1. Министерство образования и науки Российской Федерации
2. Санкт-Петербургский Политехнический Университет Петра Великого
3. —
4. Институт компьютерных наук и технологий
5. **Кафедра «Информационная безопасность компьютерных систем»**
6. **Лабораторная работа 16**
7. «Защита от компьютерных угроз типа «Отказ в обслуживании »
8. по дисциплине «Практикум по информационной безопасности»

Выполнил:

студент гр. 13558/1 Никулкин В. А.

Проверил:

ассистент преподавателя Алексеев. И. В.

1. Санкт-Петербург
2. 2017

**Цель работы**

Изучение механизма реализации компьютерной угрозы типа «отказ в обслуживании», ознакомление со способами защиты от такого рода угроз.

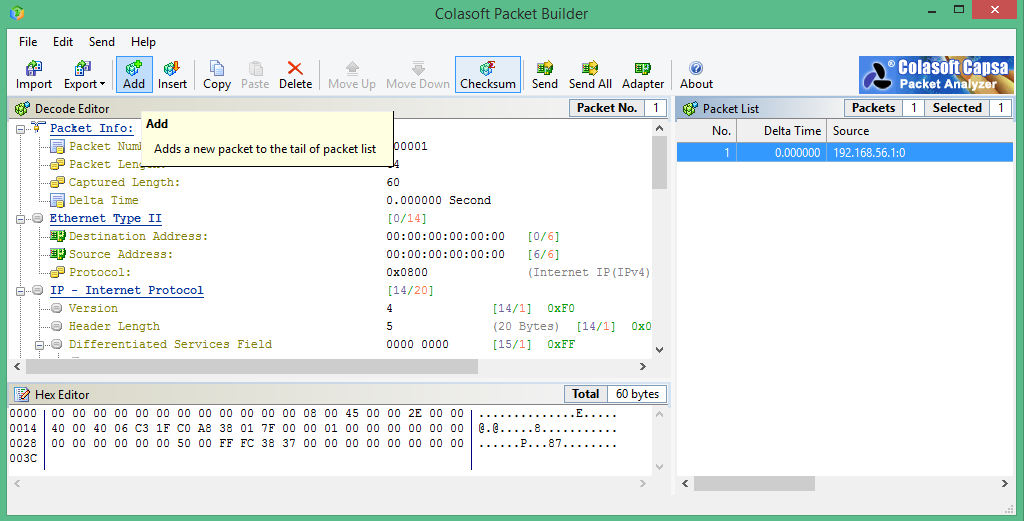
**Ход работы**

1. Были изучены основные возможности таких генераторов пакетов как Ostinato, PACKETH, Colasoft Packet builder.

- Colasoft Packet builder

Colasoft Packet Builder – это сервисная программа, которая разработана для создания настраиваемых сетевых пакетов. Он предоставляет отличные функции редактирования помимо редактирования необработанных HEX данных, данная программа представлена редактором декодирования, который позволяет вам с легкостью редактировать определенные значения поля протоколов. В дополнение к составлению пакетов Colasoft Packet Builder также поддерживает сохранение пакетных файлов и отправку пакетов по сети. Colasoft Packet Builder предоставляет несколько типов обычно используемых пакетов - ARP Пакет, IP Пакет, TCP Пакет и UDP Пакет. Все пакеты и их декодированная информация полностью редактируемы.

Интерфейс:

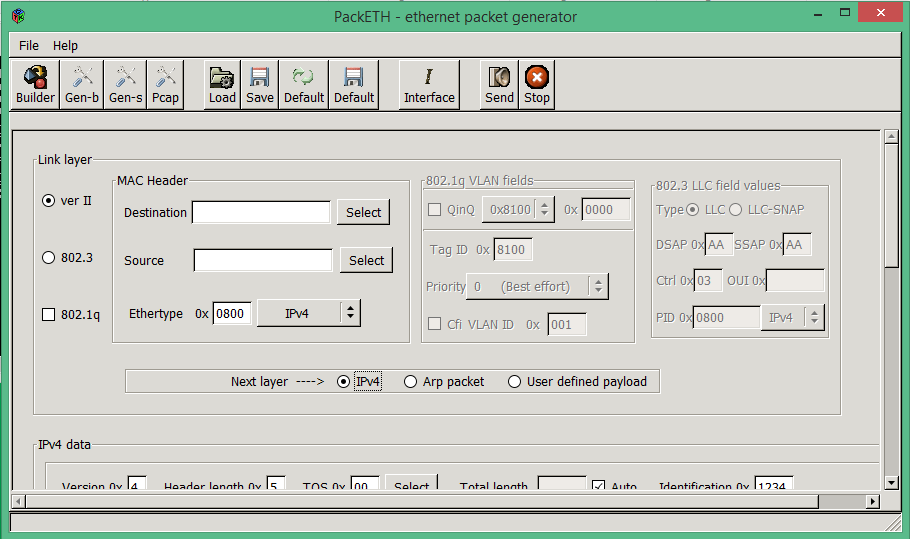


**-**PACKETH

утилита с графическим интерфейсом для генерации Ethernet-кадров, существуют ее версии под ОС Linux, Windows и Mac. Данный генератор пакетов обладает следующими возможностями:

* Генерация кадров Ethernet II, Ethernet 802.3, 802.1q, QinQ или определяемых пользователем.
* Поддержка протоколов ARP, IPv4, IPv6, UDP, TCP, ICMP, ICMPv6, IGMP, RTP (с возможностью задания полезной нагрузки) или определяемых пользователем.
* Генерация Jumbo-фреймов (в случае поддержки драйвером).
  + Посылка очереди пакетов с настраиваемой задержкой и количеством пакетов.
* Возможность сохранения настроек.

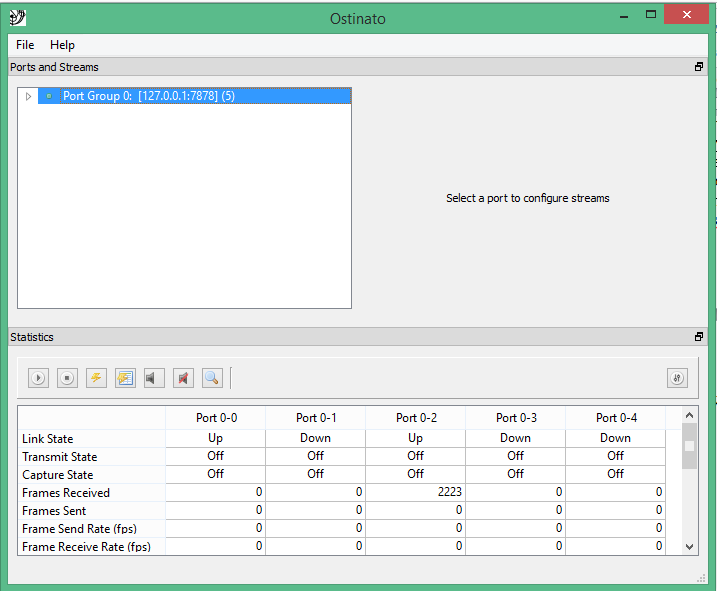
Интерфейс:



-Ostinato

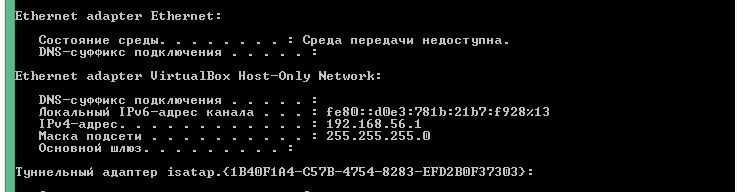
Кроссплатформенный многопоточный генератор трафика, предназначенный для тестирования служб, обеспечивающих работу сети на различных уровнях стека сетевых протоколов. К поддерживаемым протоколам относятся: Ethernet/802.3/LLC SNAP; VLAN (с поддержкой QinQ); ARP, IPv4, IPv6, IP-in-IP a.k.a IP Tunnelling (6over4, 4over6, 4over4, 6over6); TCP, UDP, ICMPv4, ICMPv6, IGMP, MLD; HTTP, SIP, RTSP, NNTP и многие другие. Пользователю предоставляется возможность создавать пакеты данных произвольного содержания, определяя как заголовок пакета, так и содержимое всех его полей. Кроме содержимого пакетов можно выбрать интерфейс и частоту генерации трафика. Ostinato обладает хорошо структурированным интерфейсом с наглядностью представления процесса работы.

