Министерство науки и высшего образования Российской Федерации

Федеральное государственное автономное образовательное учреждение высшего образования

«Санкт-Петербургский политехнический университет Петра Великого»

—

Институт компьютерных наук и кибербезопасности

**Высшая школа кибербезопасности**

**ЛАБОРАТОРНАЯ РАБОТА №14**

**Защита от угроз нарушения безопасности типа "Отказ в обслуживании"**

по дисциплине «ОИБ или Структуры данных»

Выполнили

студенты гр. 5131001/30002 Мишенев Н. С.

Квашенникова В. М.

<*подпись*>

Руководитель

программист Вагисаров В. Б.

<*подпись*>

Санкт-Петербург

2024г.

**СОДЕРЖАНИЕ**

[ЦЕЛЬ РАБОТЫ 3](#_Toc1455801405)

[ХОД РАБОТЫ 3](#_Toc1980766336)

[ВЫВОД 15](#_Toc1590371951)

**ЦЕЛЬ РАБОТЫ**

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

**ХОД РАБОТЫ**

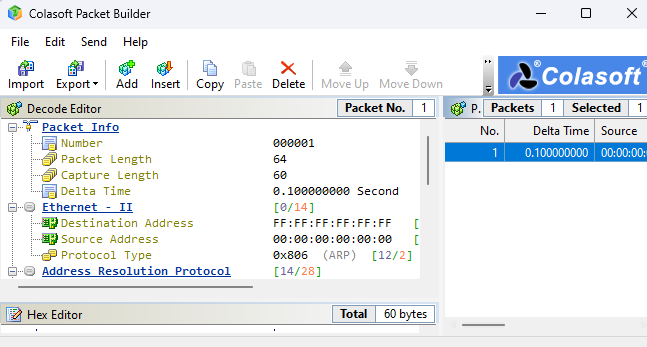
1. **Описание возможностей исследованных генераторов пакетов.**

**a. Nemesis**

Это утилита для создания и внедрения сетевых пакетов различных типов (например: ARP, DNS, ETHERNET, ICMP, IGMP, IP, OSPF, RIP, TCP, UDP). Данная программа является утилитой командной строки и не имеет интерфейса и в основном получила распространение среди Unix-систем, так же хорошо подходит для тестирования сетевых систем обнаружения вторжений, брандмауэров.

**b. Colasoft Packet Buidler**

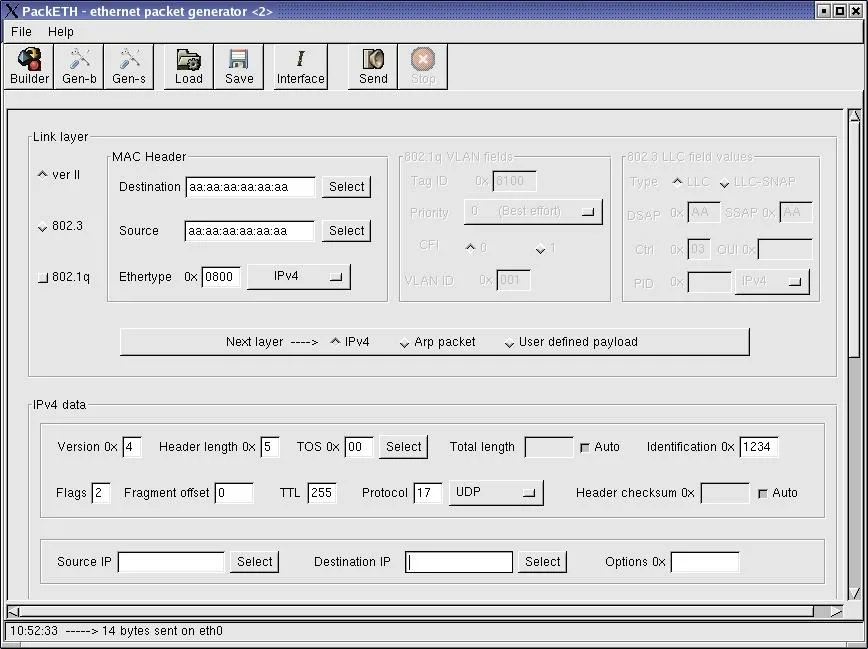
Эта программа позволяет создавать пользовательские сетевые пакеты. Пользователи могут использовать этот инструмент для проверки своей сетевой защиты на прочность, проводя различные атаки. ***Colasoft Packet Builder*** включает в себя очень мощную функцию редактирования пользовательских пакетов, их сохранения и последующего использования. Кроме того, данная утилита имеет редактор декодирования (***Hex Editor***).



