1. Министерство образования и науки Российской Федерации
2. Санкт-Петербургский Политехнический Университет Петра Великого
3. —
4. Институт прикладной математики и механики
5. **Кафедра «Информационная безопасность компьютерных систем»**

**ЛАБОРАТОРНАЯ РАБОТА № 14**

1. «Защита от угроз нарушения безопасности типа “отказ в обслуживании”»
2. по дисциплине «Основы информационной безопасности»
3. Выполнил
4. студент гр. 4851001/20001 Козлов О.И.

<*подпись*>

1. Преподаватель
2. профессор Калинин М. О.

<*подпись*>

1. Санкт-Петербург
2. 2023

Оглавление

[1) Цель работы 3](#_Toc129303227)

[2) Постановка задачи 3](#_Toc129303228)

[3) Ход работы 3](#_Toc129303229)

[4) Контрольные вопросы 24](#_Toc129303230)

[5) Выводы 25](#_Toc129303231)

## Цель работы

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

## Постановка задачи

1. Описание возможностей исследованных генераторов пакетов.
2. Описание механизмов атак *SYN-flood* и *ICMP-flood* на виртуальный сервер.
3. Пакеты, генерируемые каждым генератором пакетов.
4. Сопоставление результатов экспериментов, полученных без и с использованием элементов защиты от *SYN-flood* и *ICMP-flood.*
5. Ответы на контрольные вопросы.

## Ход работы

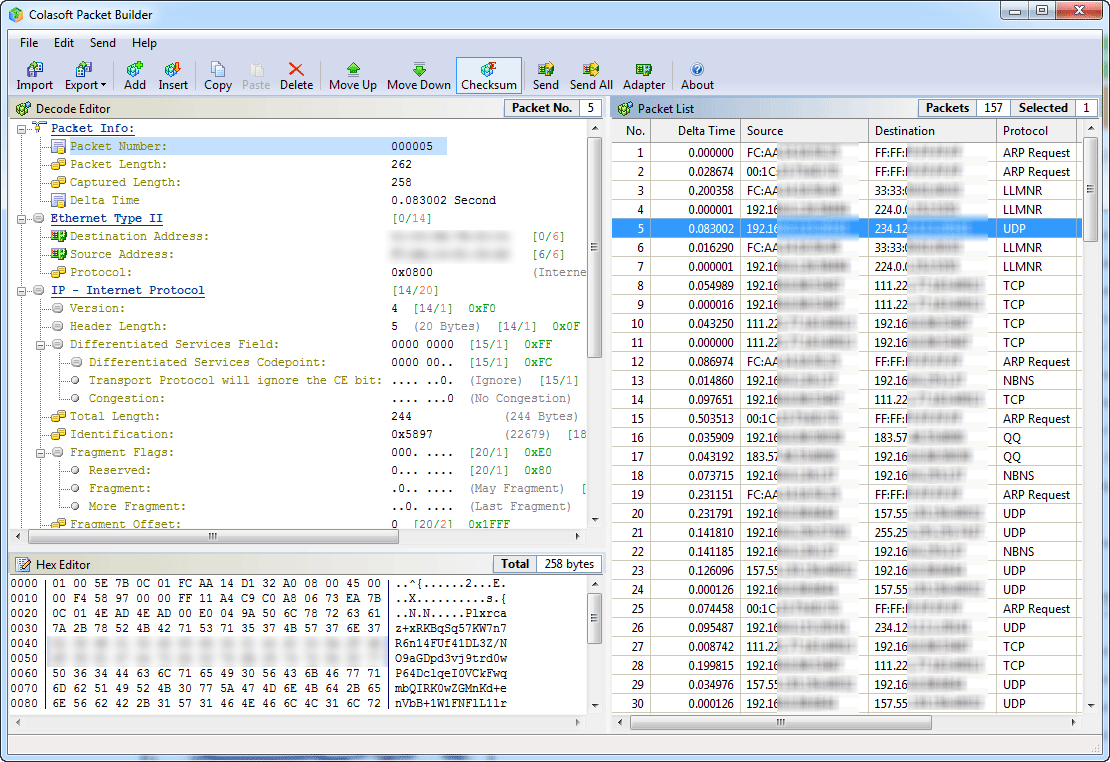
1. Рассмотрим несколько генераторов пакетов и проанализируем возможности каждого.

* *Nemesis –* конструктор и инжектор сетевых пакетов. Изначально распространялся только на \*nix-системы, чуть позже стал входить в состав портов FreeBSD (раздел security), а теперь и вовсе обзавелся виндовым портом. Позволяет собирать любые пакеты следующих протоколов: ARP, DNS, Ethernet, ICMP, IGMP, IP, OSPF, RIP, TCP, UDP, благодаря чему зарекомендовал себя как мощный хакерский инструмент. В частности, с его помощью часто реализуют различные виды атак (ICMP Redirect, DoS путем формирования аномальных пакетов). Идеально подходит для автоматизации и написания сценариев.

**

*Рисунок 1 – интерфейс программы Nemesis*

* *Colasoft Packet Builder* – позволяет создавать собственные сетевые пакеты. Пользователи могут использовать этот инструмент для проверки защиты своей сети от атак и злоумышленников. Colasoft Packet Builder включает в себя очень мощную функцию редактирования. Помимо обычного редактирования необработанных данных HEX, он имеет редактор декодирования, позволяющий пользователям намного проще редактировать значения определенных полей протокола. Пользователи могут выбрать один из предоставленных шаблонов Пакет Ethernet, Пакет ARP, Пакет IP, Пакет TCP и Пакет UDP и изменить параметры в редакторе декодера, шестнадцатеричном редакторе или редакторе ASCII для создания пакетов. Любые изменения будут немедленно отображаться в двух других окнах. Помимо создания пакетов, Colasoft Packet Builder также поддерживает сохранение пакетов в файлы пакетов и отправку пакетов в сеть.



*Рисунок 2 – интерфейс программы Colasoft Packet Builder*

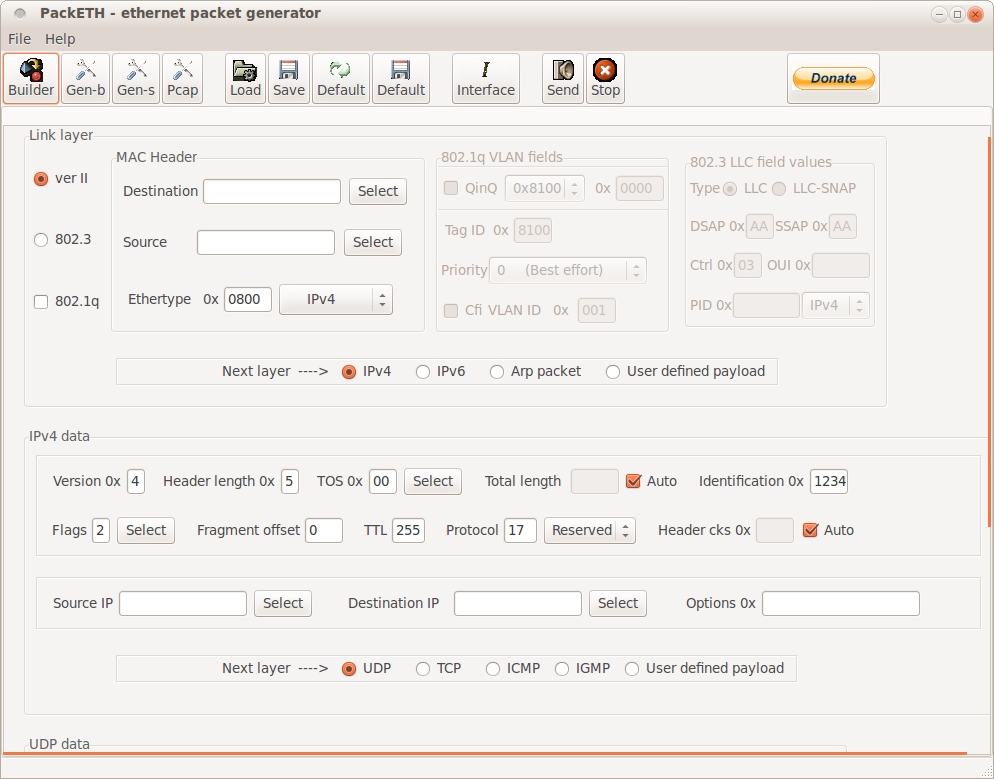
* *PACKETH* – это GUI и CLI генератор пакетов ethernet. Он позволяет создавать и посылать любые возможные пакеты или последовательности пакетов в сеть Ethernet. Это очень простая и мощная программа, которая поддерживает большое количество параметров и настроек. Вы можете создать и послать любой ethernet пакет.

На данный момент поддерживаются следующие протоколы:

* ethernet II, ethernet 802.3, 802.1q, QinQ, пользовательские ethernet фреймы
* ARP, IPv4, IPv6, пользовательские типы данных сетевого уровня
* UDP, TCP, ICMP, ICMPv6, IGMP, пользовательские типы данных транспортного уровня
* RTP
* JUMBO фреймы (если позволяет сетевая карта и драйвера)

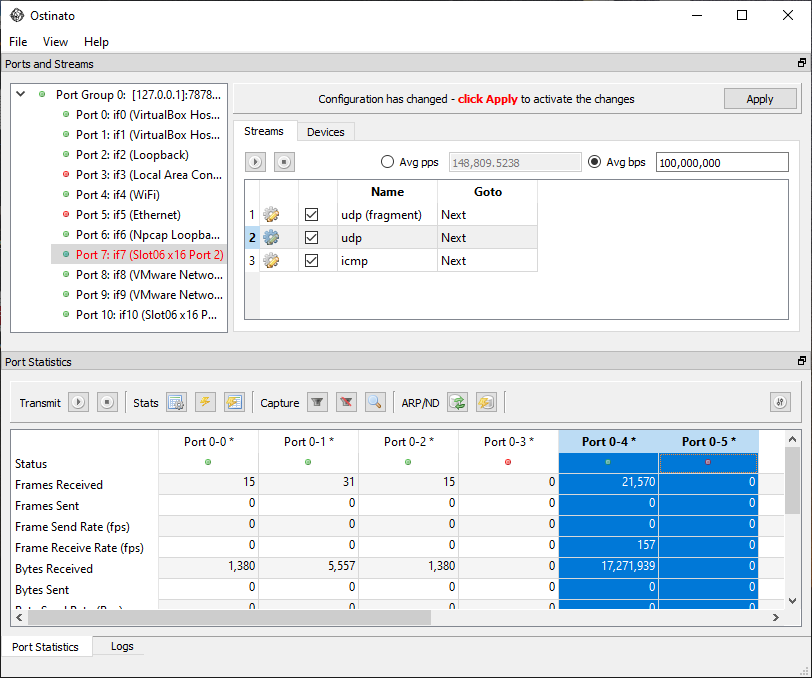
Возможности посылки последовательностей пакетов:

* Задержки между отправкой пакетов, задание количества пакетов
* Отправка с максимальной скоростью, которую позволяет оборудование
* Изменение параметров во время тестов (изменение IP или mac адреса, содержание пакетов UDP, и т.д.)
* Сохранение конфигурации в файл и загрузка из него, поддержка формата pcap.



*Рисунок 3 – интерфейс программы PACKETETH*

* *Ostinato* – многопоточныйгенератор трафика, предназначенный для тестирования служб, обеспечивающих работу сети на различных уровнях стека сетевых протоколов. 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. Основные функции приложения ориентированы на мониторинг и отображение подробных входящих и исходящих сетевых пакетов. На панели “Порты и потоки” вы можете просмотреть доступные и используемые порты, а также IP-адреса и устройства, которыми они используются. Кроме того, потоки могут быть созданы для любого из доступных портов, с возможностью их включения или отключения, сохранения в файл или импорта уже существующего.