Интерфейс:

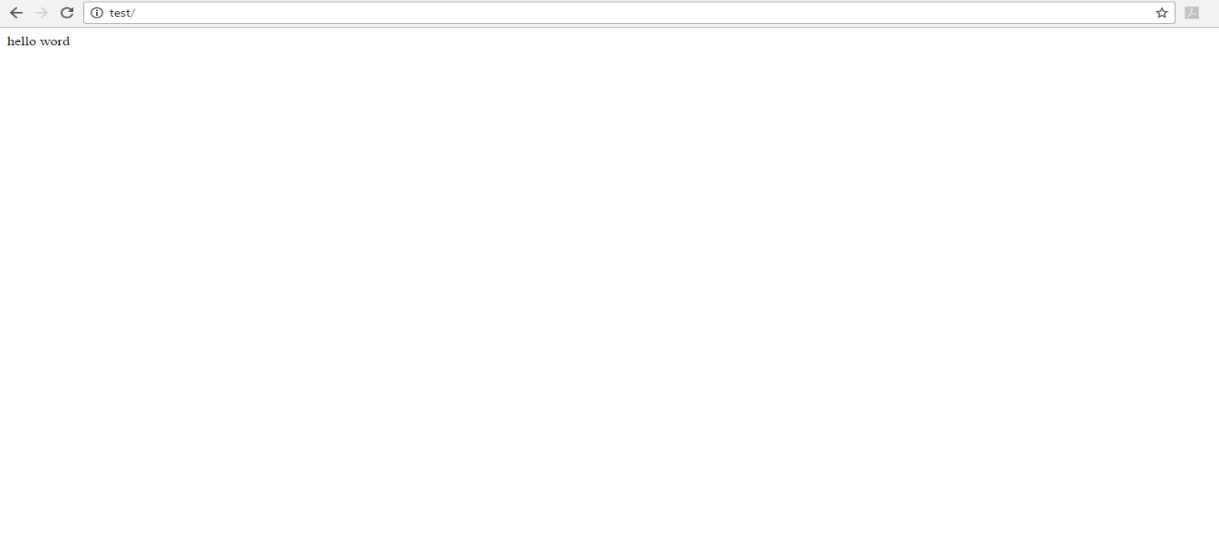


1. Для отправки пакетов на виртуальный веб сервер была выбрана программа Colasoft Packet Builder.

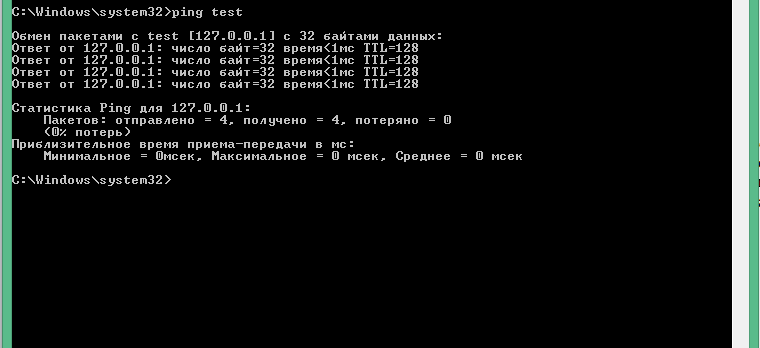
С помощью команды ipconfig устанавливаем IP адрес компьютера



Далее был настроен виртуальный веб сервер, его IP адрес 127.0.0.1



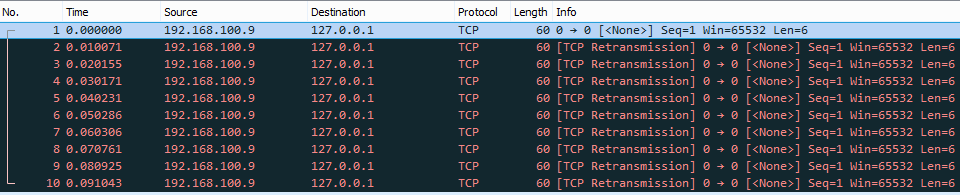
Для того, чтобы убедиться, что все работает, была использована команда ping.



Как видно из скриншота, было отправлено 4 пакета и 4 пакета доставлено, значит, сервер работает корректно.

Теперь отправим несколько пакетов с помощью Colasoft Packet Builder.

