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

**ЛАБОРАТОРНАЯ РАБОТА № 14**

1. «**Защита от угроз нарушения безопасности типа “Отказ в обслуживании”**»
2. по дисциплине «Основы информационной безопасности»
3. Выполнил
4. студент гр. 4851003/00001 Маронова К.Д.

<*подпись*>

1. Преподаватель
2. асс. преподавателя Пахомов М.А.

<*подпись*>

1. Санкт-Петербург
2. 2023
3. **Цель работы**

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

1. **Постановка задачи**

1.Изучение интерфейса и основных функций генераторов пакетов Nemesis, Colasoft Packet Builder, PACKETH и Ostinato. Сравнение и описание возможностей данных программных продуктов;

2.Моделирование SYN-flood на виртуальный сервер;

3.Моделирование ICMP-flood на виртуальный сервер;

4.Организация элементов защиты от SYN-flood и ICMP-flood.

1. **Теоретические исследования**

Компьютерные угрозы типа "отказ в обслуживании" (Deinal-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 генерируется злоумышленником. Если атака одновременно осуществляется с большого количества компьютеров, ее классифицируют как DDoS (Distributed Denial of Service), в переводе с английского — распределенная атака на отказ в обслуживании.

Обобщенный сценарий 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, который при передаче отправляет уведомление о получении пакета. Если уведомление не получено, пакет посылается заново. Процесс начала сеанса TCP также называется “рукопожатие”, состоящие из 3-х шагов (см. рис 1).

· UDP-пакет — тип пакета, не уведомляющий о его получении.

· ICMP-пакет — тип пакета, предназначенного для служебных задач и не используемого для передачи информации.

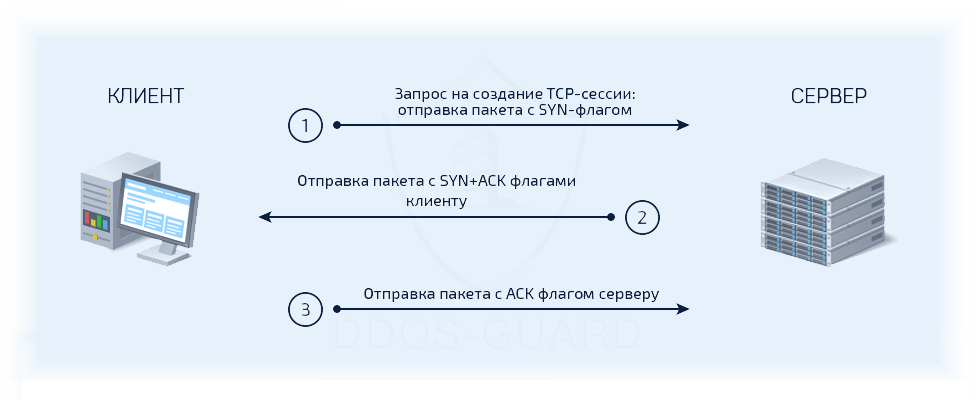
DoS-атаки основаны на идее флуда (flооd), то есть "затопления" жертвы огромным количеством пакетов. Рассмотрим пример флуда с помощью ТСР-пакета. Перед началом обмена данными протокол ТСР устанавливает соединение методом трехэтапного подтверждения. Флаг SYN обозначает начало запроса на установку соединения. 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.

Рисунок 1 — Трёхуровневое рукопожатие.

Рассмотрим последовательность событий:

1. Узел А посылает пакет узлу В, установив в нем значение бита SYN равным 1. Поле Sequenсе Number cодержит начальное значение.

2. Узел В создает структуры данных для установки соединения. Узел В отвечает на запрос соединения, направляя узлу А пакет с флагом АСК, равным 1, и тем самым подтверждая прием пакета от узла А. Флаг SYN в этом втором пакете также равен 1, таким образом узел А знает, что поле Sequence Number в пакете содержит начальное значение для узла В.

3. После получения подтверждения от узла В узел А подтверждает прием начального значения от узла В. При этом пересылается уже содержательный пакет с установленным флагом АСК. В нормальных условиях соединение успешно устанавливается, и узлы могут продолжать обмен данными между собой.

Предположим, что в первом пакете с запросом на установку соединения, пришедшим от узла А, указан неверный IP-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-flоod.