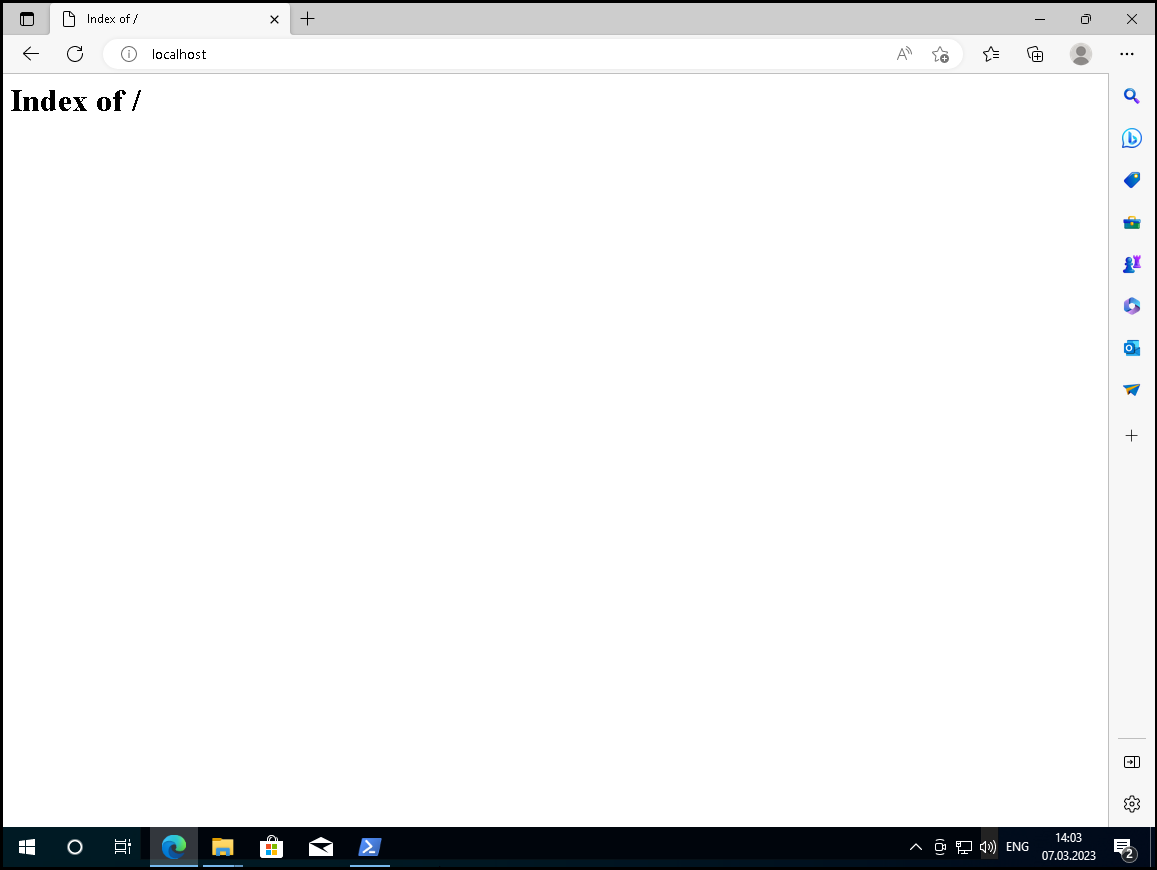


*Рисунок 4 – интерфейс программы Ostinato*

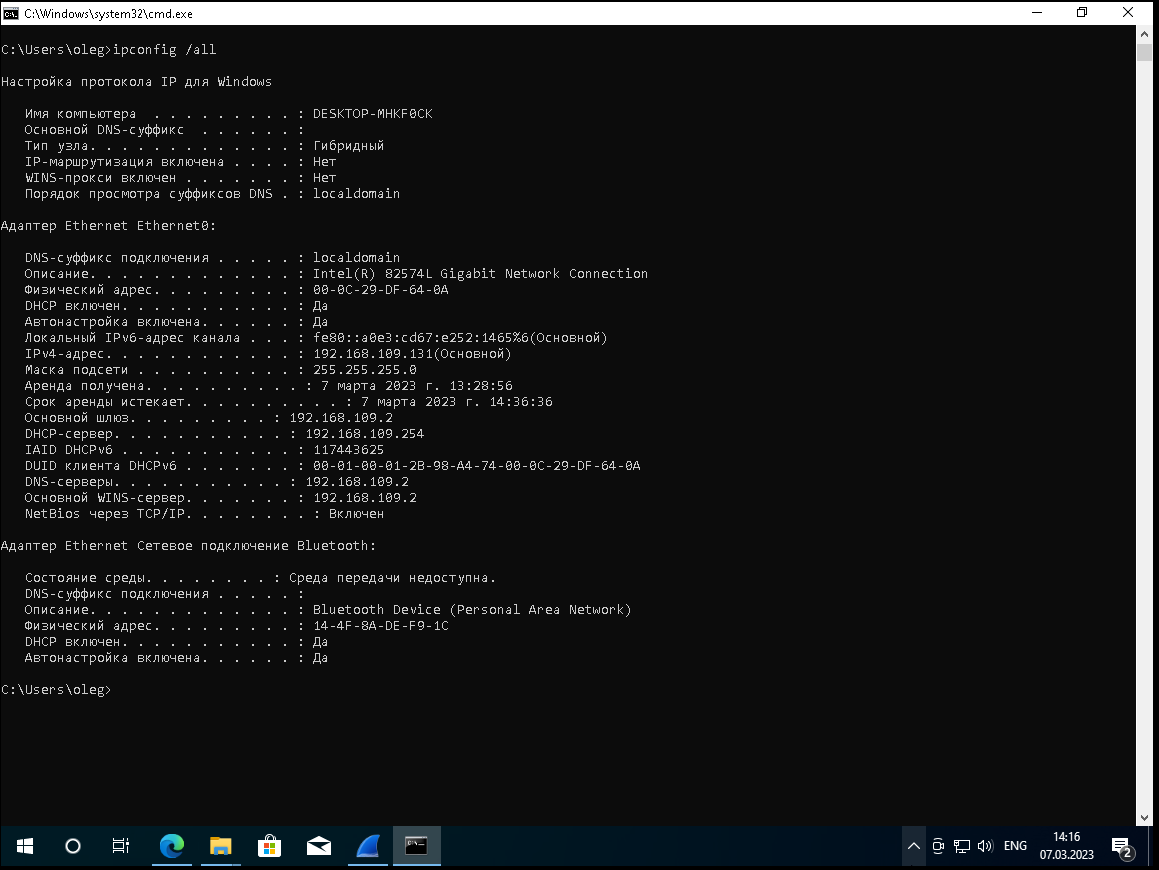
1. Механизмы атак *SYN-flood и ICMP-flood*
   1. *SYN-flood*

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

Для реализации DOS-атаки был создан виртуальный сервер Apache.

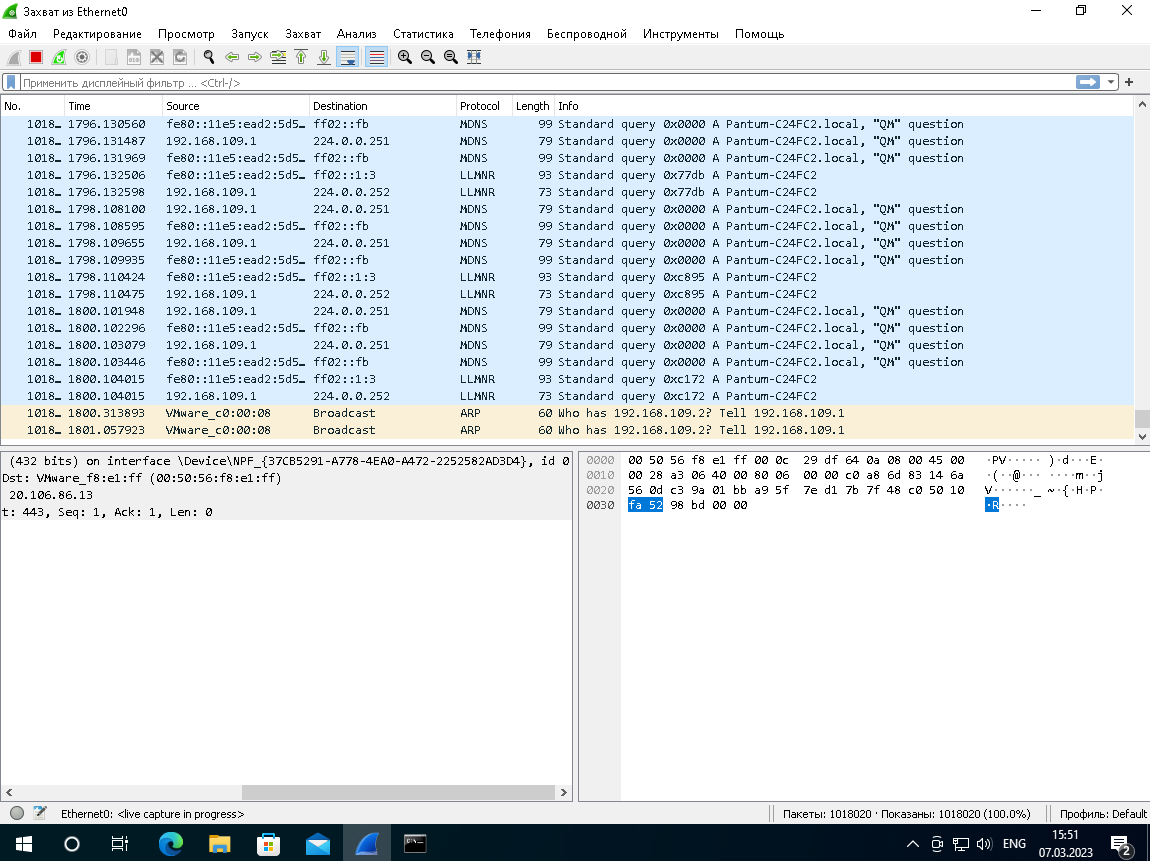


*Рисунок 5 – Сервер Apache*

**

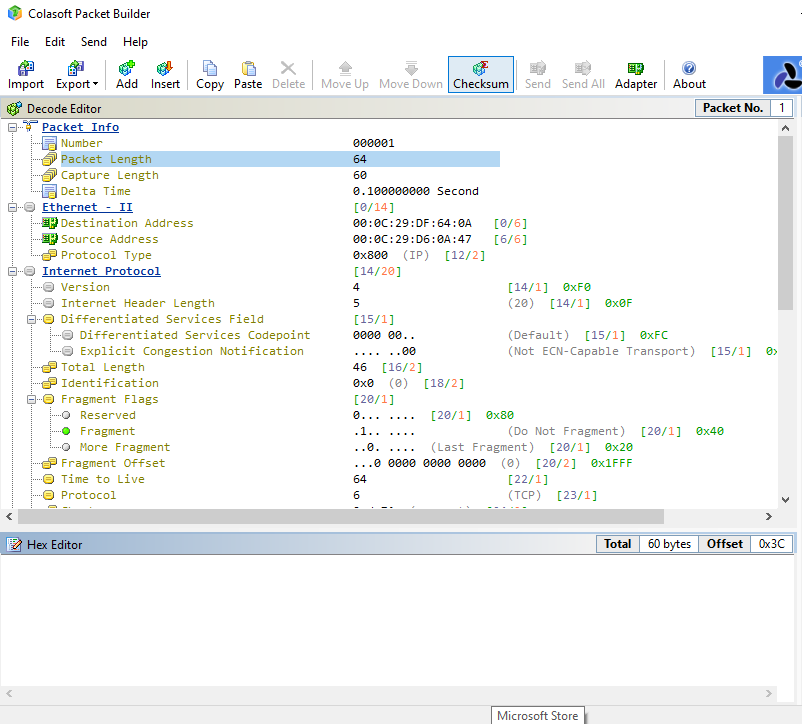
*Рисунок 6 – интерфейс конфигурации сети TCP/IP Windows*

Для того, чтобы отслеживать сетевой трафик, приходящий на сервер, будем использовать WireShark.