*рис. 1. Интерфейс программы Colasoft Packet Builder*

**c. PACKETH**

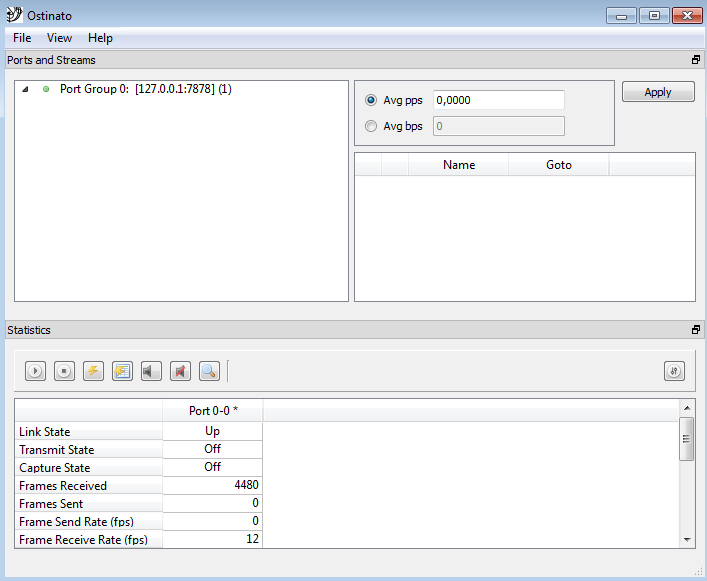
Это генератор пакетов с **GUI** и **CLI** для Ethernet. Он позволяет создавать и отправлять любые возможные пакеты или их последовательности по каналу Ethernet. Он очень прост в использовании, но тем не менее, очень мощный и поддерживает множество различных настроек при отправке.



*рис. 2. Интерфейс программы PACKETH*

**d. ostinato**

Это универсальный обработчик сетевых пакетов и генератор трафика с интуитивно понятным и дружественным графическим интерфейсом, позволяющий создавать и отправлять пакеты различных протоколов с любыми значениями полей этих пакетов, отправлять трафик с требуемой скоростью, выбирать его размер, а также отправлять несколько потоков трафика – последовательно или же вместе.



*рис. 3. Интерфейс программы Ostinato*

1. **Описание механизмов атак SYN-flood и ICMP-flood на виртуальный сервер.**

Все действия проводились на виртуальных машинах, с установленным дистрибутивом ***Debian.*** Эти виртуалные машины были подключены к одному ***Ethernet*** адаптеру, получили свои ***IPv4*** адреса и ***“пинговались”*** друг другом, а также исходной машиной.

Для моделирования ***SYN-flood*** и ***ICMP-flood*** атак была использована утилита ***hping3.***

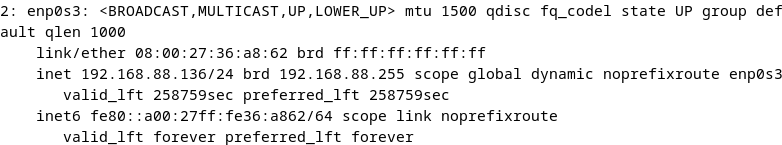
**a. SYN-flood**

Суть такой атаки заключается в безостановочной отправке пакетов с установленным ***SYN*** флагом и неверном обратным IP адресом. Таким образом, атакуемая машина, отправив пакет на неверный IP адрес, указанный в пакете, не дождется ответа и будет вынуждена затрачивать свои ресурсы на ожидание. Этой особенностью установки соединения и пользуются атаки типа ***SYN-flood***.

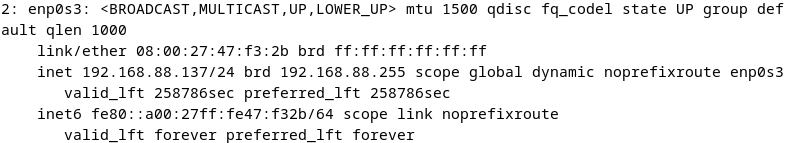
Для начала узнаем IP адреса атакующей и атакуемой машин. В установленном дистрибутиве Debian это можно сделать с помощью команды.

sudo ip addr

Атакуемая машина имеет IP адрес **192.168.88.137**, а атакующая **192.168.88.136**.



