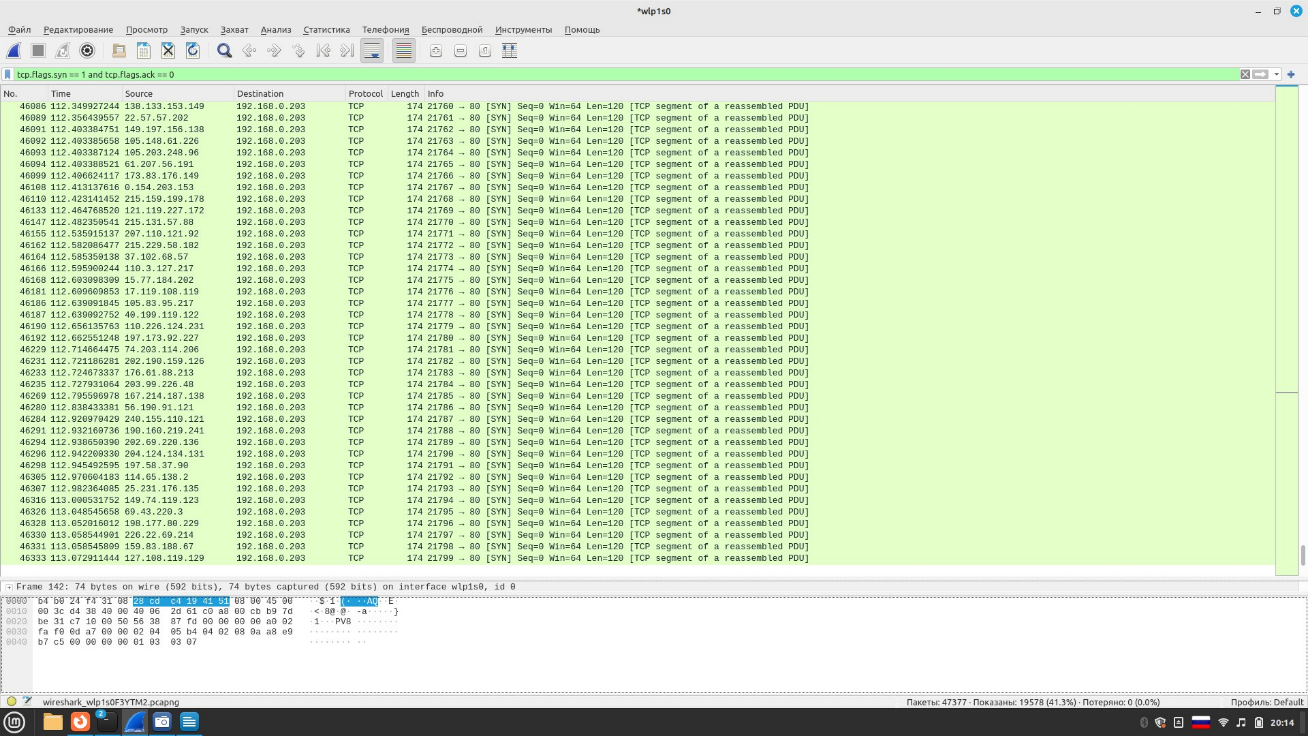
С помощью команды *ping* с устройства-клиент будем отслеживать задержку получения пакетов по времени во время атаки:

Рис.3. Время получения пакетов до начала атаки

Рис.4. Время задержки получения пакетов во время атаки

Видно, что в некоторых случаях время увеличилось в 10-100 раз.