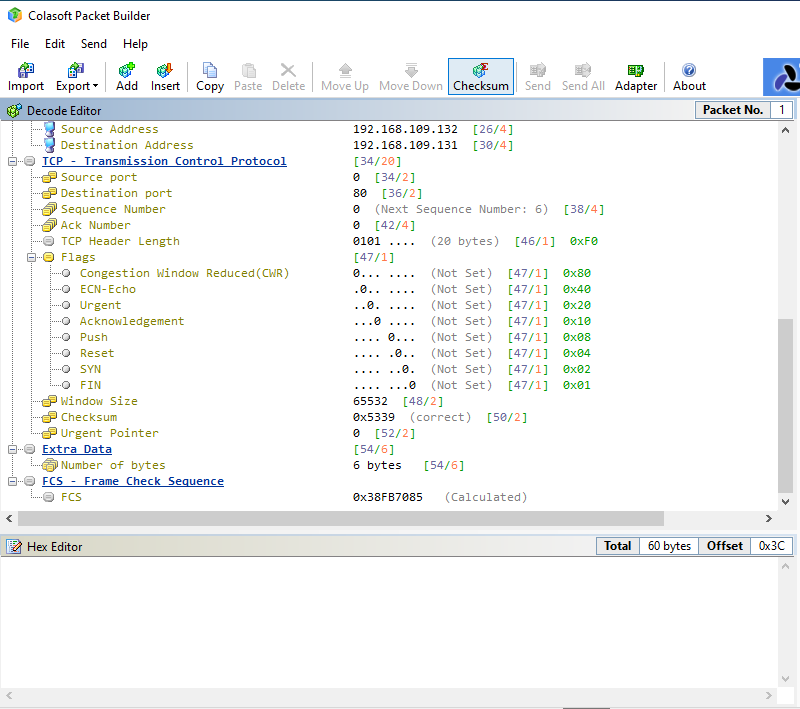


*Рисунок 7 - интерфейс программы WireShark*

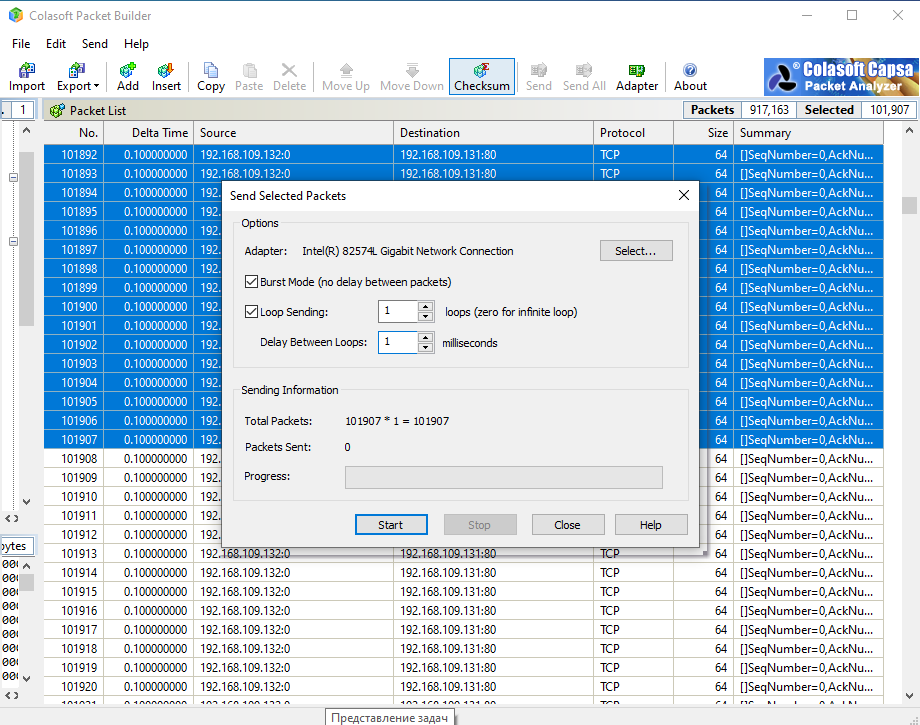
Для реализации *SYN - flood* атаки будем использовать Colasoft Packet Builder.



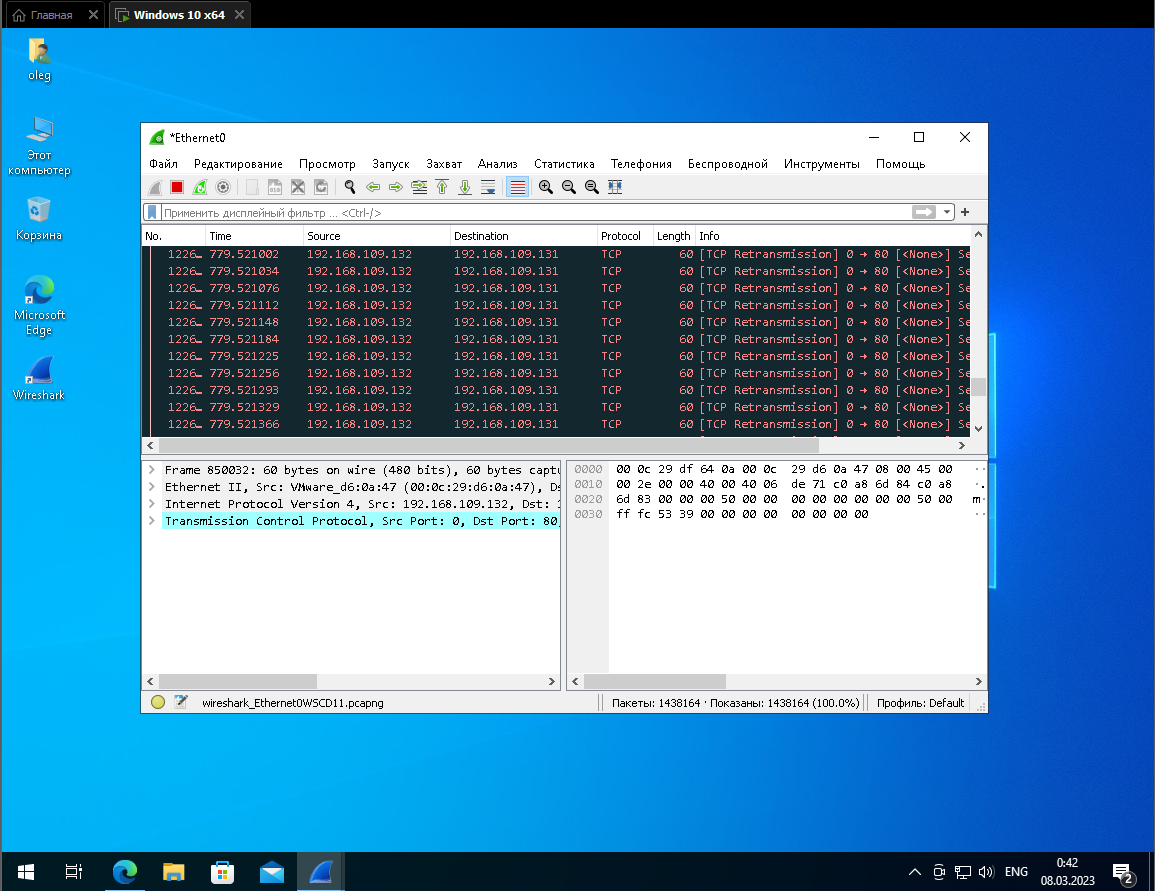
*Рисунок 8 – параметры Colasoft Packet Builder*



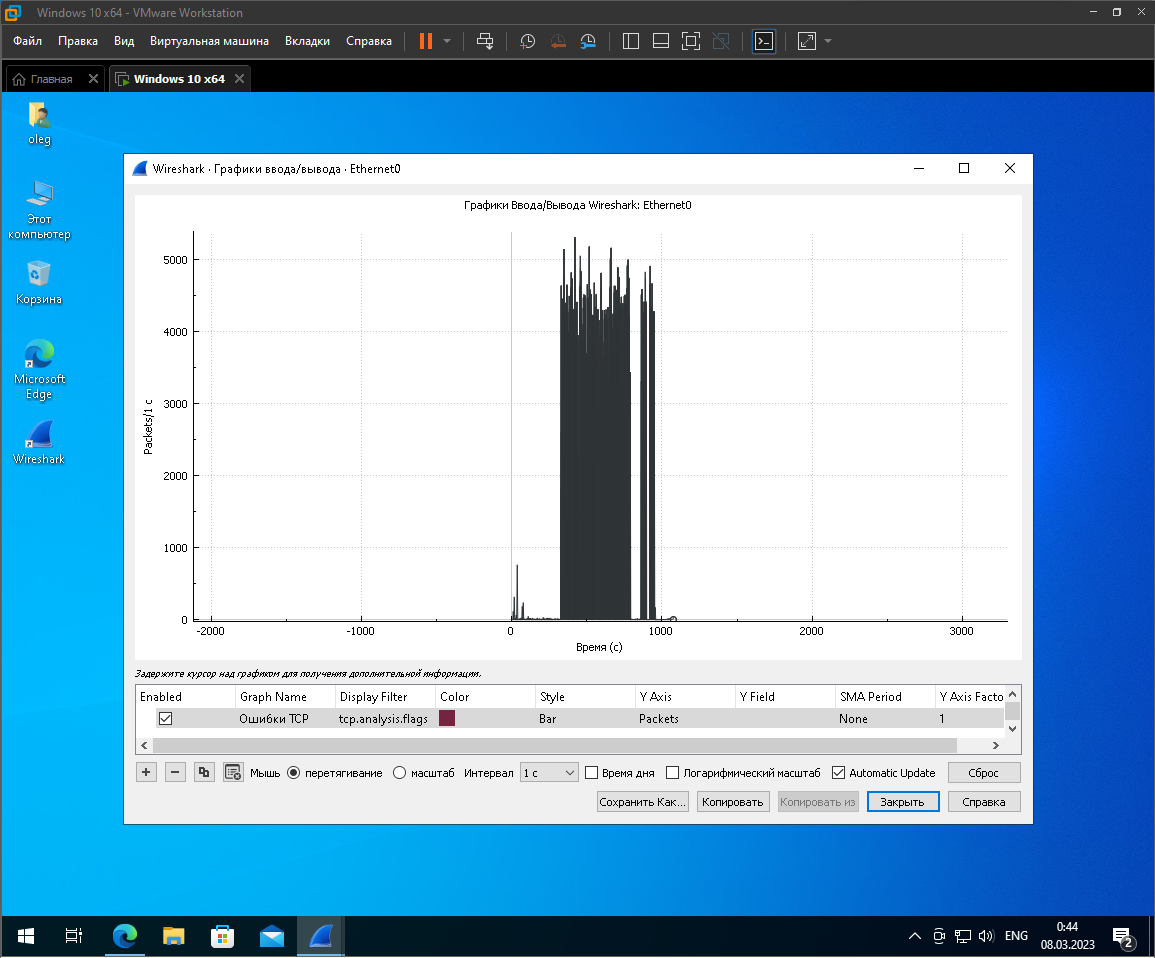
*Рисунок 9 – параметры Colasoft Packet Builder*



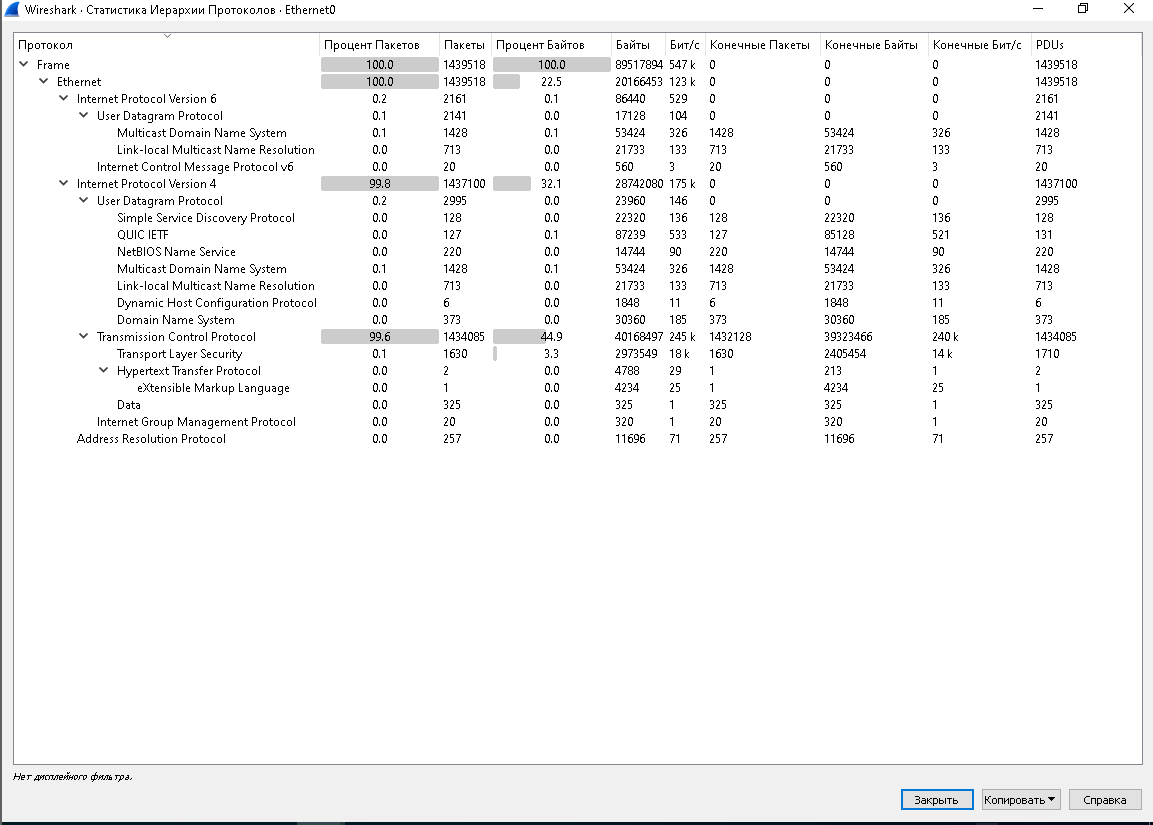
*Рисунок 10 – параметры Colasoft Packet Builder*