При проведении SYN-flоod, атакующий компьютер непрерывно посылает сообщение с запросами на установку соединения. 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 свои ресурсы. После этого атакуемый компьютер перестает отвечать на попытки подключения. Проведение SYN-flоod выявляется путем подсчета “полуоткрытых” TCP-соединений. При нормальном состоянии системы “полуоткрытых” соединений не должно быть, либо их число не должно превышать 1-3.

Принцип атаки ICMP-flood (или Ping flood) схож с SYN-flood, но атакуемы компьютер “забрасывается” пакетами типа ICMP. Поскольку система должна ответить на такой пакет, это приводит к созданию большого количества ответных пакетов, и, как следствие, к снижению пропускной способности канала.

С помощью протокола ICMP злоумышленник в состоянии изменить настройки сети, например, таблицы маршрутизации. В этом случае возникает эффект недоступности узла, хотя на самом деле не так. Поскольку соответствующая запись в таблице маршрутизации является неверной, сетевой трафик до узла не дойдет.

1. **Описание решения**

В данной работе рассматриваются одновременно несколько генераторов пакетов. Отметим возможности каждого.

Nemesis – утилита для создания и внедрения сетевых пакетов командной строки для UNIX-подобных и Windows-систем. Nemesis хорошо подходит для тестирования систем обнаружения сетевых вторжений и IP-стеков, а также других задач. Как утилита командной строки, Nemesis идеально подходит для автоматизации и написания сценариев.

Отметим, что можно создать и ввести практически любой пользовательский пакет. В частности, с его помощью часто реализуют различные виды атак.

Nemesis может изначально создавать и внедрять ICMP, TCP, UDP, ARP, DNS, ETHERNET, IGMP, IP, OSPF и RIP-пакеты.

Colasoft Packet Builder позволяет создавать пользовательские сетевые пакеты. Пользователи могут использовать этот инструмент для проверки своей сетевой защиты от атак злоумышленников. Colasoft Packet Builder включает в себя очень мощную функцию редактирования. Кроме того, данная утилита имеет редактор декодирования.

Пользователи могут редактировать информацию декодирования в двух редакторах – Decode Editor и Hex Editor. Пользователи могут выбрать один из предоставленных шаблонов Ethernet, ARP, IP, TCP и UDP-пакета, а также изменить параметры в Редакторе декодера, шестнадцатеричном редакторе или редакторе ASCII для создания пакетов.

В Colasoft Packet Builder пользователи могут выбрать один из предоставленных шаблонов Ethernet, ARP, IP, TCP и UDP-пакета.