Отследить SYN-flood атаку достаточно просто, поставив фильтры в программе анализа трафика. Основным признаком этой атаки является огромное количество пакетов с флагом SYN, получаемых атакуемым сервером. Следует отфильтровать трафик по полученным пакетам с установленным флагом SYN без последующего подтверждения (получения пакетов с установленным флагом ACK), используя следующий фильтр: «tcp.flags.syn == 1 and tcp.flags.ack == 0». Источники каждого такого SYN-пакета отличаются (все пакеты отправлены с различных IP-адресов), но все они имеют идентичный порт назначения 80 (HTTP), идентичную длину (120) и размер TCP окна (64). При установке фильтра «tcp.flags.syn == 1 and tcp.flags.ack == 1», видно, что количество полученных пар пакетов от клиентов (сразу с установленным флагом SYN, а затем — с флагом ACK) относительно небольшое. Это признак атаки TCP SYN-flood на систему.

Рис.5. Анализ трафика с установленным фильтром «tcp.flags.syn == 1 and tcp.flags.ack == 0»

## Моделирование ICMP-flood атаки



Рис. 6. Реализация ICMP-flood атаки

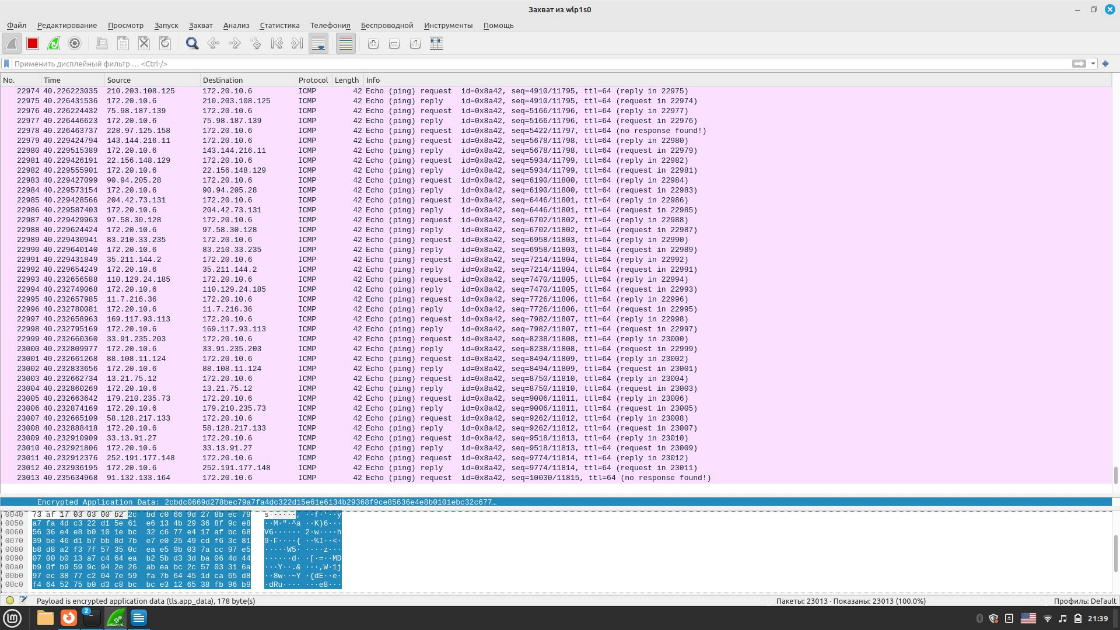
Составные части команды аналогичны описываемым выше частям реализации STN-flood атаки.

Рис. 7. Анализ трафика при ICMP-flood атаке

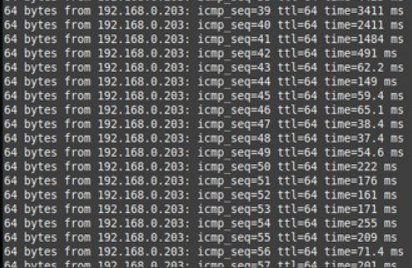


Рис.8. Время задержки при ICMP-flood атаке

## Защита от SYN-flood атаки

SYN-flood: защита заключается в ограничении числа “полуоткрытых” TCP-соединений:



Данный способ защиты не оказался эффективным, время задержки приёма файлов не изменилось:

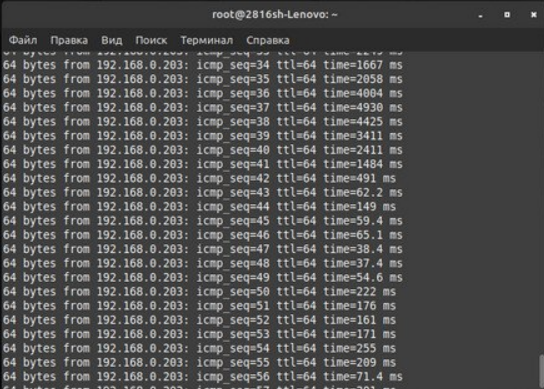


Рис.6. Время задержки при включенной защите

## Защита от ICMP-flood атаки

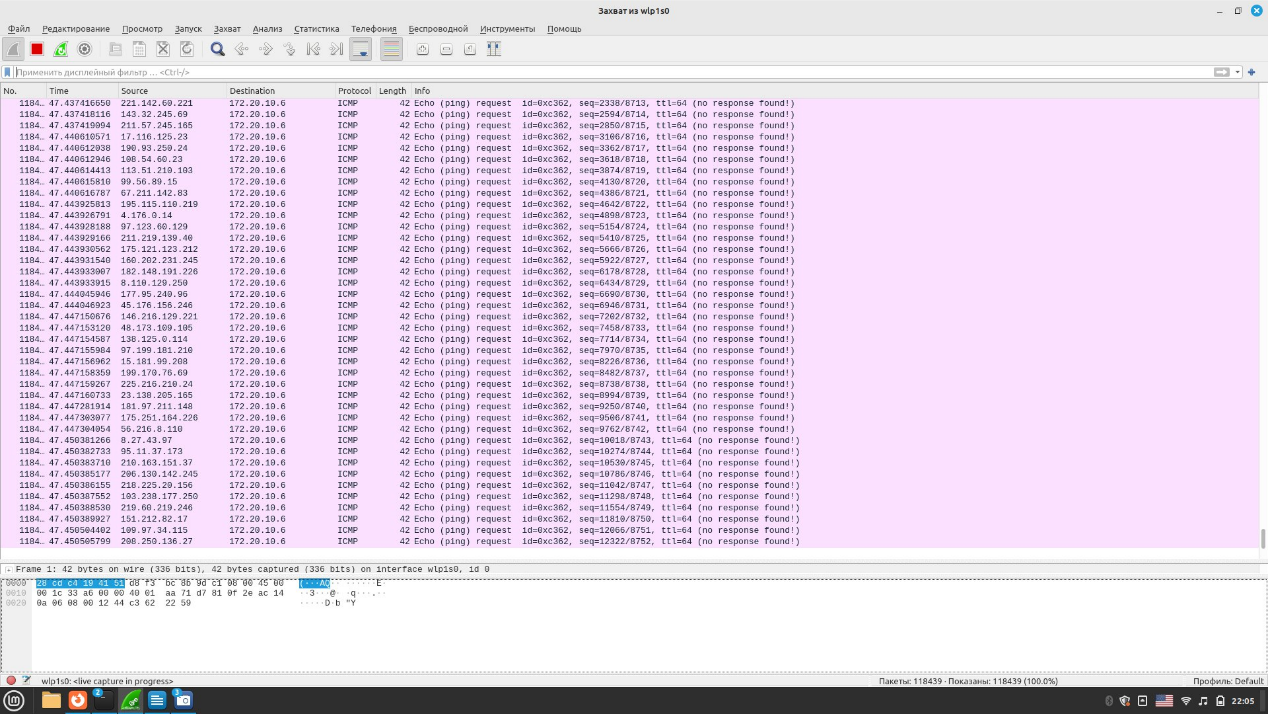
ICMP-flood: защита заключается в отключении ответов на запросы ICMP-echo:

Рис.7. Анализ трафика при защите

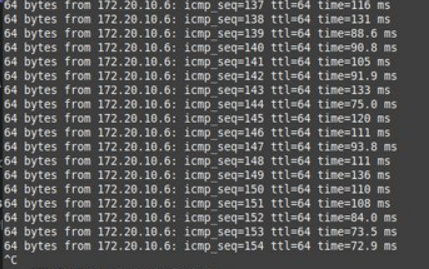
Данная защита эффективна, т.к. наблюдается заметное уменьшение времени задержки:

Рис. 8. Задержка при защите от ICMP-flood

# Результаты работы

В результате проведение SYN-flood и ICMP-flood атак не получилось полностью вывести сервер из строя, т.к. ???. Однако наблюдалось значительное время задержки получения пакетов, во время проведения атак. Защита от SYN-flood-атаки, в отличие от защиты от ICMP-flood-атаки, оказалась неэффективной.

# 7. Вывод

В данной лабораторной работе были рассмотрены различные Dos-атаки, реализованы SYN-flood и ICMP-flood атаки, а также защита от них, установлено какая из защит является эффективной. Таким образом, разработанный метод решает поставленные задачи.

# Ответы на контрольные вопросы

1. *В чем заключается общий принцип проведения DoS-атаки?*

DoS-атаки основаны на идее флуда (flood), т.е. “затопления” жертвы огромным количеством пакетов. Нападающая сторона использует ограниченность вычислительных и информационных ресурсов: производительность сетевого оборудования и серверов ограничена, они не в состоянии обрабатывать огромное число одновременно поступающих запросов («шквал запросов»).

1. *Какие способы защиты от Dos-атак существуют?*

Способы защиты будут зависеть от конкретного типа атаки. SYN-flood -атаки - отключение очереди “полуоткрытых” TCP-соединений. ICMP-flood-атаки - отключение ответов на запросы ICMP echo. HTTP-flood-атаки - увеличение одновременного количества максимальных подключений к базе данных сервера. UDP-flood-атаки - отключение UDP-сервисов и установление ограничения на число соединений с DNS-сервером.

1. *В чем заключается работа генератора пакетов? Какие настройки можно установить при генерации пакетов?*

Генератор пакетов – компьютерная программа, генерирующая случайные пакеты или позволяющая пользователю сформировать и отправить в компьютерную сеть произвольный пакет.

При генерации пакетов можно устанавливать количество и тип создаваемых пакетов, режим отправки (например, непрерывная отправка), адреса источника (в т.ч. указание несуществующего IP-адреса) и приемника, содержание пакета и т.д.

1. *Какова структура UDP-пакета? Что делает возможным проведение DoS-атаки на уровне UDP-трафика?*

Заголовок UDP (User Datagram Protocol) состоит из четырех полей, каждое по 2 байта (т.е. 16 бит). Поля: порт отправителя (указывается номер порта отправителя), порт получателя (содержит порт получателя), длина датаграммы (поле, задающее длину всей датаграммы (заголовка и данных) в байтах) и контрольная сумма (используется для проверки заголовка и данных на ошибки; если сумма не сгенерирована передатчиком, то поле заполняется нулями).

В протоколе UDP отсутствует механизм предотвращения перегрузок, а потому становится возможным проведение DoS-атаки на уровне UDP-трафика. После начала атаки паразитный трафик быстро захватит всю доступную полосу пропускания, полезному трафику останется лишь малая ее часть.

1. *За счет чего отключение ответов на запросы ICMP позволяет решить проблему ICMP-flood?*

Атакуемый компьютер “забрасывается” пакетами типа ICMP. Система должна ответить на данные пакеты, в результате чего создается колоссальное число ответных пакетов, а пропускная способность канала снижается. Если же отключить ответы на ICMP запросы, то такое огромное число ответных пакетов создано не будет, и, как следствие, пропускная способность канала снижена также не будет.