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. **ОТКАЗ В ОБСЛУЖИВАНИИ**
2. по дисциплине «Основы информационной безопасности»
3. Выполнил
4. студент гр. 4851003/20001 Федорова А.А.

<*подпись*>

1. Преподаватель

асс. преподавателя Климшин И.И

<*подпись*>

1. **Цель работы**

Изучить компьютерную угрозу типа "отказ в обслуживании", ознакомиться со способами защиты от такого рода угроз.

1. **Постановка задачи**

1) Изучить интерфейсы генераторов пакетов

2) Смоделировать атаку SYN-flood на виртуальный сервер

3) Смоделировать атаку ICMP-flood на виртуальный сервер

4) Организовать защиту от проведённых атак

1. **Теоретические сведения**

## 3.1 Понятие DoS

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 генерируется злоумышленником.

DoS-атака обычно является промежуточным этапом в процессе получения полного контроля над системой или ее вывода из нормального режима функционирования из-за перегрузок.

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.

## Сетевые пакеты

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

Наиболее распространены три типа сетевых пакетов:

ТСР 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;

ICMP-пакет - тип пакета, предназначенного для служебных задач (например, для диагностики сети, выполнения ping) и не используемого для передачи информации.

## Виды DoS-атак

При проведении SYN-flood, атакующий компьютер непрерывно посылает сообщение 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 подключения.

Проведение SYN-flood выявляется, путем числа "полуоткрытых" ТСР-соединений, например:

# netstat -na I grep ":80 " I grep SYN\_RCVD

При нормальном состоянии системы "полуоткрытых" соединений быть не должно, либо их число не должно превышать 1-3.

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

Атака HTTP-flood организована по аналогии с рассмотренными атаками. Целью атаки является web-сервер. При подозрении на HTTP-flood прежде всего следует подсчитать количество процессов web-сервера (например, для web-сервера Apache) и количество соединений на порт 80:

# ps aux grep httpd | wc -1

# netstat -na | grep ":80 " wc - 1

Если значения в несколько раз превышают среднестатистические, то есть основания подозревать HTTP-flood. Далее следует просмотреть список IP-адресов, с которых идут запросы на подключение:

# netstat -na | grep ":80 " | sort | uniq -c | sort -nr | less

Дополнительным подтверждением атаки может стать результат анализа пакетов с помощью утилиты tcpdump:

# tcpdump -n -i eth0 -s 0 -w output. Txt dst port 80 and host

Показателем также может служить большой поток однообразных пакетов с различных IP-адресов, направленных на один порт или сервис (например, на определенный исполняемый скрипт).

Проведение UDP-flood организовано следующим образом. На атакуемый компьютер по широковещательному запросу направляются echo-команды. Затем IP-адрес злоумышленника подменяется на IP-адрес атакуемого. В результате этого атакуемый компьютер получает множество ответных сообщений. Число таких сообщений зависит от числа узлов в сети. UDP-flood приводит к исчерпанию полосы пропускания и затем к полному отказу в обслуживании атакуемого компьютера. Если служба отключена, то будут сгенерированы ICMP-пакеты, что также вызывает отказ в обслуживании.

## Способы защиты от DoS-атак

Рассмотрим некоторые способы защиты от рассмотренных примеров DoS-aтaк. Защита от SYN-flood строится на отключении очереди "полуоткрытых" ТСР-соединений:

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

Ограничение максимального числа "полуоткрытых" соединений с одного IP-адреса к конкретному порту:

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

Для того, чтобы защититься от ICMP-flood необходимо отключать ответы на запросы ICMP echo:

# sysctl 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

Для защиты от HTTP-flood следует увеличить одновременное количество максимальных подключений к базе данных сервера, установив перед web-сервером более производительный web-сервер Nginx для кэширования запросов.

Защита от UDP-flood заключается в том, чтобы отключить UDP-сервисы и установить ограничение на число соединений с DNS-сервером:

# iptables -I INPUT -p udp –dport 53 -j DROP -m iplimit –iplimit –iplimit-above 1

## Дополнительные рекомендации по защите от DoS-атак

Все серверы, имеющие доступ во внешнюю сеть, должны быть подготовлены к удаленной аварийной перезагрузке.