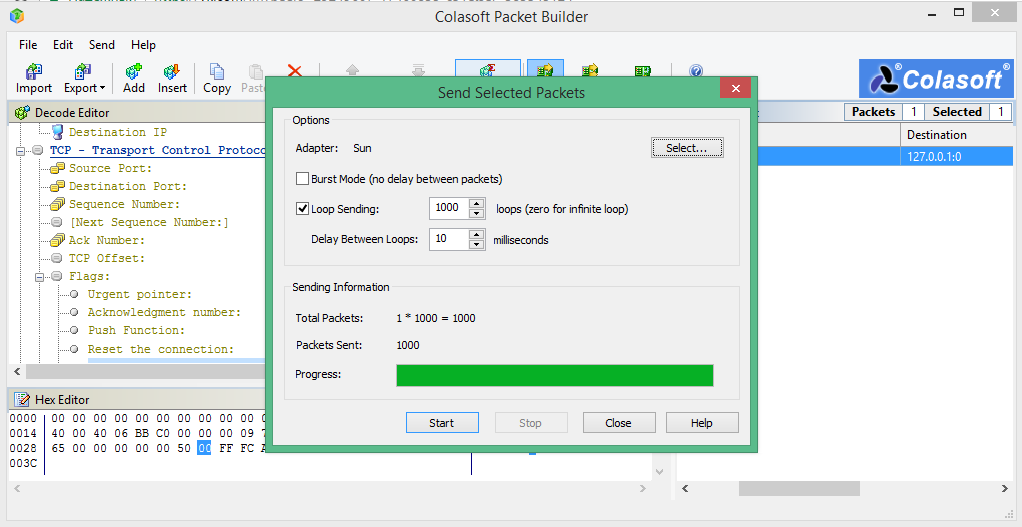
Выбираем тип пакета TCP, в данных пакета вводим IP жертвы и IP получателя, то есть сервера. Я выслал 10 пакетов с интервалом в 100мс. С помощью программы Wireshark проверим, были ли доставлены пакеты.



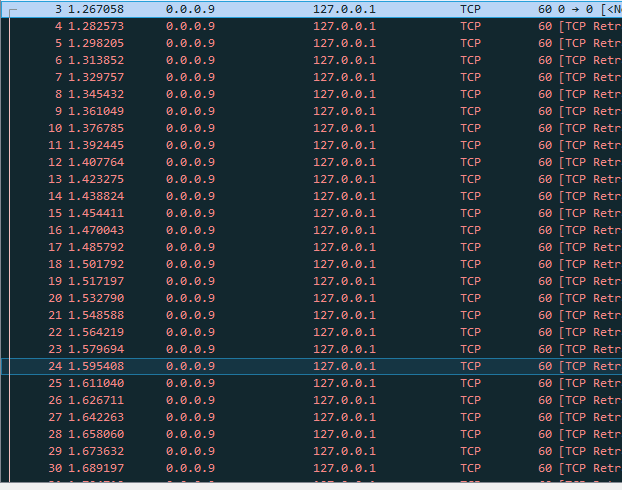
Из скриншота видно, что пакеты были доставлены.

1. Теперь попробуем осуществить SYN-flood атаку. Она заключается в следующем: непрерывное отправление сообщений с запросами на соединение определенному серверу. В пакете указывается несуществующий IP-адрес. Атакуемый узел создает новые динамические структуры данных и запускает таймер для каждой новой попытки соединения до тех пор, пока не исчерпает все свои ресурсы. После этого атакуемый компьютер перестает реагировать на попытки подключения.