*Рисунок 11 – SYN - flood атака*



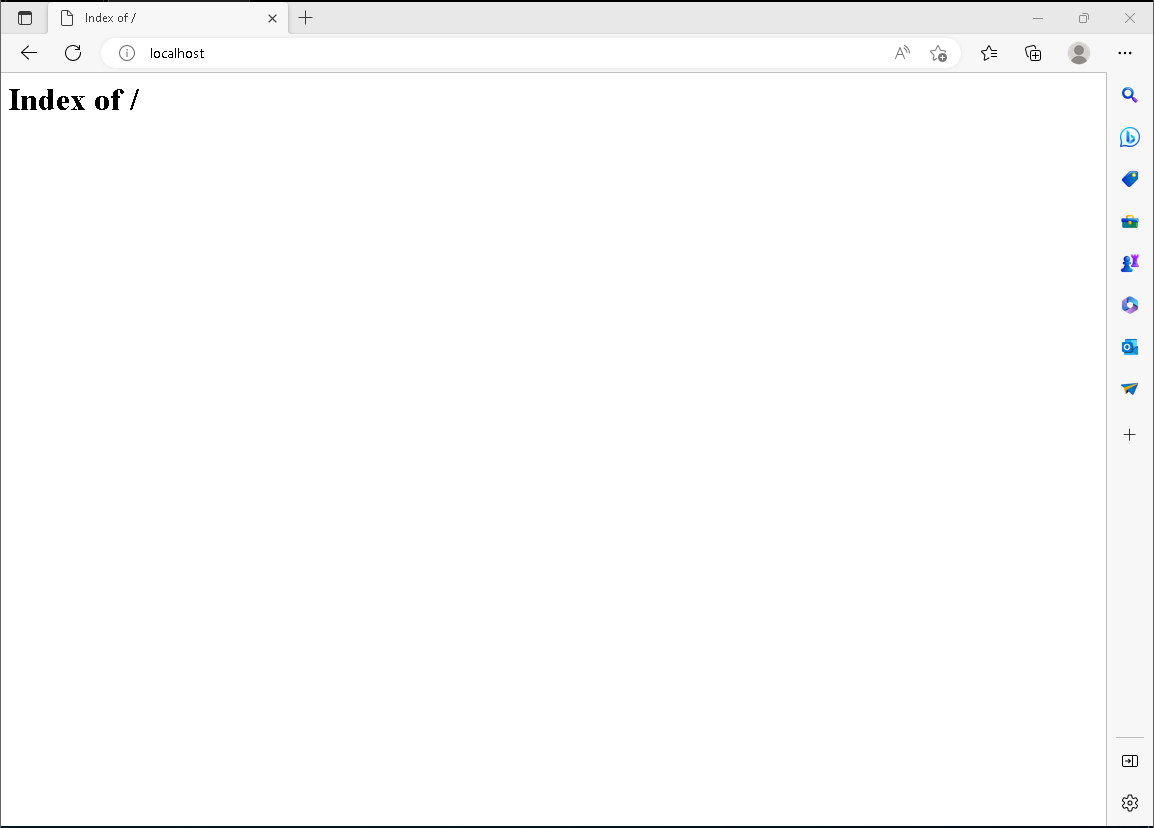
*Рисунок 12 – Иллюстрация атаки TCP SYN-flood с помощью графика Wireshark*



*Рисунок 13 – Иллюстрация атаки TCP SYN-flood с помощью статистических данных*

*иерархии протоколов WireShark*

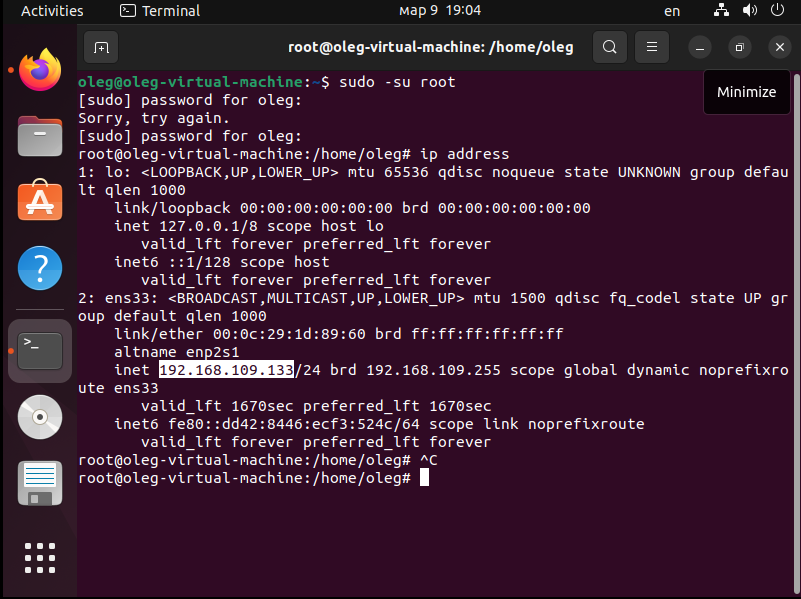
*SYN-flood* атака была проведена успешно, однако сервер продолжил свое функционирование.



*Рисунок 14 – Apache сервер продолжил свою работу*

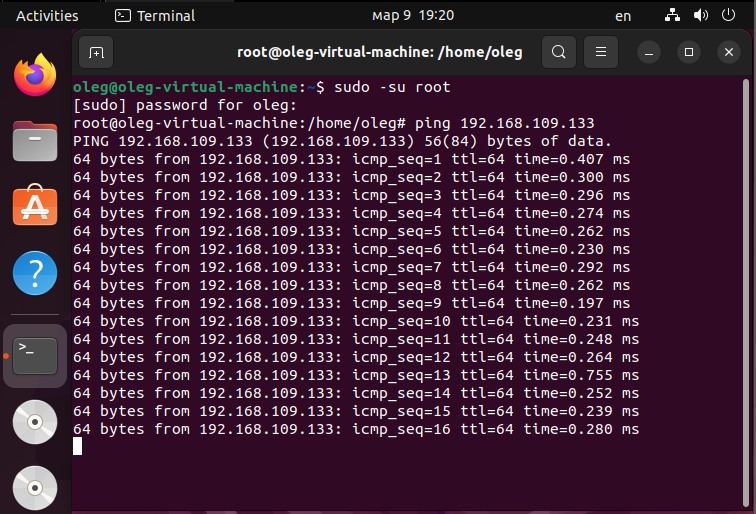
Попробуем провести DOS – атаку при помощи генератора пакетов hping3 в Linux. Для проверки отправим один пакет, чтобы рассмотреть «тройное рукопожатие». Команда для Linux:

~$ sudo hping3 -S -c 1 -s 1023 -p 80 192.168.109.133



*Рисунок 15 – IP адрес атакуемой системы*

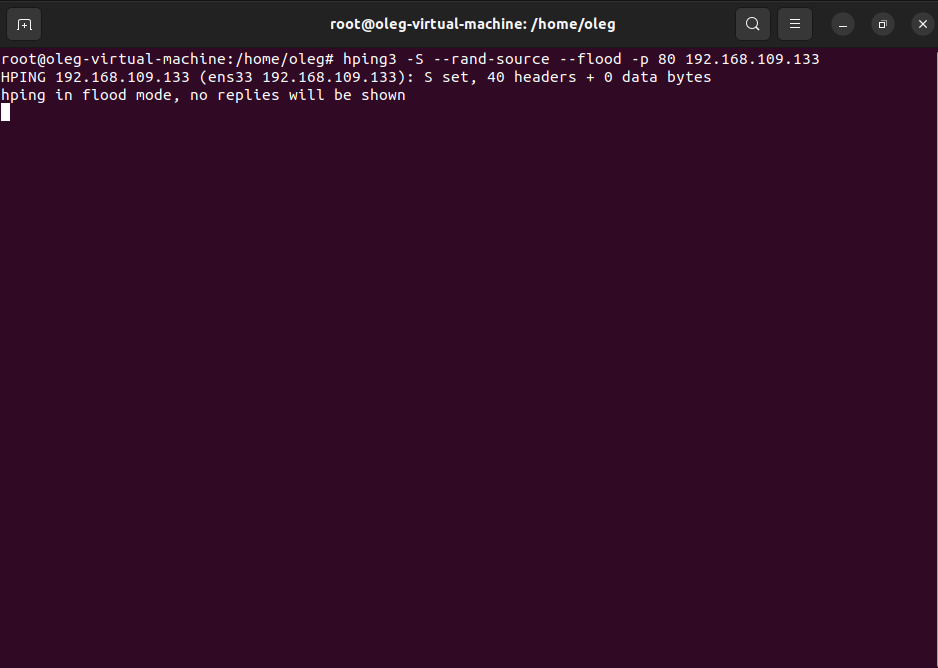
Измерим задержку до «жертвы» до *SYN-flood* атаки.



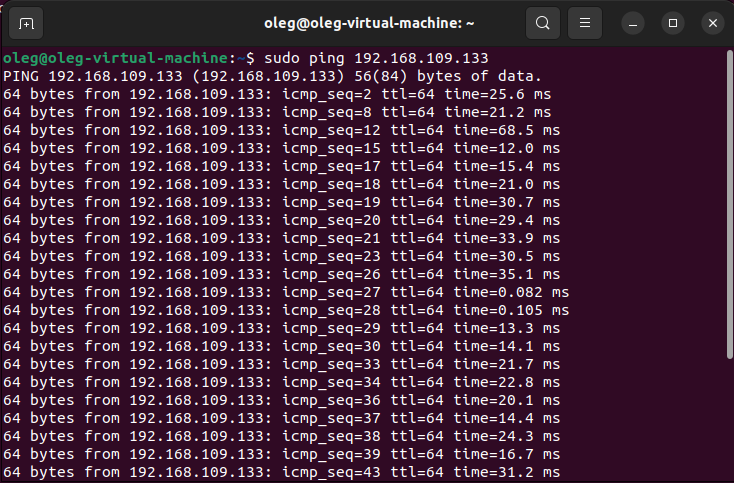
Создадим виртуальный сервер Apache на Linux. Теперь смоделируем SYN-flood на него при помощи hping3 в Linux. Данную операцию удается выполнить с помощью команды:

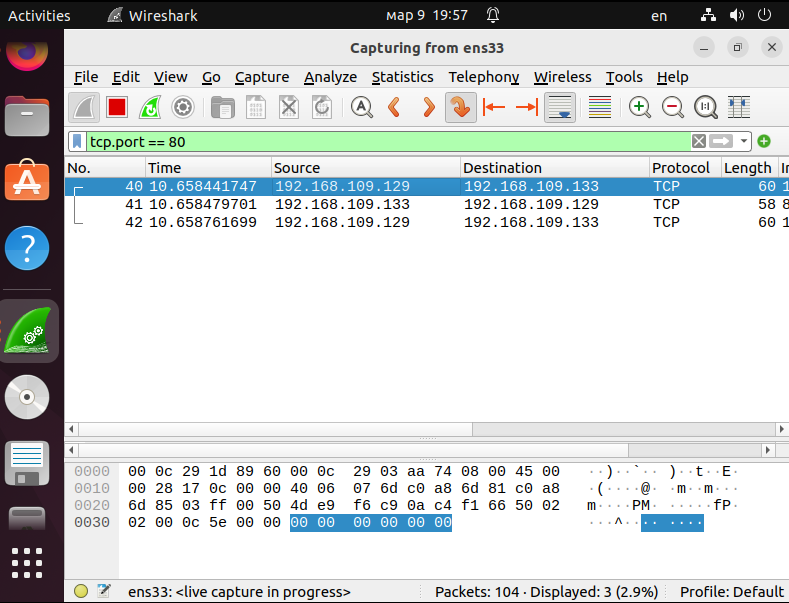
sudo hping3 -S --rand-source --flood -p 80 192.168.109.133

Данная команда отправляет SYN-пакеты. Использован флаг «--flood» для быстрой отправки большого количества пакетов. Флаг «--rand source» генерирует поддельные IP-адреса. В конце указывается IP-адрес атакуемого виртуального сервера.