Программное обеспечение сервера всегда должно быть обновленным;

Использование межсетевых экранов позволяет блокировать конкретный поток трафика, но не позволяют отделить полезный трафик от флуда. АСL-списки фильтруют второстепенные протоколы и не затрагивают протокол ТСР.

1. **Ход работы**

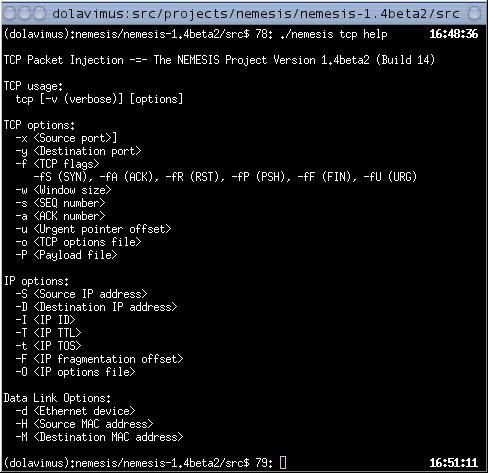
**1. Изучение генераторов пакетов:**

Рисунок 1 – интерфейс Nemesis

1) Nemesis (рисунок 1) – консольное приложение, генерирующее пакеты.

Позволяет собирать любые пакеты следующих протоколов: ARP, DNS, Ethernet, ICMP, IGMP, IP, OSPF, RIP, TCP, UDP.

2) Colasoft Packet Builder (рисунок 2) – приложение, позволяющее не только создавать пакеты, но и проверять защиту своей сети. Можно выбрать один из предоставленных шаблонов:  Ethernet-пакет , ARP-пакет , IP-пакет , TCP-пакет и UDP-пакет , а также изменить параметры в редакторе декодера, шестнадцатеричном редакторе или редакторе ASCII для создания пакетов.

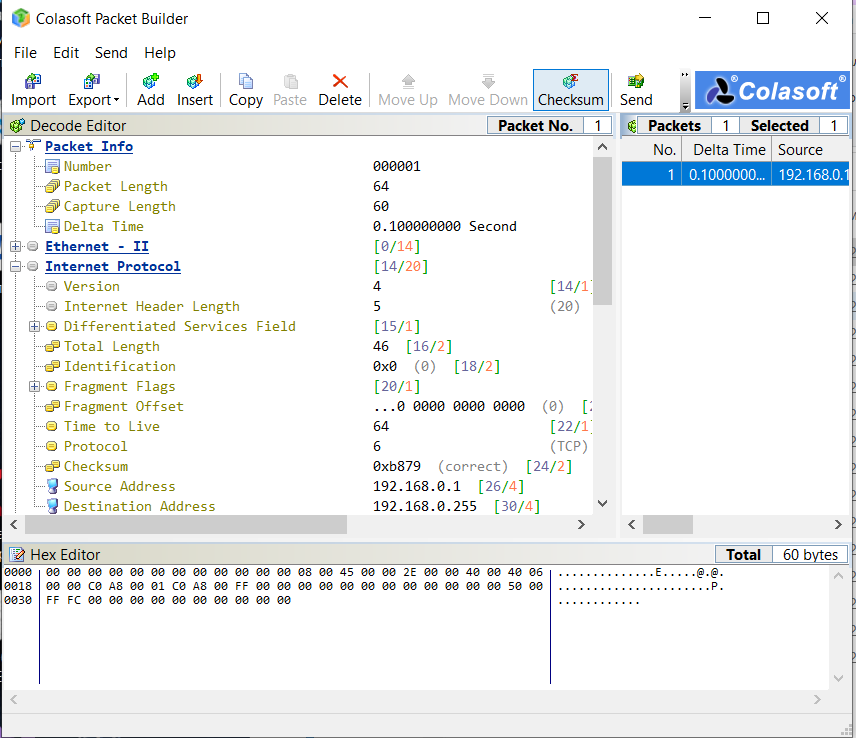
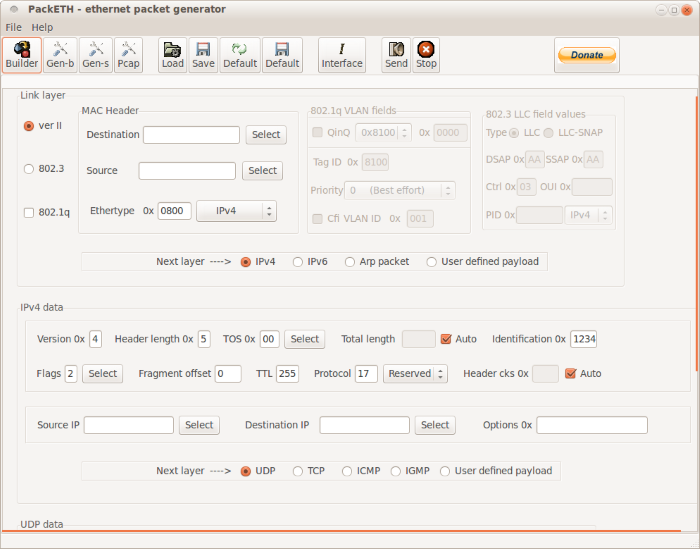