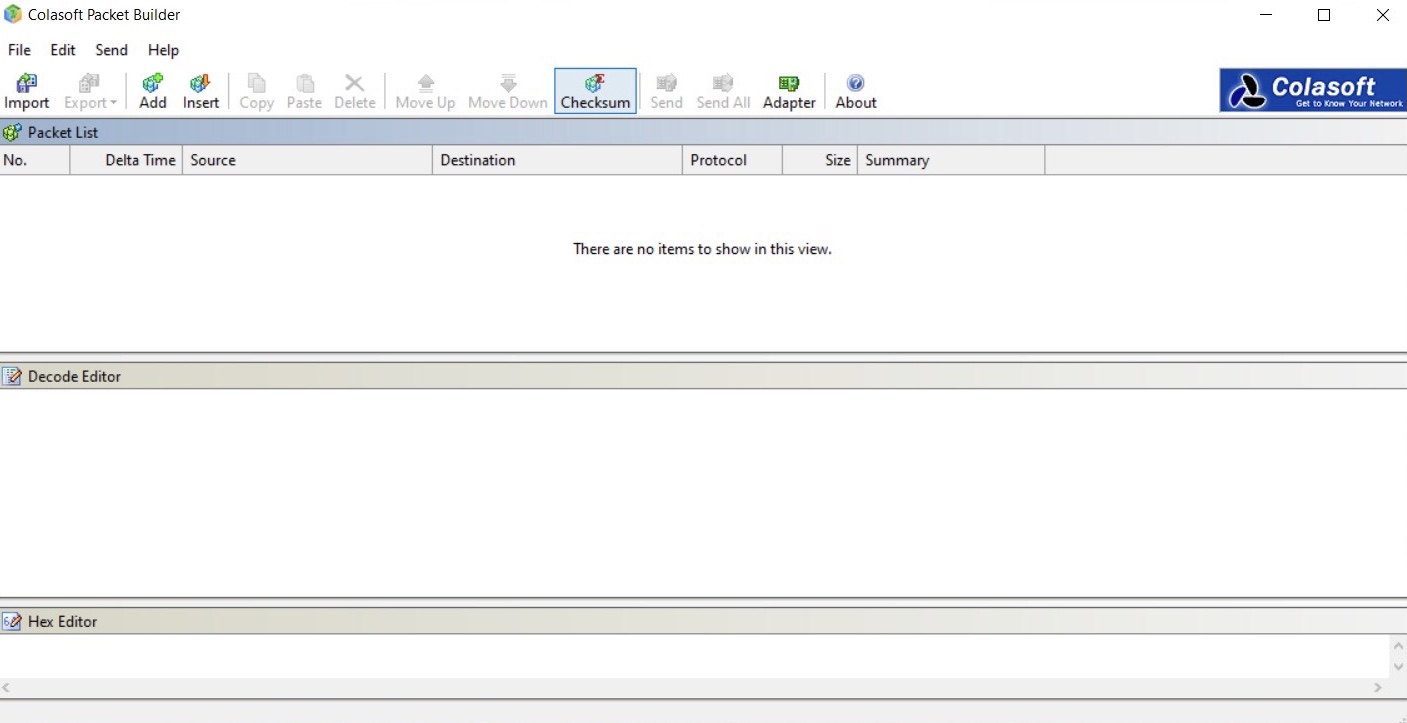


Рисунок 2 – Интерфейс Colasoft Packet Builder

PACKETH позволяет создавать и посылать любые возможные пакеты или последовательности пакетов в сеть Ethernet. На данный момент поддерживаются следующие протоколы: ethernet II, ethernet 802.3, 802.1q, QinQ; ARP, IPv4, IPv6; UDP, TCP, ICMP, ICMPv6, IGMP; RTP и т.д.

Также есть возможность выбора режима отправки пакетов:

* Задержки между отправкой пакетов, задание количества пакетов;
* Отправка с максимальной скоростью, которую позволяет оборудование;
* Изменение параметров во время тестов (например, изменение IP адреса).

На данный момент в PACKETH поддерживаются следующие протоколы: ethernet II, ethernet 802.3, 802.1q, QinQ; ARP, IPv4, IPv6; UDP, TCP, ICMP, ICMPv6, IGMP; RTP и т.д.