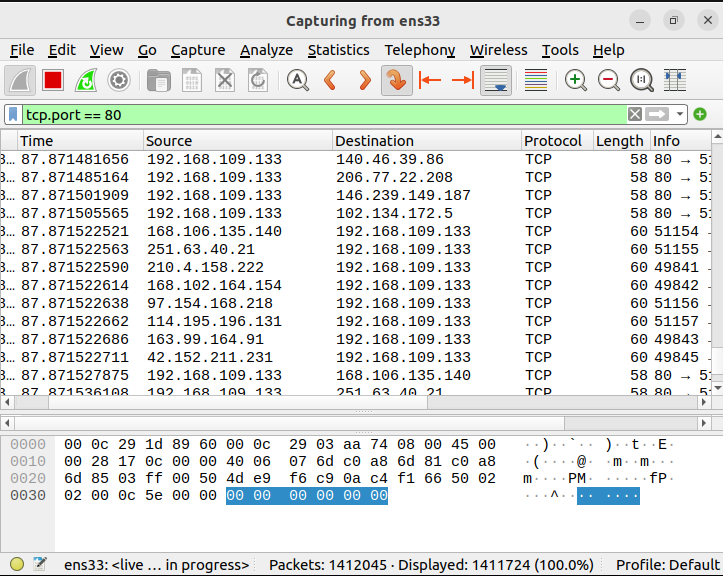


*Рисунок 16 – hping3 для реализации SYN-flood атаки*



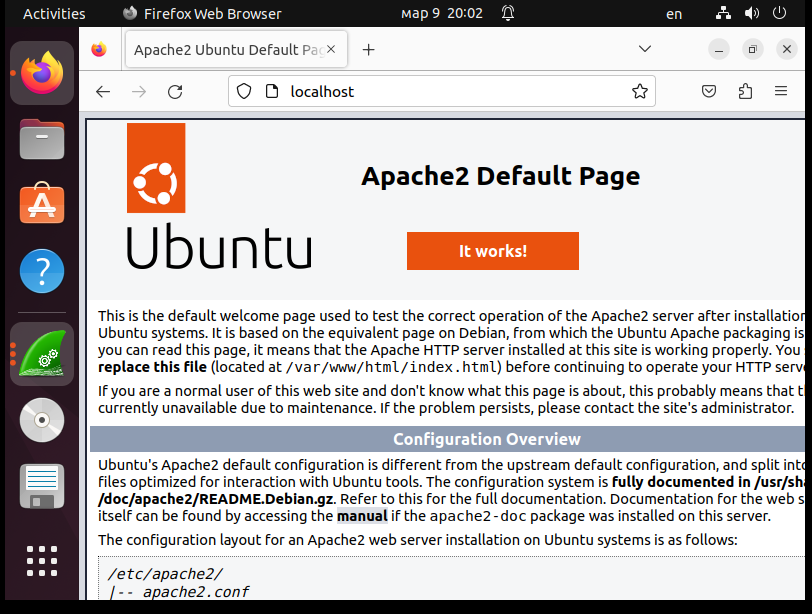


*Рисунок 17 – «тройное рукопожатие» при получении TCP-пакета*

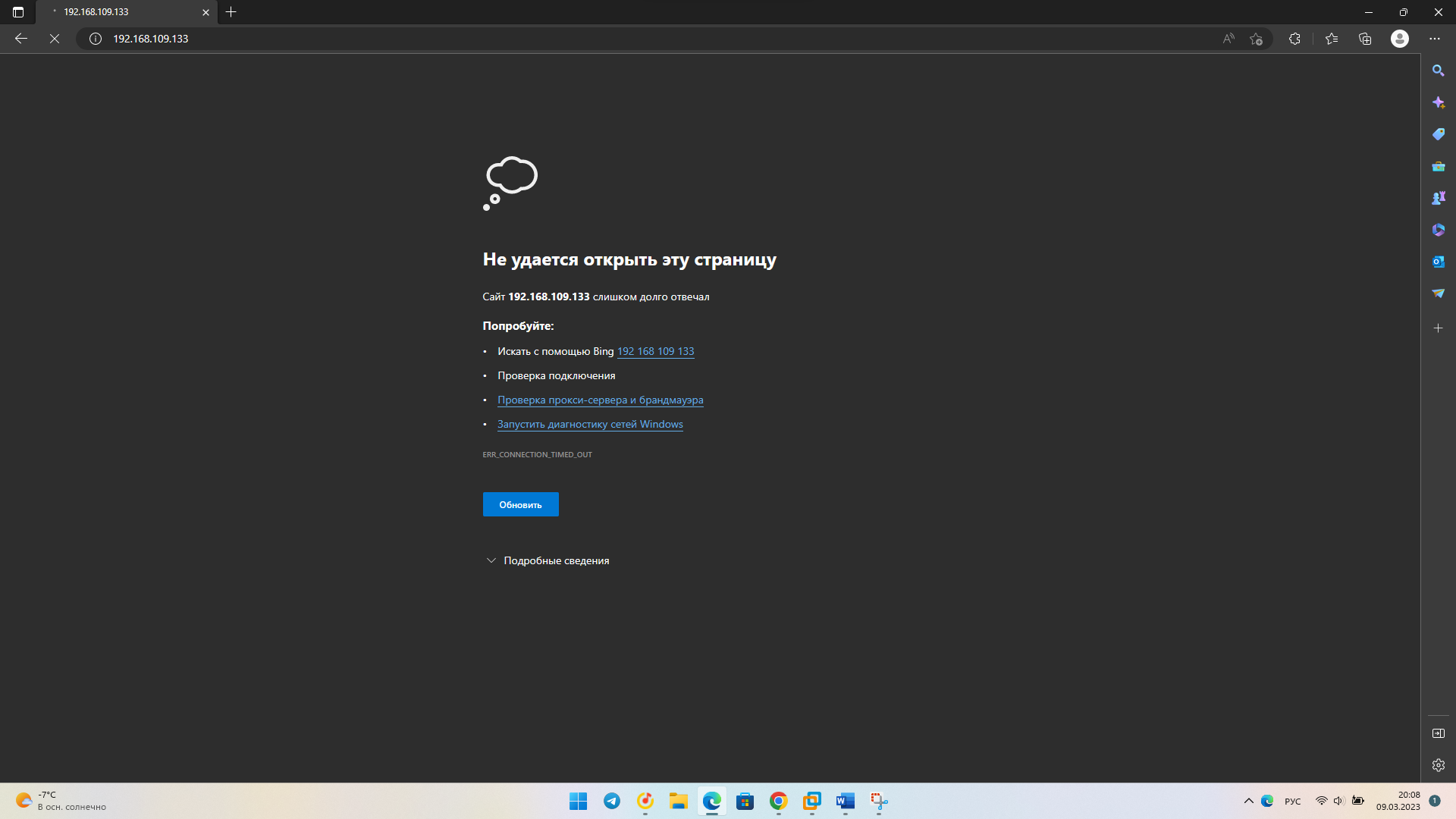


*Рисунок 18– SYN-flood атака*

К сожалению, в этом случае график и статистику SYN-flood атаки получить не удалось, поскольку система зависла и перестала реагировать на нажатия.



*Рисунок 19 – Ubuntu завис*



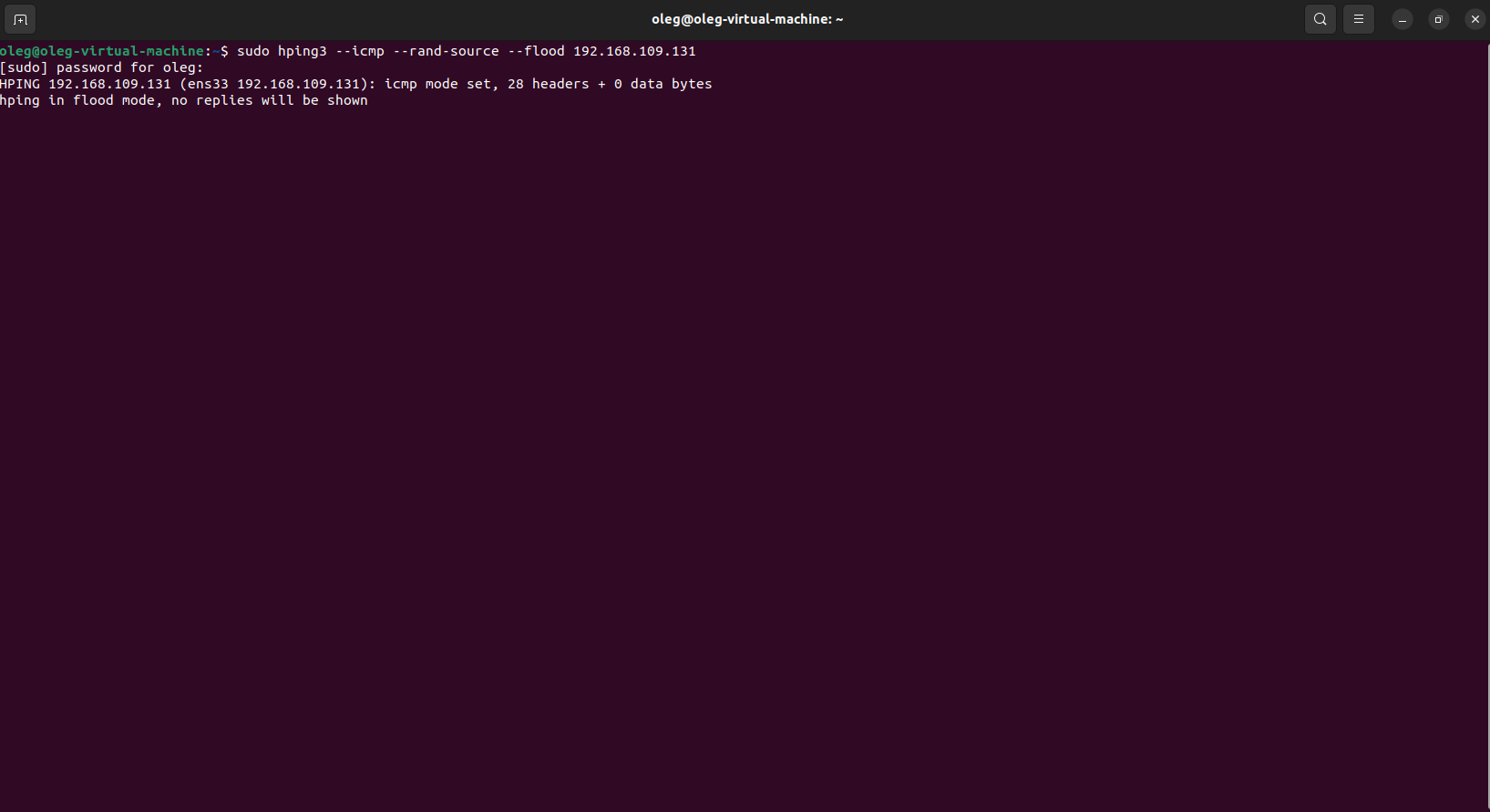
*Рисунок 20 – сервер перестал отвечать на запросы*

Отсюда можно сделать вывод, что для Windows *SYN-flood* атака неэффективна, поскольку она не смогла вывести сервер, основанный на этой операционной системе из работы, а значит защита от данной атаки для нее не требуется. Однако, UNIX – системы подвержены данной атаке, поэтому для таких систем необходимо предпринимать меры по их защите от сетевого влияния.