Рисунок 3 – интерфейс packETH

Рисунок 2 – интерфейс Colasoft packet builder

3) packETH (рисунок 3) – генератор пакетов Ethernet. Он позволяет создавать и посылать любые возможные пакеты или последовательности пакетов в сеть Ethernet. Поддерживает пакеты: UDP, TCP, ICMP, ICMPv6, IGMP, а также ARP, IPv4, IPv6 уровни.

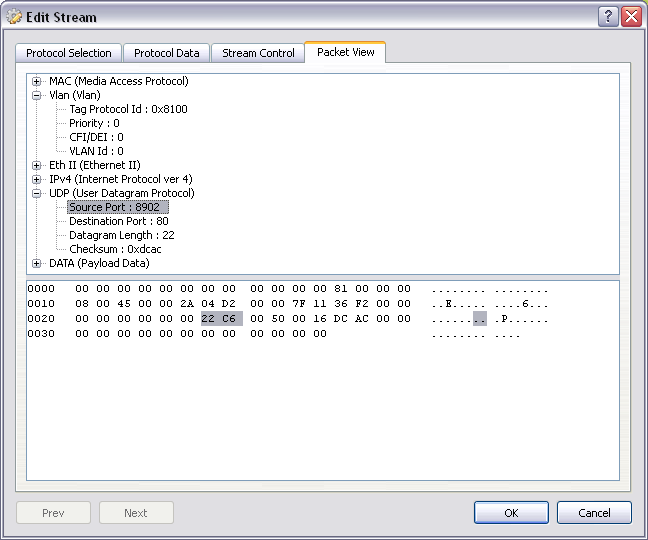
4) Ostinato – это универсальный разработчик пакетов. Поддерживает TCP, UDP, ICMPv4, ICMPv6, IGMP, MLD пакеты. Поддерживает ARP, IPv4, IPv6, IP-in-IP или IP-туннелирование.

Рисунок 4 – интерфейс Ostinato

# 2. Установка веб-сервера Apache

Apache доступен в репозиториях программного обеспечения Ubuntu по умолчанию, и поэтому его можно установить с помощью стандартных инструментов управления пакетами.

Для начала выгрузим указатель локальных пакетов, чтобы отразить последние изменения на предыдущих уровнях:

# sudo apt update

Затем установим пакет apache2:

# sudo apt install apache2

Выведем список профилей приложений ufw, введя следующую команду:

# sudo ufw app list

Output

Available applications:

Apache

Apache Full

Apache Secure

OpenSSH

Рисунок 5 – список профилей приложений

Выберем **Apache**: этот профиль открывает только порт 80 (нормальный веб-трафик без шифрования)

# sudo ufw allow 'Apache'

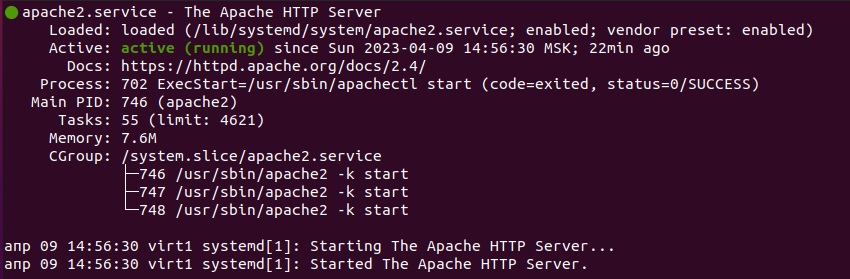


Рисунок 6 – статус сервера

**3. Проведение атаки SYN-flood.**

* **SYN-flood атака**

TCP-соединение строится из 3 этапов:

1. Узел А посылает пакет узлу В, установив в нем значение бита SYN =1.