*рис. 4. IP адрес атакующей машины*



*рис. 5. IP адрес атакуемой машины*

Атака будет проводиться с помощью утилиты ***hping3***, с помощью такой команды

hping3 -c 10000 -d 90 -p 80 -S --flood --rand-source 192.168.88.137

Где:

-c 10000 - количество пакетов,

-d 90 - размер одного пакета,

-p 80 - атакуемый порт,

-S - установка SYN флага,

--flood - максимально быстрая отправка пакетов

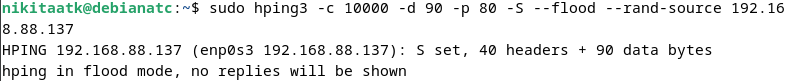
--rand-sources - имитация различных точек отправки

Далее, подготовим атакуемую машину к отслеживанию входящих пакетов с помощью утилиты ***tcpdump*** введя следующую команду

sudo tcpdump -i enp0s3 tcp and host 192.168.88.137

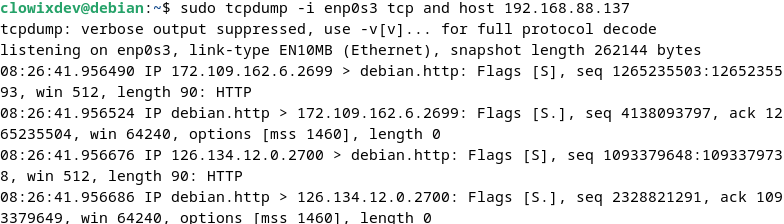
С ее помощью мы сможем отслеживать TCP пакеты направленные на атакуемую машину.

После начала проведения атаки, мы можем увидеть соответствующее сообщение в консоли атакующей машины



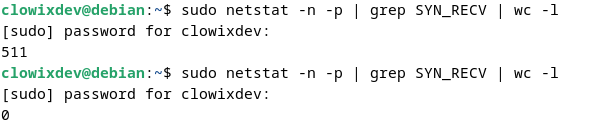
*рис. 6. сообщение атакующей машины о начале SYN атаки*

Наблюдая в этот момент за консолью атакуемой машины, можно заметить, что начали поступать пакеты с различных IP адресов и размером **90**, как мы и указывали при начале атаки. На них отправляются ответные пакеты, но пакет с **ACK** флагом от исходного IP так и не поступает.



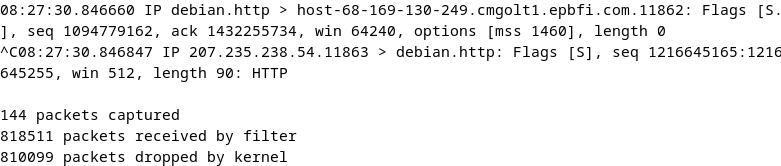
*рис. 7. Пакеты поступающие атакуемой машине*

Во время атаки наблюдается заметная нагрузка на систему, однако она остается функционирующей все время. Мы можем даже проверить количество полуоткрытых соединений, и заметим, что их количество значительно превышает **0** в простое, а значит, что система и в самом деле находится под атакой.



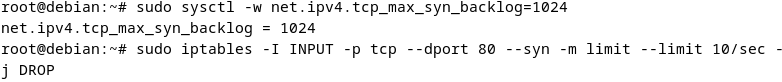
*рис. 8. Количество полуоткрытых соединений во время атаки и во время простоя*

После завершения атаки и прослушивания входящих пакетов, мы можем заметить, что ядро системы сбросило более **98%** входящих пакетов и именно поэтому система осталась функционирующей и не легла полностью.



*рис. 9. Информация о полученных пакетах после проведения атаки*

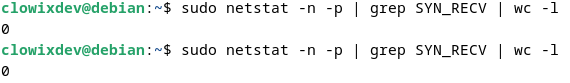
Теперь попробуем применить предложенные нам методы защиты от такого типа атак. На атакуемой машине выполним следующие команды



*рис. 10. Принятые меры защиты от атак типа SYN-flood*

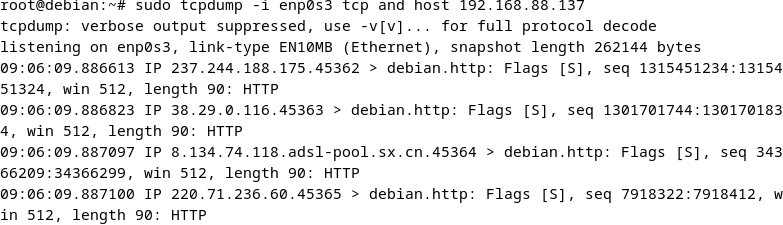
Первая из них отключает очередь “полуоткрытых” TCP соединений, а вторая ограничивает максимальное число полуоткрытых соединений с одного IP адреса к определенному порту.

После принятых мер по обеспечению безопасности системы, во время атаки, число полуоткрытых соединений было равно 0, как и во время простоя.