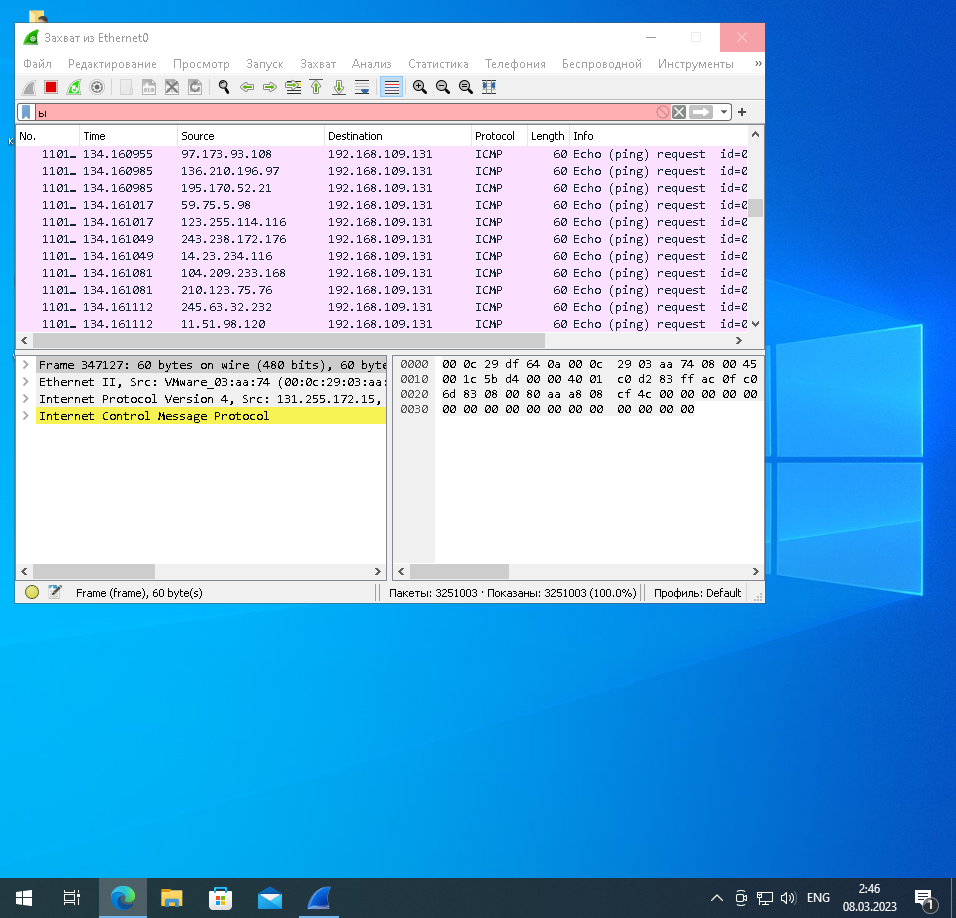
* 1. *ICMP-flood*

Принцип атаки *ICMP-flood* схож с вышеописанной *SYN-flood* атакой*.* Однако в данном случает атакуемый компьютер “забрасывается” пакетами типа ICMP. Поскольку система должна ответить на такие пакеты, создается огромное число ответных пакетов, в результате чего пропускная способность канала снижается.

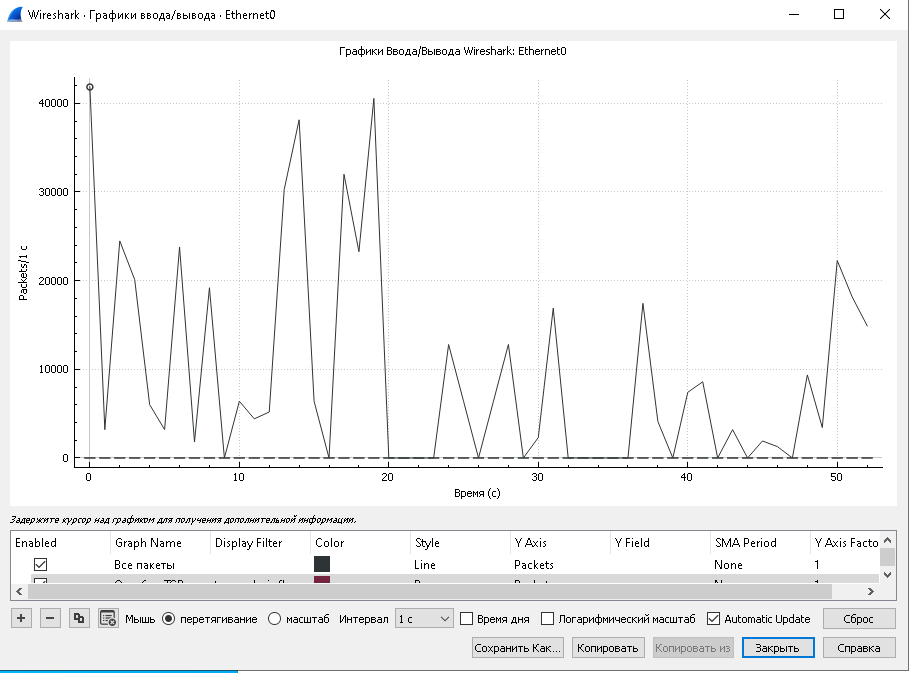
Для проведения атаки использовалась команда в Linux: «sudo hping3 --icmp --rand-source --flood 192.168.109.131». То есть через генератор пакетов hping3 отправляются ICMP-пакеты. Использован флаг «--flood» для быстрой отправки большого количества пакетов. Флаг «--rand source» генерирует поддельные IP-адреса. В конце указывается IP-адрес атакуемого виртуального сервера.



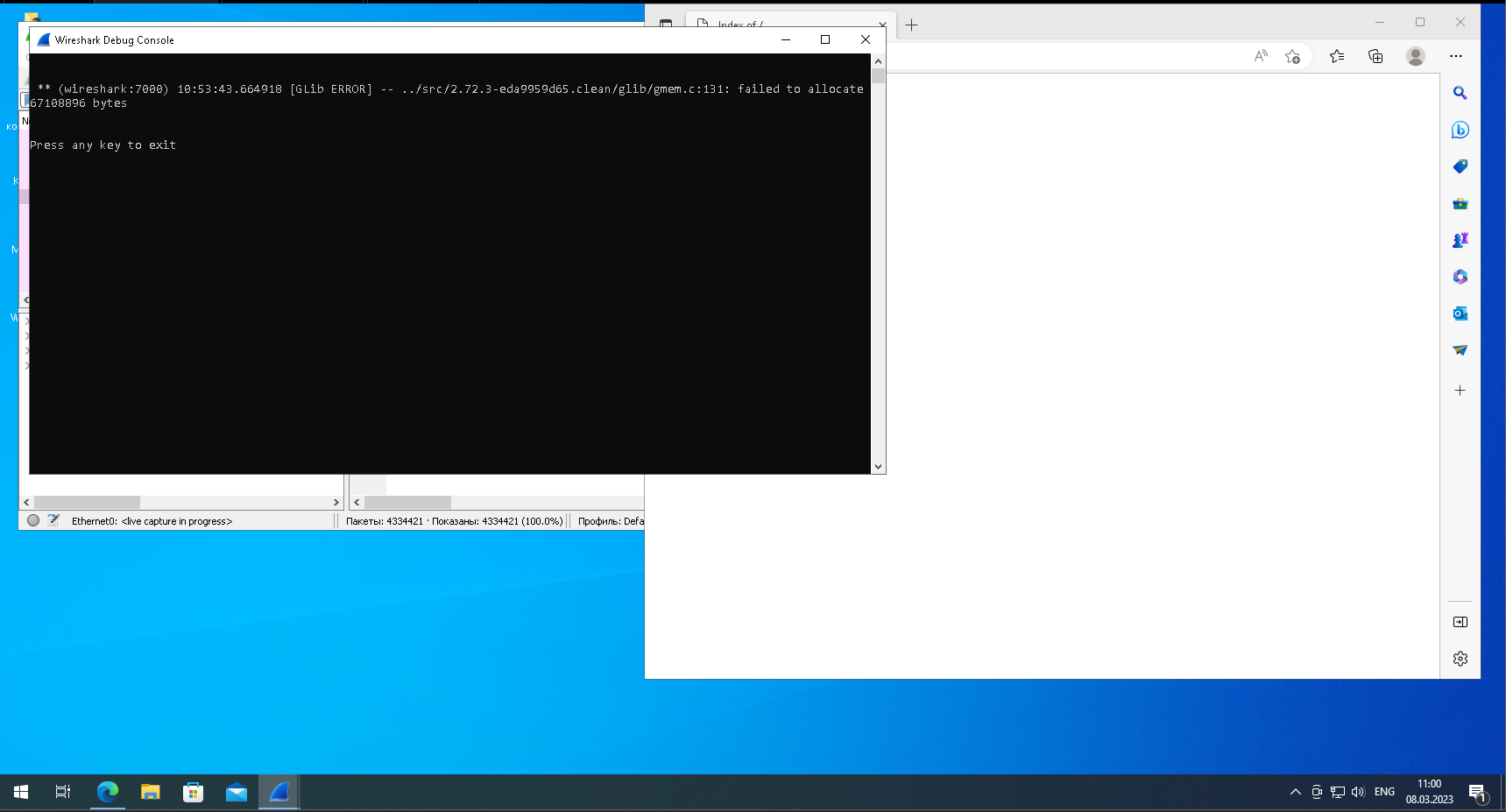
*Рисунок 21 – hping3 для генерации ICMP-flood атаки*



*Рисунок 22 – WireShark зафиксировал атаку*



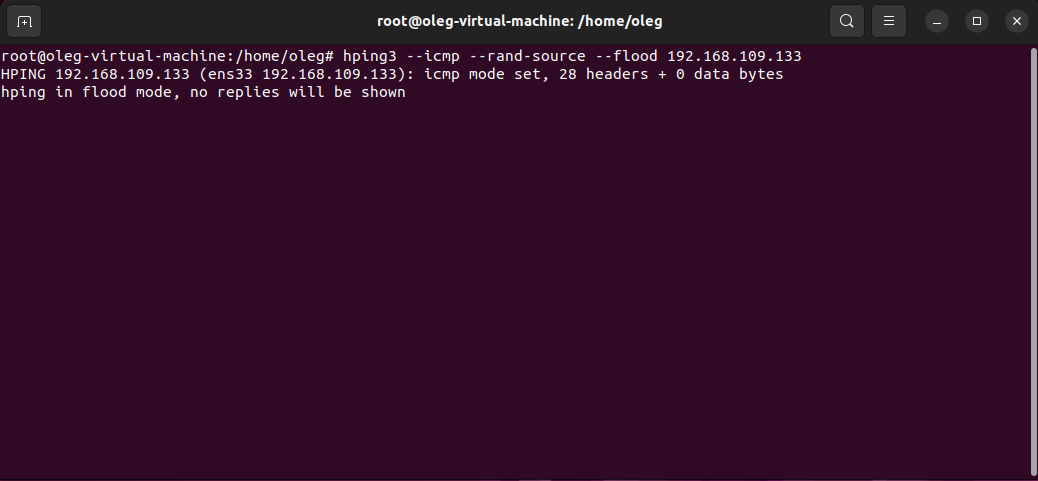
*Рисунок 23 – график ICMP-flood атаки*



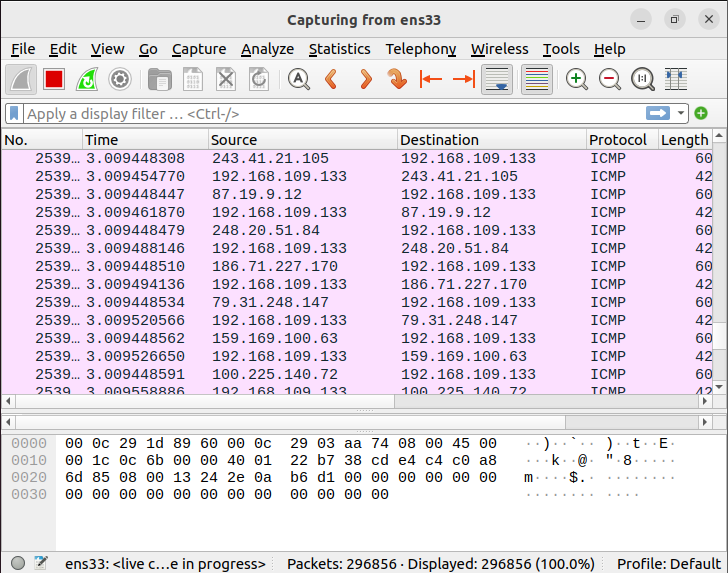
*Рисунок 24 – аварийное завершение работы WireShark*

После получение графика атаки WireShark аварийно завершил работу и производительность атакуемой машины «сильно просела». При всем этом виртуальный сервер остался работоспособным, что свидетельствует об недостаточности данной атаки для вывода сетевого оборудования, основанного на операционной системе Windows из строя.