2. Узел В создает структуры данных для установки соединения. Узел В отвечает на запрос соединения, направляя узлу А пакет с флагом ACK = 1, и тем самым подтверждая прием пакета от узла А. Флаг SYN = 1 в этом втором пакете, 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 ACK.

SYN-flood строится на создании большого количества полуоткрытых TCP соединений, то есть 3 шаг не выполняется. Для реализации этого была использована утилита hping3. Были выбраны такие параметры: -S – флаг SYN, -w 64 – размер TCP окна, -p 80 означает 80 порт, -d 120 устанавливает размер пакета 120 байт, --rand-source подменяет адрес источника на случайный, --flood позволяет отправлять пакеты с максимально возможной скоростью. Последний параметр - ip-адрес цели. В результате сервер перестаёт отвечать в течение 3-х секунд. Скорость передачи пакетов порядка 70000 в секунду, то есть было отправлено порядка 210000 пакетов для вывода из строя.

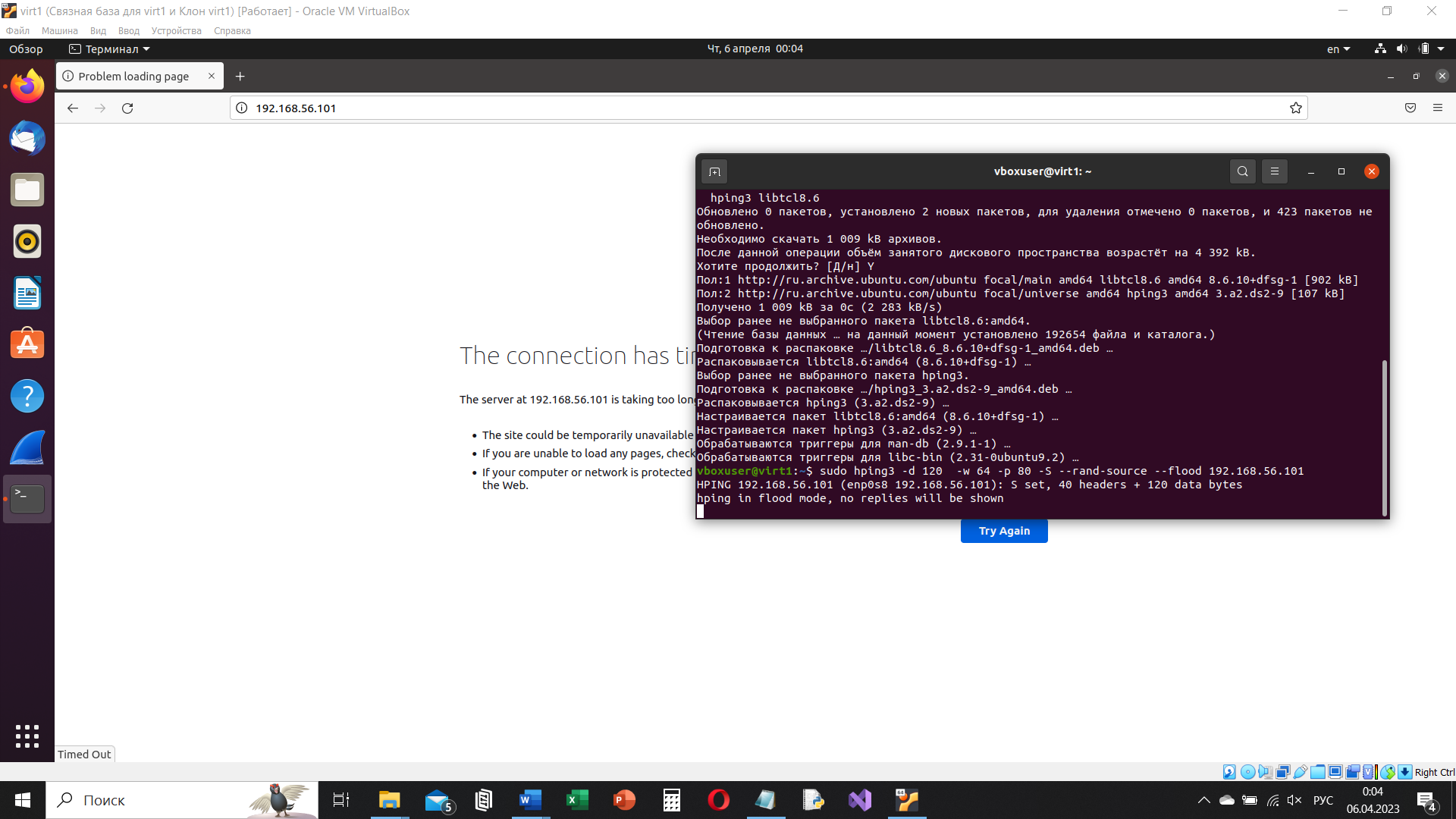


Рисунок 6 – последствия атаки

* **SYN-flood защита**

Для защиты от SYN-flood, на атакуемой системе была уменьшена очередь полуоткрытых TCP-соединений. Для этого в консоли вводится команда «sysctl -w net.ipv4.tcp\_max\_syn\_backlog=100». После, ограничивается максимальное число полуоткрытых соединений, для этого вводится «iptables -I INPUT -p tcp --syn --dport 80 -m connlimit --connlimit-above 10 -j DROP».

**4. Проведение атаки ICMP-flood**

* **ICMP-flood атака**

Идея состоит в том, что сервер обязан отвечать на ICMP-пакеты, таким образом при большом количестве пакетов пропускная способность сервера значительно снижается.

ICMP-flood проводится с помощью команды ping (рисунок 8), которая получает время ожидания ответа на запрос. Были добавлены параметры: -f – отправление запросов без задержки и ip-адрес цели. В результате атаки скорость загрузки страницы снизилась с доли секунды до нескольких секунд, но сервер не переставал отвечать. После завершения атаки загрузка страницы происходила снова за долю секунды.