Посылаем TCP пакеты, 1000 штук, через каждые 0,01 секунды



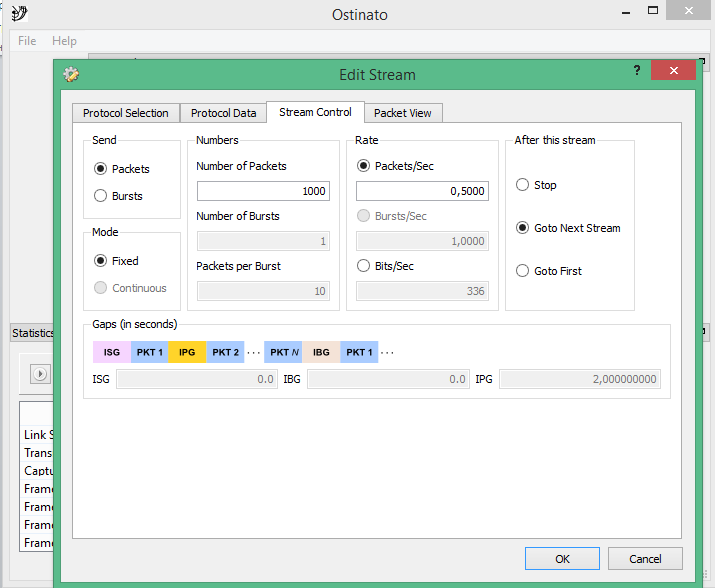
В результате получается следующее



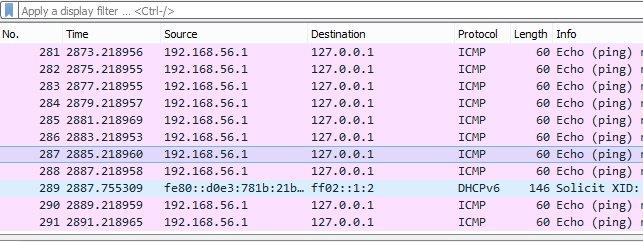
1. Теперь попробуем осуществить ICMP-flood атаку.

Принцип ICMP-flood заключается в отправки большого количества пакетов типа ICMP. Система отвечает на эти пакеты, что отражается на пропускной способности канала. Модуляция атаки ICMP – flood на виртуальный сервер: отправлялся ping запрос на атакуемый сервер. После проверки связи на атакуемый компьютер отправлялось неограниченное количество пакетов ICMP

Для осуществления данного типа атаки используем программу Ostinato, в которой выставляем настройки пакетов. Высылаем 1000 пакетов ICMP интервалом 0, 5 секунды.



В результате получаем следующее



Теоретически, если хватит ресурсов, то данным методом можно перегрузить сервер.

1. Теперь защитимся от спама:

После ввода команды:

sysctl –w net.ipv4.tcp\_max\_syn\_backlog=1024» сервер перестал отвечать на SYN пакеты.

После этого была реализована защита от ICMP-flood с помощью команды «sysctl net.ipv4.icmp\_echo\_ignore\_all=1». В результате система перестала отвечать на запросы ICMP и работа системы восстановилась.

1. Контрольные вопросы:
2. DoS-атаки основаны на идее флуда (flood), т.е. «заваливания» жертвы огромным количеством пакетов.
3. Структура UDP-пакета: заголовок UDP состоит из четырёх полей, каждое по 2 байта: порт отправителя, порт получателя, длина датаграммы (поле, задающее длину всей датаграммы (заголовка и данных) в байтах), контрольная сумма (поле контрольной суммы используется для проверки заголовка и данных на ошибки). Проведение DoS-атаки с его помощью возможно, так как в протоколе UDP механизм предотвращения перегрузок отсутствует, поэтому после начала атаки паразитный трафик быстро захватит всю доступную полосу пропускания, и полезному трафику останется лишь малая её часть.
4. Защита от DoS-атак:

* Защита от SYN-flood строится на отключении очереди «полуоткрытых» TCP-соединений.
* Для того чтобы защититься от ICMP-flood, необходимо отключить ответы на запросы ICMP echo.
* Защита от UDP-flood заключается в том, чтобы отключить UDP-сервисы от внешнего мира и установить ограничение на количество соединений к DNS-серверу.

1. Генератор пакетов — компьютерная программа, генерирующая случайные пакеты или позволяющая пользователю сформировать (с помощью предоставляемых возможностей настроек) и отправить в компьютерную сеть произвольный пакет.
2. При отключении ответов на запросы ICMP, не создается большого числа ответных пакетов и не снижается пропускная способность канала, поэтому этот метод применяется для защиты от ICMP-flood.

**Вывод**

DoS-атака является промежуточным этапом получения полного контроля над системой или вывода ее из состояния нормального функционирования, что идет на руку злоумышленникам. DoS-атака возможна из-за ограниченностью информационных и вычислительных ресурсов. В настоящее время DoS и DDoS-атаки наиболее популярны, так как позволяют довести до отказа практически любую систему, не оставляя юридически значимых улик. Для защиты от сетевых атак применяется ряд фильтров, подключенных к интернет-каналу с большой пропускной способностью. Фильтры действуют таким образом, что последовательно анализируют проходящий трафик, выявляя нестандартную сетевую активность и ошибки.