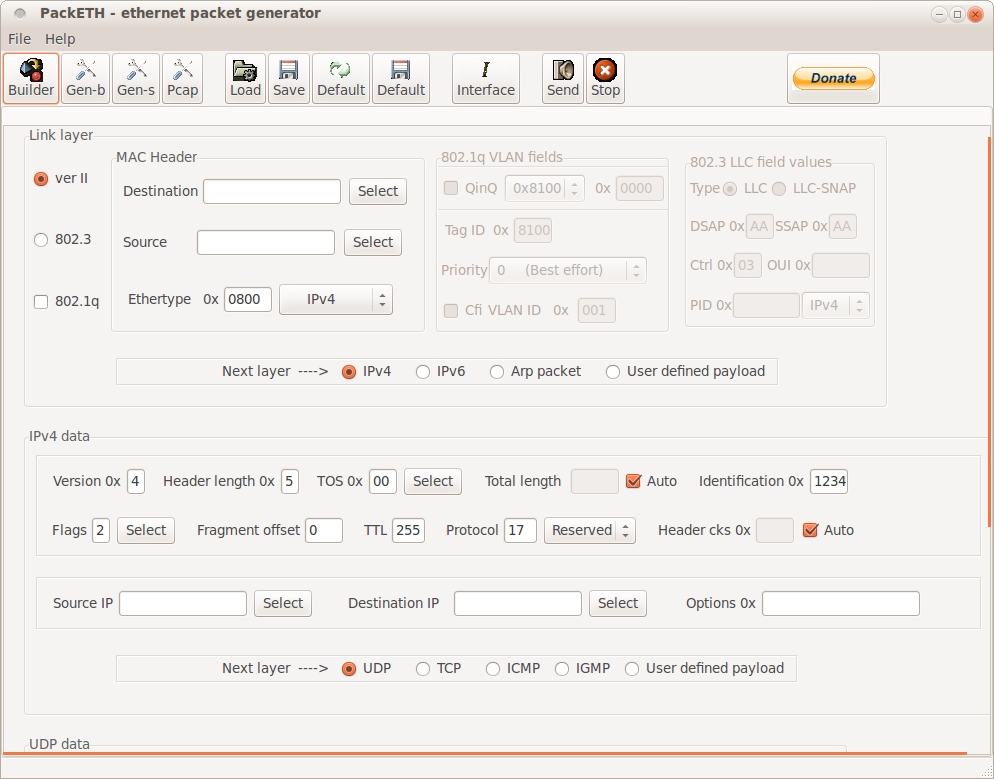


Рисунок 3 – Интерфейс PACKETH

Ostinato – 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 т.д.

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.

К поддерживаемым Ostinato 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 т.д.

Таким образом, рассмотренные генераторы схожи по своему функционалу. Мы можем наблюдать различие лишь в некоторых характеристиках, возможностях, а также доступных для генерации пакетов.

Данная работа была выполнена на операционной системе Linux Ubuntu 22.04 c использованием генератора пакетов hping3. Он позволяет подменять реальные IP-адреса случайными. С его помощью мы и реализуем DoS-атаку.

Сначала получим наш IP-адрес на который будет направлена атака при помощи команды  sudo ifconfig. IP-адресс «жертвы»: 10.0.2.15

Смоделируем SYN-flood на виртуальный сервер. Данную операцию позволяет выполнить следующая команда:

***hping3 -c 15000 -d 120 -S -w 64 -p 80 --flood --rand-source 10.0.2.15***

Мы отправляем 15000 пакетов (“-c 15000”) размером 120 байт (“-d 120”) каждый. Мы также указываем, что флаг SYN (“-S”) должен быть включен, а размер TCP-окна имеет значение 64 (“-w 64”). Чтобы направить атаку на HTTP-веб-сервер нашей жертвы, мы указываем порт 80 (“-p 80”) и используем флаг (“—flood”) для максимально быстрой отправки пакетов. Также реализуем генерацию поддельных IP-адресов, установив флаг (“--rand-source”). В завершение укажем IP-адрес “жертвы”

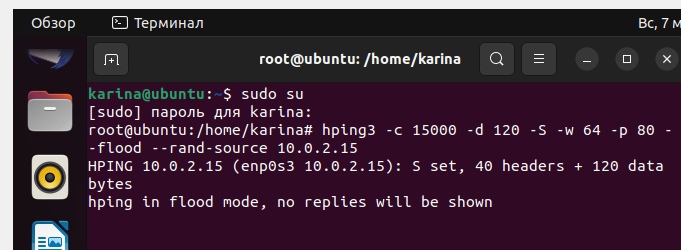


Рисунок 4 – SYN-flood на виртуальный сервер

Для отслеживания получения пакетов сервером был использован Wireshark:

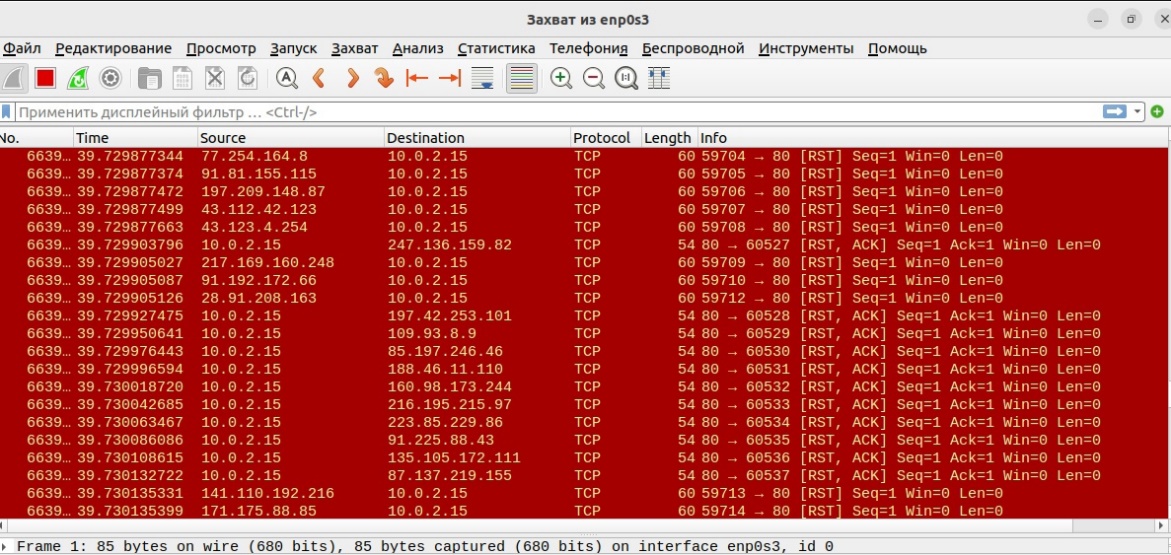


Рисунок 5– SYN-flood

Далее реализуем ICMP-flood. Для этого воспользуемся командой:

***hping3 --icmp --rand-source -c 1234567 --flood 10.0.2.15***

“hping3” – генератор пакетов; “—icmp” – используемых протокол;  
“—rand-source” – генерация поддельных адресов; “-с 1234567” – количество отправляемых пакетов; “—flood” – флаг флуда для ускорения отправки пакетов; “10.0.2.15” – IP-адрес жертвы.

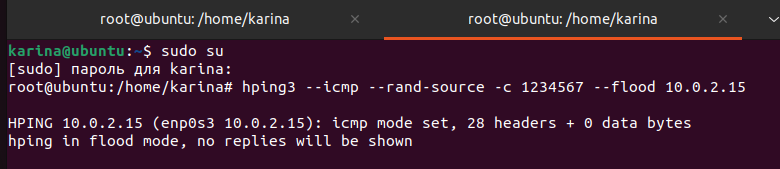
******

Рисунок 6– реализация ICMP-flood

Как видим, принцип схож с вышеописанной и проведенной SYN-flood атакой. Система вновь выводит сообщение о том, что теперь она находится в состоянии “flood”.

Возможно проверить работоспособность сети с помощью ping, простого инструмента для диагностики сети. Эта утилита позволяет проверить, доступен удаленный хост или нет и все. Для этого утилита проверяет, может ли хост отвечать на сетевые запросы с помощью протокола ICMP. Так же мы можем отследить поступающие пакеты с помощью утилиты Wireshark:

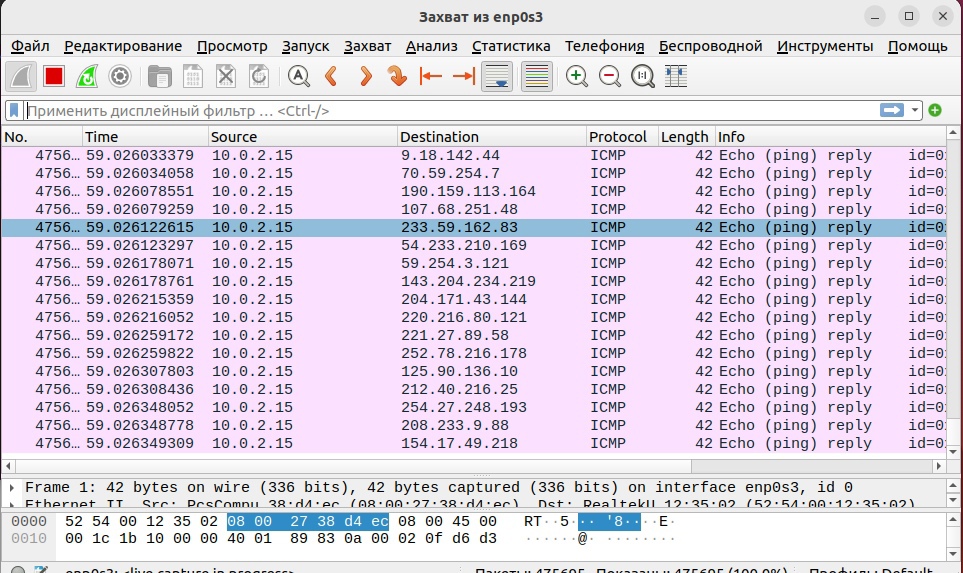


Рисунок 7– ICMP-flood. Wireshark

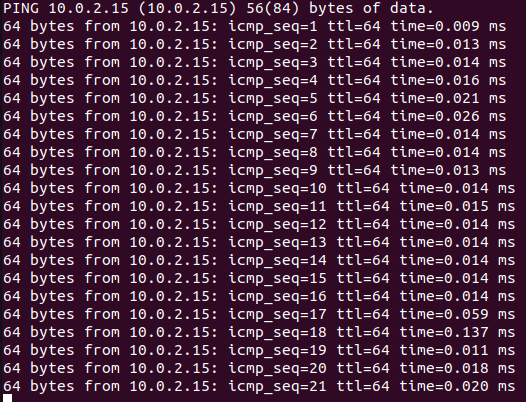


Рисунок 8– ICMP-flood. PING 10.0.2.15

Атака ICMP-flood отправляет бОльшее количество запросов, но при этом с меньшей скоростью и бОльшим интервалом времени, чем атака SYN-flood

Согласно учебному пособию “Основы информационной безопасности. Лабораторный практикум”, повторим проделанную выше работу, но перед этим реализуем элементы защиты от рассматриваемых нами атак.

Для отключения очереди “полуоткрытых” TCP-соединений воспользуемся командой:

***#sysctl –w net.ipv4.tcp\_max\_syn\_backlog=1024***

Предпринятые меры защиты не привели к желаемому результату. Мы вновь можем отследить количество поступающих пакетов. Отличия от результатов, достигнутых в прошлом пункте работы, отсутствуют.

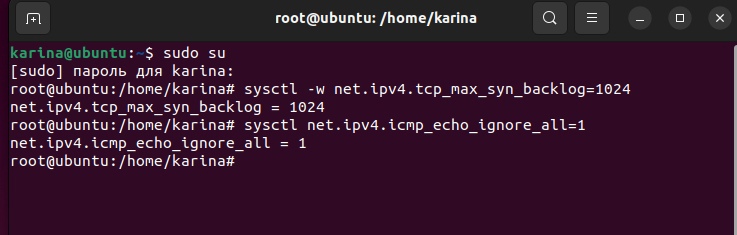


Рисунок 9 – установка защиты от SYN-flood

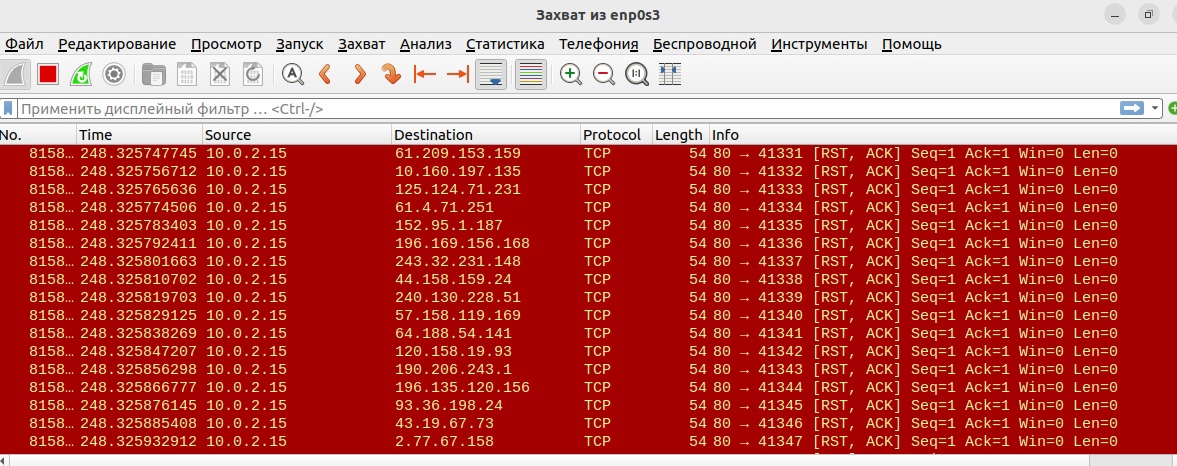


Рисунок 10 – проверка результатов защиты от SYN-flood

Для отключения ответов на запросы ICMP echo применим следующую команду:

***#sysctl net.ipv4.icmp\_echo\_ignore\_all=1***

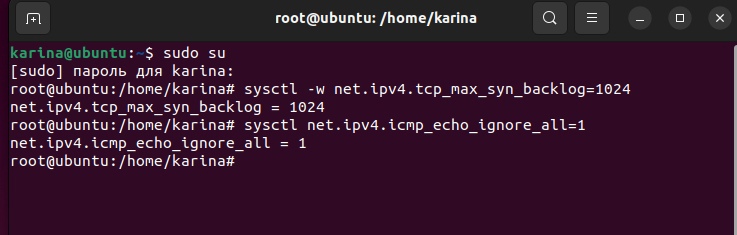


Рисунок 12– установка защиты от ICMP-flood

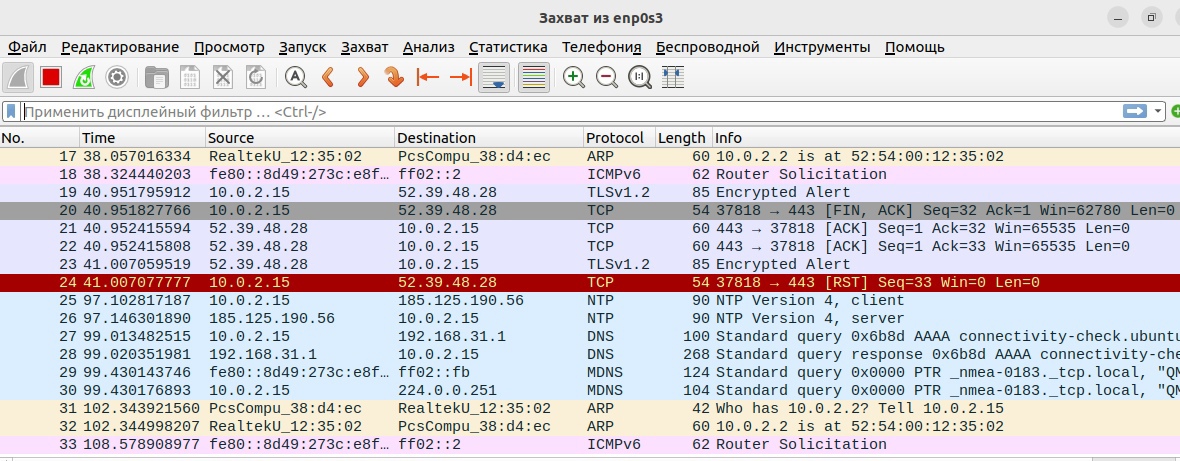


Рисунок 13 – проверка результатов защиты от ICMP-flood

В данном случае защита дала свои плоды, запросы на ICMP пакеты прекратились. Возможно это обусловлено малым количеством отправленных пакетов.

Хотя в ходе работы получилось реализовать атаки, но не от всех получилось защититься. У этого может быть несколько причин: нахождение отправителя и получателя в одной локальной сети, управление операционными системами в виртуальной среде и т.д.

1. **Контрольные вопросы**

1)*В чем заключается общий принцип проведения DoS-атаки?* DoS-атаки основаны на идее флуда (flood), т.е. «заваливания» жертвы огромным количеством пакетов.

2)*Какие способы защиты от DoS-атак существуют?*

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.

3)*В чем заключается работа генератора пакетов? Какие настройки можно установить при генерации пакетов?* Генератор пакетов — компьютерная программа, генерирующая случайные пакеты или позволяющая пользователю сформировать (с помощью предоставляемых возможностей настроек) и отправить в компьютерную сеть произвольный пакет.

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

5)*За счет чего отключение ответов на запросы ICMP позволяет решить проблему ICMP-flood?* При отключении ответов на запросы ICMP, не создается большого числа ответных пакетов и не снижается пропускная способность канала.

1. **Выводы**

В ходе работы был изучен механизм реализации компьютерной угрозы типа «отказ в обслуживании»; рассмотрены некоторые способы защиты от такого рода угроз; изучены программы для создания разного типа пакетов и для отслеживания и анализа трафика.