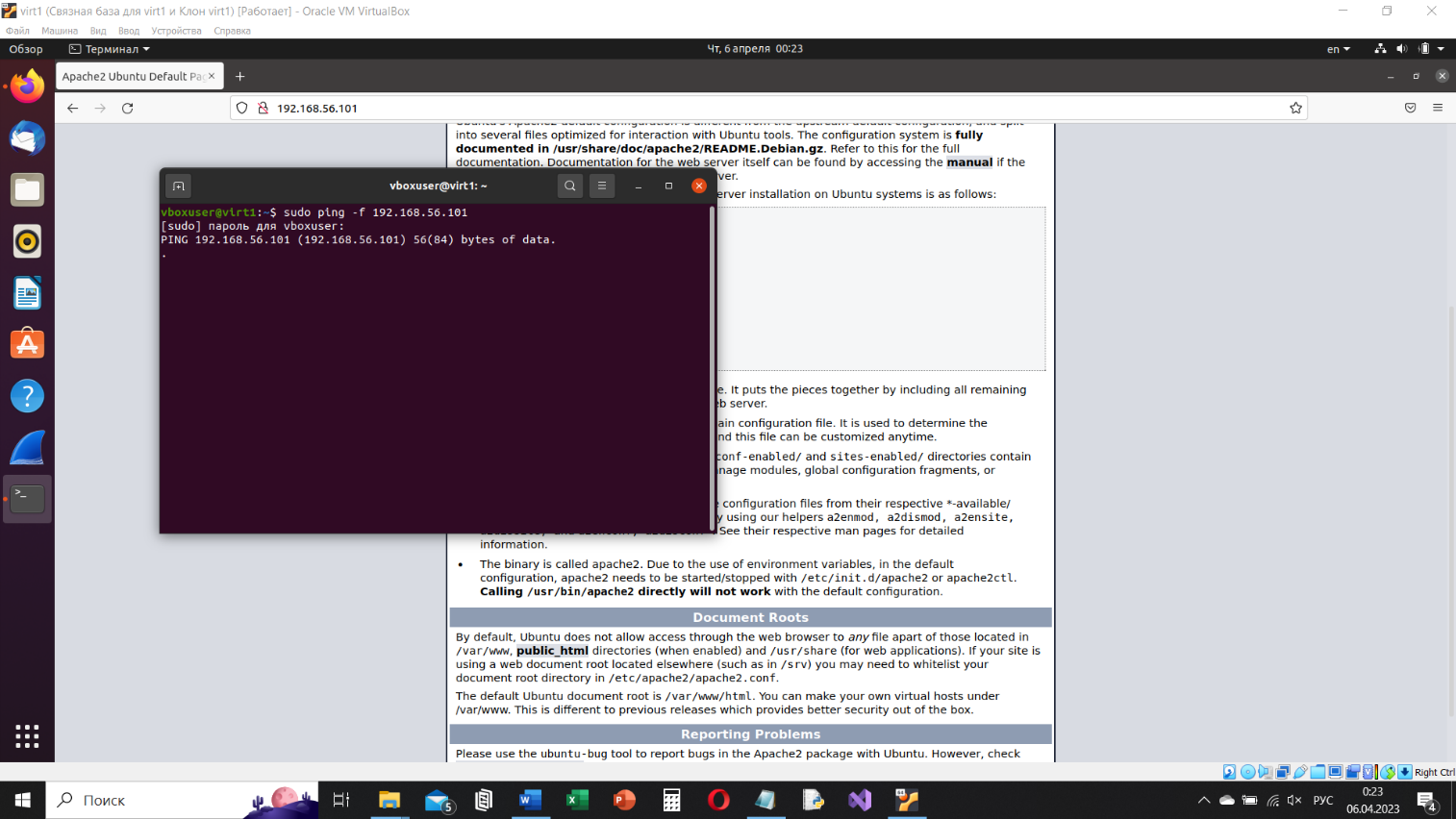


Рисунок 7 – последствия атаки ICMP-flood

* ICMP-flood – защита

Для защиты от ICMP-flood, при помощи консольной команды «sysctl net.ipv4.icmp\_echo\_ignore\_all=1», были отключены ответы на запросы ICMP echo.

1. **Выводы**

В ходе работы получены базовые навыки работы с сервером, с генераторами пакетов и их функционалом. Исследованы механизмы различных DoS-атак и способы защиты от них. Проведены 2 атаки на виртуальный сервер – SYN-flood и ICMP-flood. Получены знания о том, как отправка пакетов может использоваться злоумышленниками для увеличения нагрузки на сервер и как этому противостоять. Противостоять DoS-атаке также можно, фильтруя проходящие через межсетевой экран пакеты. Если обнаружено много однотипных входящих пакетов, можно сделать вывод что от пользователя, пославших их, ведётся DoS-атака.

*Контрольные вопросы:*

1)Dos-атака призвана забрать бóльшую часть вычислительной мощности сервера, чтобы тот не смог обслуживать остальных пользователей.

2)Защита от атаки SYN-flood реализуется путём уменьшения времени ожидания подтверждения подключения, то есть полуоткрытые соединения закрываются быстрее и загрузить сервер становится сложнее.

Защита от ICMP-flood реализуется путём отключения ответа сервера на входящие запросы, таким образом сервер никак не реагирует на любые входящие ICMP-пакеты.

3)Генератор пакетов формирует файл, который содержит в себе всю необходимую информацию в определённом виде, понятном для сервера. Исходя из данных, записанных в пакете, сервер может совершать те или иные действия.

В генераторе пакетов можно установить протокол пакета: tcp, icmp, udp и т.д., также можно установить адрес и порт отправителя и получателя, установить необходимые флаги и задать размер пакета.

4)Проведение UDP-flood организовано следующим образом. На атакуемый компьютер по широковещательному запросу направляются echo-команды. Затем IP-адрес злоумышленника подменяется на IP-адрес атакуемого. В результате этого атакуемый компьютер получает множество ответных сообщений. Число таких сообщений зависит от числа узлов в сети. UDP-flood приводит к исчерпанию полосы пропускания и затем к полному отказу в обслуживании атакуемого компьютера. Если служба echo отключена, то будут сгенерированы ICMP-пакеты, что также вызывает отказ в обслуживании.

5) При ответе на ICMP-пакеты сервер тратит свои ресурсы на ответ, при отключении запросов сервер не будет тратить ресурсы, таким образом атаку организовать не получится.