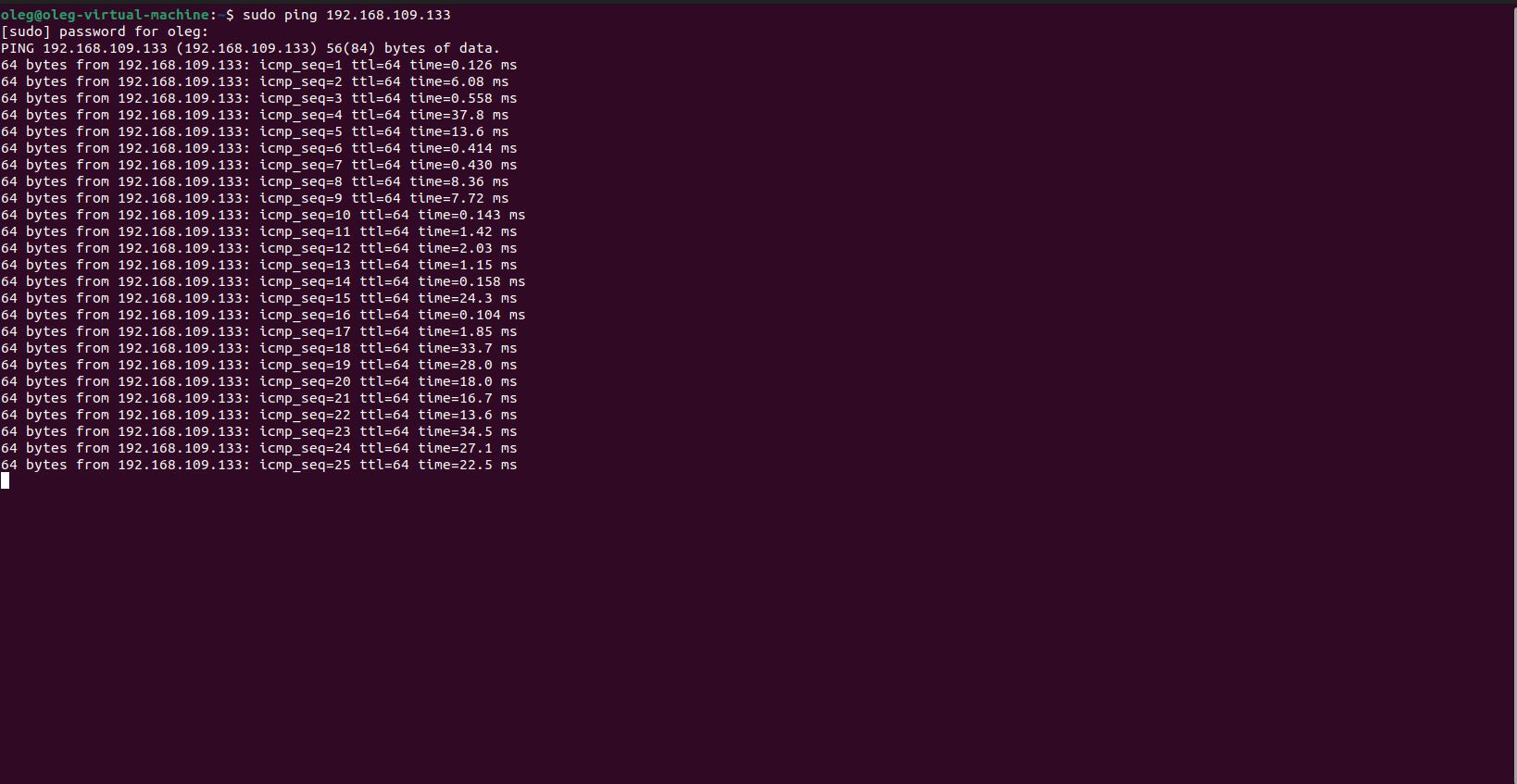
Попробуем сделать тоже самое для UNIX – систем.

****

*Рисунок 25 – ICMP-flood атака через hping3*

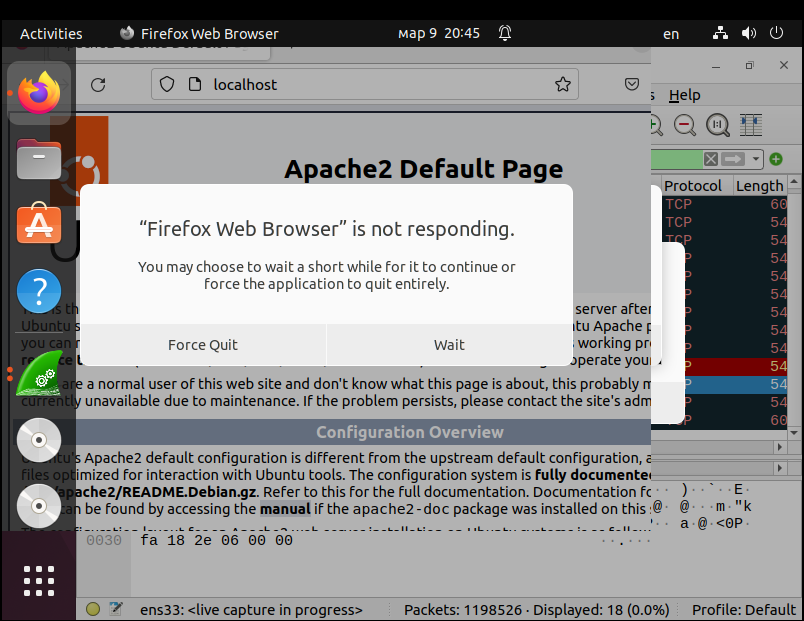


*Рисунок 26 –WireShark вовремя ICMP- flood атаки*

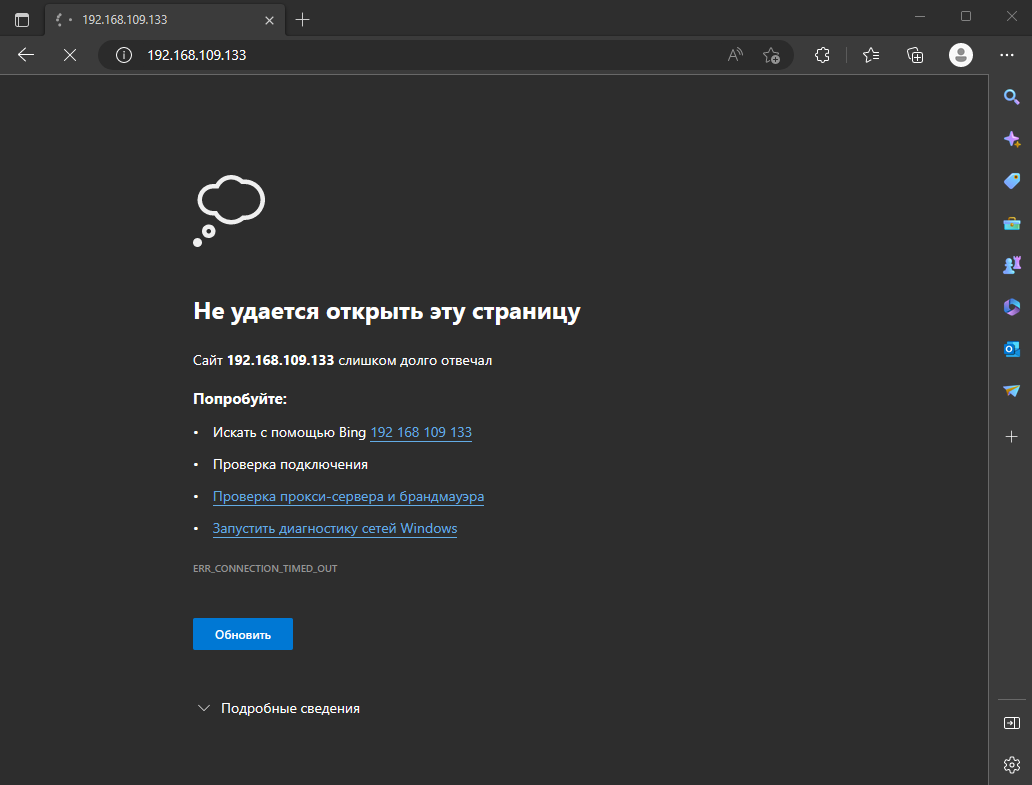


*Рисунок 27 –задержка до сервера вовремя ICMP – flood атаки*

Через некоторое время система начала работать нестабильно



*Рисунок 28 – Linux стал глючить и перестал реагировать на действия пользователя*



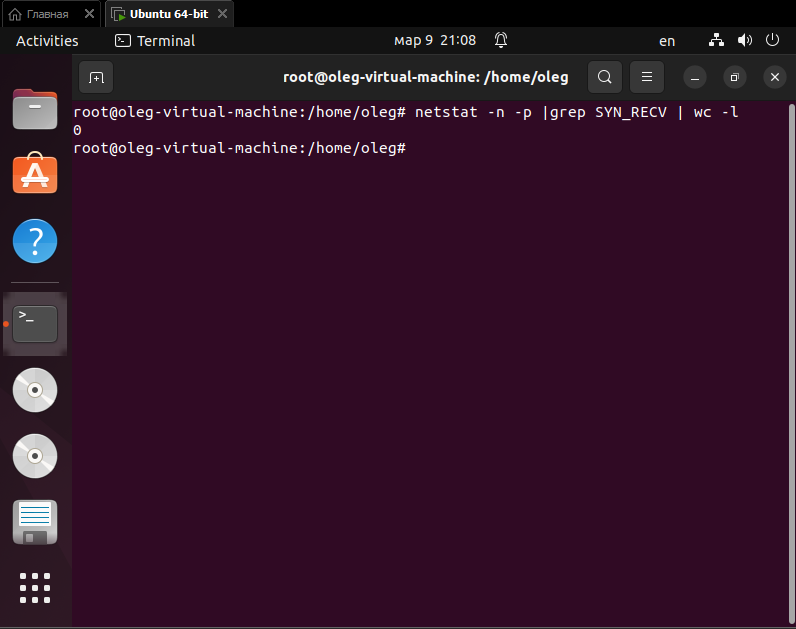
*Рисунок 29 – Сервер перестал реагировать на действия пользователя*

При данной атаке виртуальный сервер перестал функционировать, что говорит о незащищенности Linux от *ICMP-flood* атак.

1. Защита от *SYN–flood* и *ISMP–flood* атак

*3.1 SYN-flood атака*

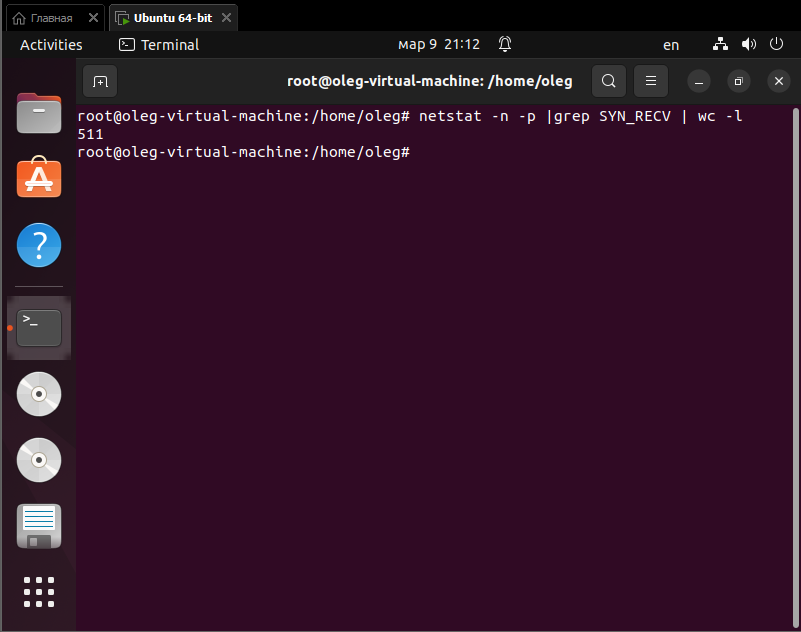
Замеряем количество «полуоткрытых» TCP-соединений в начале эксперимента при помощи netstat -n -p |grep SYN­\_RECV| wc -l

**

*Рисунок 30 - количество "полуоткрытых" TCP-соединений до эксперимента*

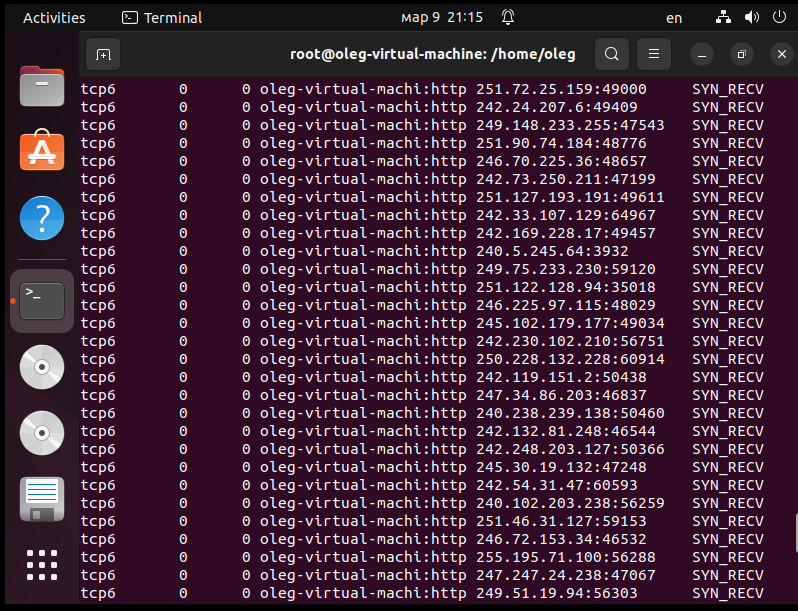
После применения

$ sudo hping3 --icmp --rand-source --flood 192.168.109.133



*Рисунок 31 – Количество «полуоткрытых» TCP – соединений во время эксперимента*

Количество полуоткрытых соединений увеличилось до 511.