*рис. 11. Количество полуоткрытых соединений во время атаки и во время простоя*

А также, атакуемая система больше не отправляла ответные пакеты на несуществующие IP адреса.



*рис. 12. Пакеты поступающие атакуемой машине*

Тем не менее, система все равно оставалась нагруженной во время атаки и немного ***“тормозила”***, ведь ей все равно приходится обрабатывать пакеты поступающие с огромной скоростью

**b. ICMP-flood**

Суть атаки такого типа очень схож с атакой ***SYN-flood***, однако атакуемая машина забрасывается ***ICMP*** пакетами, т. е. служебными (они используются, например при попытке “пропинговать” сервер.) Они не используются для передачи информации. Это приводит к созданию огромного количества ответных пакетов и как следствие снижению пропускной способности канала.

Так как мы уже знаем адреса наших виртуальных машин, то атака будет проводиться с помощью следующей команды.

hping3 -c 10000 -p 80 -1 --flood --rand-source 192.168.88.137

Ее параметры сильно не изменились. Единственное что поменялось, это флаг ***-1*** вместо флага ***-S*** который соответствует ***ICMP*** пакету.

Отслеживать пакеты на атакуемой машине будем с помозью той же утилиты ***tcpdump***, однако переведем ее в режим отслеживания ***ICMP*** пакетов.

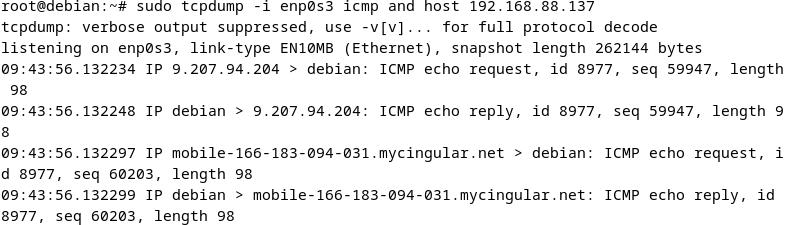
sudo tcpdump -i enp0s3 icmp and host 192.168.88.137

После начала атаки, мы видим соответствующее сообщение в консоли атакующей машины.



*рис. 13. сообщение атакующей машины о начале ICMP атаки*

В это время, атакуемая машина получает ***ICMP*** пакеты с несуществующих IP адресов и отправляет на них ответы.



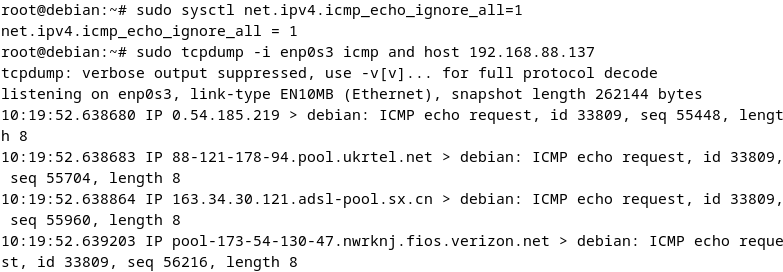
*рис. 14. Пакеты поступающие атакуемой машине*

Для защиты от такого типа атак необходимо отключить ответы на ***ICMP*** ***echo***. Таким образом, нагрузка на канал уменьшится. Сделать это можно следующим образом



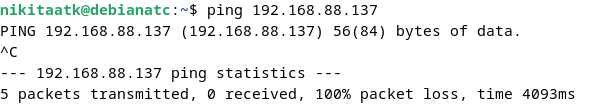
*рис. 15. Принятые меры защиты от атак типа ICMP-flood*

После внесения вышеупомянутых мер защиты в систему, во время атаки, атакуемая машина больше не отвечает на ***ICMP*** пакеты, а значит нагрузка на канал уменьшена.

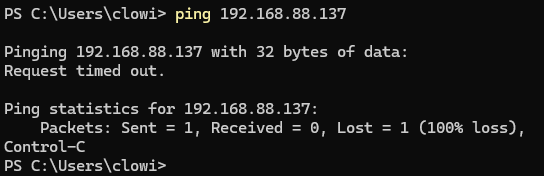


*рис. 16. Пакеты поступающие атакуемой машине*

Теперь так же при попытке ***“пропинговать”*** атакуемую машину с основной и атакующей, мы не получим никаких ответов