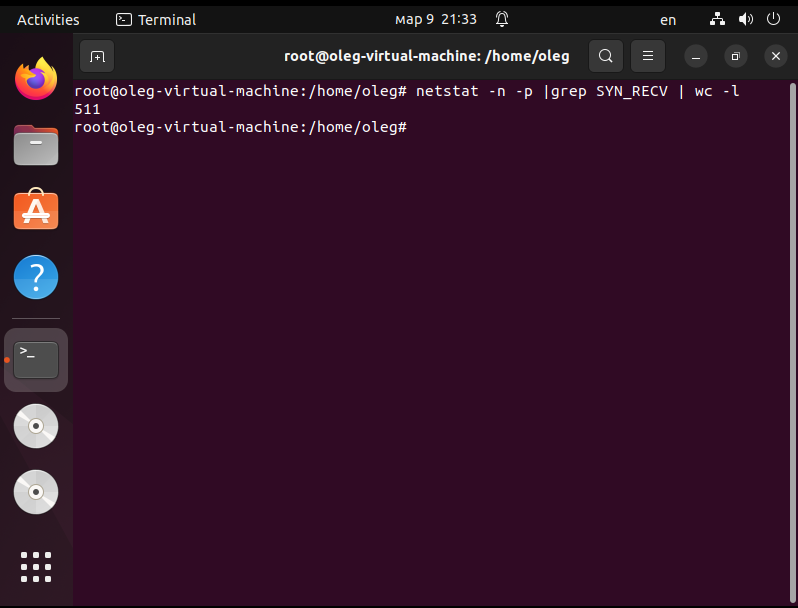
*Рисунок 32 – TCP - подключения во время атаки*

TCP-подключения во время атаки при помощи netstat -a

Отключим очередь «полуоткрытых» TCP – соединений и ограничим максимальное число «полуоткрытых» соединений с одного IP-адреса к конкретному порту через команды

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

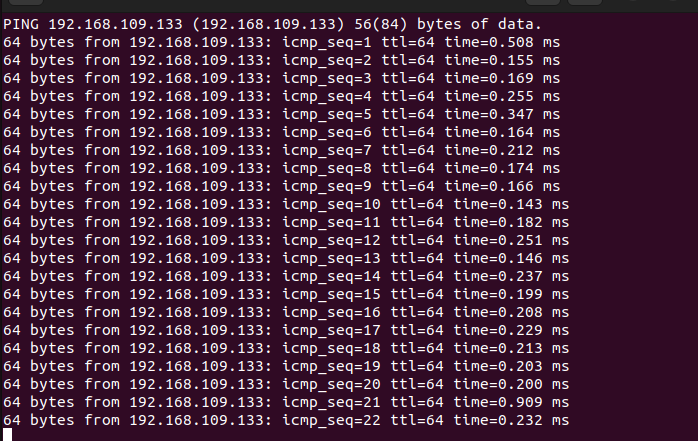
# iptables -I INPUT -p tcp --syn --dport 80 -m iplimit --iplimit-above 10 -j DROP

**

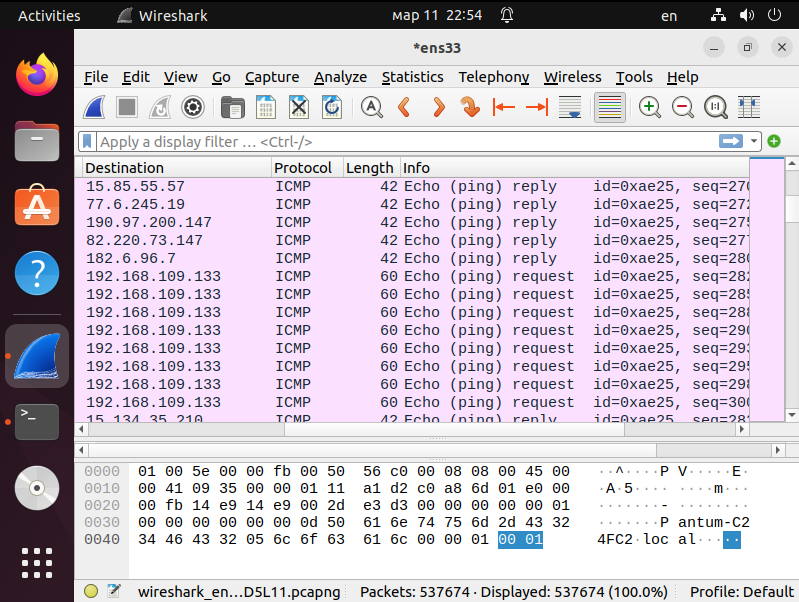
*Рисунок 33 –Количество «полуоткрытых» TCP – соединений во время эксперимента после применения команд*

Данная защита не сработала и количество «полуоткрытых» TCP-соединений не изменилось.

*3.2) ICMP-flood атака*

**

*Рисунок 34 – задержка до сервера до проведения эксперимента*



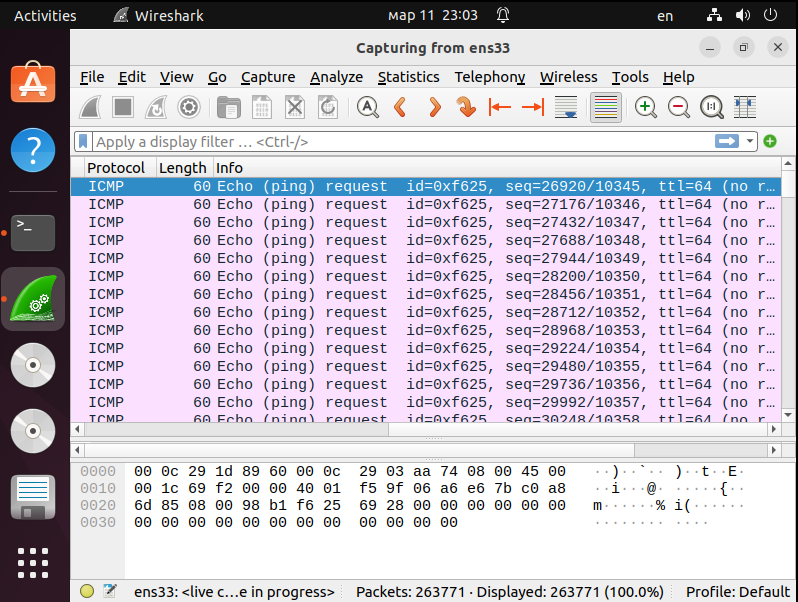
*Рисунок 35 – WireShark вовремя ICMP - атаки*



*Рисунок 36 ­– отключим ответ сервера на запрос*

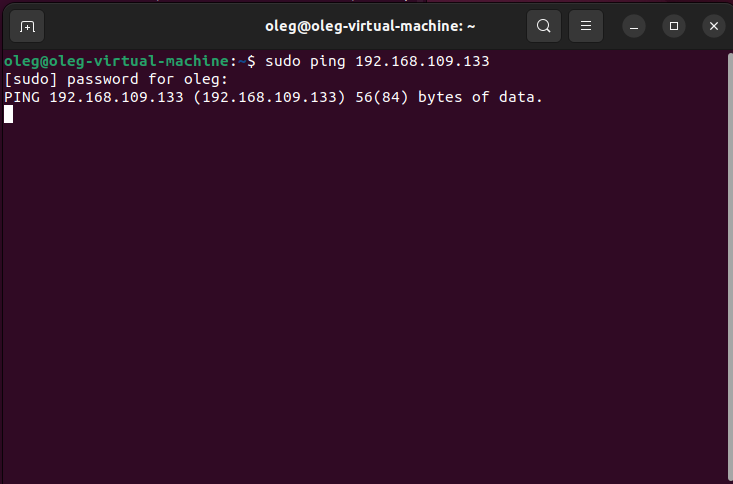
Применим команду отключения ответов на запросы ICMP echo:

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



*Рисунок 37 – Команда сработала и на сервер приходят только запросы*

После применения команды сервер перестал отправлять ответы на запросы, что подтверждает команда ping на атакующей машине:



*Рисунок 38 – задержка до сервера вовремя ICMP-flood атаки*

Следовательно, защита от *ICMP-flood* атаки работает.

Итог: в обоих случаях сервер на UNIX системе остался работоспособным, однако защита от *SYN-flood* атаки неэффективна, что может быть вызвано тем, что обе виртуальные машины подключены к одной локальной сети.

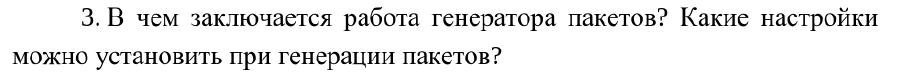
## Контрольные вопросы



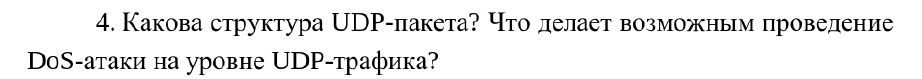
Принцип DOS – атаки основан на идее flood, т.е «затопление» сервера большим количеством сетевых пакета, которые содержат рандомно сгенерированную информацию. Огромное количество сетевых пакетов перегружают буфер жертвы, тем самым выводя ее из строя.



* Для *SYN-Flood* атаки: ограничение максимального числа «полуоткрытых» соединений к конкретному порту.
* Для *ICMP-Flood* атаки: отключение ответа на запросы ICMP echo.
* Для *UDP-flood* атаки: отключение UDP – сервисы и установление ограниченного числа соединений с DNS-сервером.
* Для *HTTP-flood* атаки: увеличение максимального числа одновременных подключений;



Работа генераторов пакетов заключается в создании случайных пакетов или отправить в компьютерную сеть произвольный пакет. При генерации пакетов можно указать тип пакета, количество пакета, IP-адрес источника, режим отправки пакетов (--flood).



Заголовок UDP (*User Datagram Protocol*) состоит из четырех полей, каждое по 2 байта (т.е. 16 бит). Два из них необязательны к использованию в IPv4, в то время как в IPv6 необязателен только порт отправителя. 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.



При проведении ICMP-flood атаки «жертва» создает большое количество ответных пакетов. Если же отключить ответы на запросы ICMP, то ответные пакеты создаваться не будет, то есть повышается пропускная способность канала.

## Выводы

В ходе работы был изучен механизм реализации компьютерной угрозы типа «отказ в обслуживании». Были рассмотрены различные генераторы пактов и их функциональность. Были изучены различные типы пакетов, проведены SYN-flood и ICMP-flood атаки, изучены методы защита от данных атак. Были получены навыки работы с некоторым программами для генерации пакетов, а также с приложением для отслеживания и анализа трафика получаемых и отправленных пакетов. При *SYN-flood* и *ICMP-flood* атаке сервер на Windows продолжил работать, при этом UNIX-сервер перестал функционировать.