*рис. 17. Попытка “пропинговать” атакуемую машину с атакующей*



*рис. 18. Попытка “пропинговать” атакуемую машину с основной*

1. **Пакеты, генерируемые каждым генератором пакетов.**

**Структура IP пакета (версии 4)**

IP-пакет — это форматированный блок [информации](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D1%8F), передаваемый по [компьютерной сети](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C), структура которого определена протоколом IP. Соединения компьютерных сетей, не поддерживающие IP-пакеты, такие как традиционные соединения типа «точка—точка» в телекоммуникациях, просто передают данные в виде последовательности [байтов](https://ru.wikipedia.org/wiki/%D0%91%D0%B0%D0%B9%D1%82), [символов](https://ru.wikipedia.org/wiki/%D0%A1%D0%B8%D0%BC%D0%B2%D0%BE%D0%BB) или [битов](https://ru.wikipedia.org/wiki/%D0%91%D0%B8%D1%82). При использовании пакетного форматирования сеть может передавать длинные сообщения более надежно и эффективно.

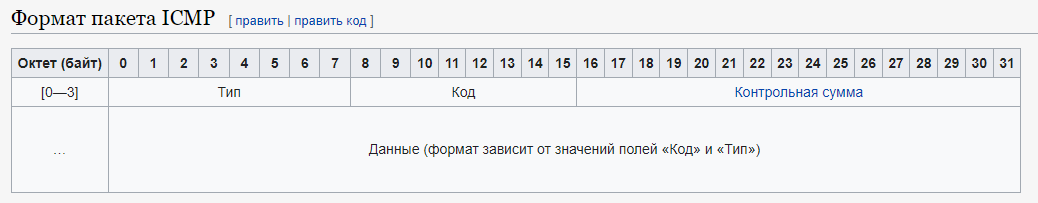
IP-пакет состоит из секции заголовка и секции данных, структура его представлена на рис. 19



*рис. 19. Структура IPv4 пакета*

**Структура ICMP пакета**

ICMP пакет (служебный) основан на протоколе IP. Каждое ICMP-сообщение инкапсулируется непосредственно в пределах одного IP-пакета, и, таким образом является «ненадежным» (не контролирующим доставку и её правильность). В отличие от UDP, где реализация надёжности возложена на ПО прикладного уровня, ICMP (в силу специфики применения) обычно не нуждается в реализации надёжной доставки. Его цели отличны от целей транспортных протоколов: он, как правило, не используется для передачи и приёма данных между конечными системами. Его структура представлена на рис. 20



*рис. 20. Структура ICMP пакета*

**ОТВЕТЫ НА КОНТРОЛЬНЫЕ ВОПРОСЫ**

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

Общий принцип проведения DoS-атак заключается в “затоплении” (flood) конечного пользователя-жертвы запросами различного вида. Основная идея этой атаки заточена на ограниченности вычислительных ресурсов жертвы и как следствие невозможность сгенерировать ответ обычному пользователю.

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

Рассмотрим несколько видов DoS-атак и способы защиты от них:

1. SYN-flood: Отключение очереди “полуоткрытых” TCP-соединений
2. ICMP-flood: Отключение ответов на запросы ICMP *echo*
3. HTTP-flood: Увеличение одновременного количества максимальных подключений к базе данных сервера
4. UDP-flood: Отключение UDP-сервисов и установление ограничения на число соединений с DNS-сервером
5. **В чем заключается работа генератора пакетов? Какие настройки можно установить при генерации пакетов?**

Работа генератора пакетов заключается в создании некоторой единицы, называемой пакетом и последующей его отправкой в компьютерную сеть.

При генерации пакета можно выбрать один из существующих или же создать пакет с нуля, при этом выбрав его тип, наполнение, флаги и т. д.

Далее можно выбрать режим отправки этих пакетов и конечную цель.

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

UDP-пакет состоит из четырех полей, каждое по 2 байта. Два из них необязательны к использованию в IPv4, в то время как в IPv6 необязателен только порт отправителя.

Поля: порт отправителя, порт получателя, длина датаграммы и контрольная сумма (используется для проверки заголовка и данных на ошибки; если же контрольная сумма не сгенерирована передатчиком, то поле заполняется нулями).

Так как в протоколе UDP отсутствует механизм предотвращения перегрузок, то становится возможным проведение DoS-атаки на уровне UDP-трафика.

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 огромное число ответных пакетов, а пропускная способность канала снижается. После отключения ответов на ICMP запросы, такое огромное число ответных пакетов создано не будет, и, как следствие, пропускная способность канала снижена также не будет.

ВЫВОД

В ходе данной работы был изучен механизм угрозы типа “Отказ в обслуживании”. Рассмотрены генераторы различных пакетов, такие как *Nemesis, Colasoft Packet Builder, PACKETH и Ostinato*. Изучены способы реализации атак типа “Отказ в обслуживании”, а также некоторые методы защиты от них.