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. 4851003/20001 Павлов И. А.

<*подпись*>

1. Преподаватель
2. асс. преподавателя Климшин И. И.

<*подпись*>

1. **Цель работы**

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

1. **Описание задач**
2. Изучить функционал генераторов пакетов Nemesis, Colasoft Packet Builder, PACKETH.
3. Смоделировать и проанализировать SYN и ICMP flood атаки.
4. Организовать элементы защиты от этих атак.
5. **Описание генераторов пакетов**
6. Nemesis – это консольная программа, с помощью которой можно посылать различные пакеты по заданному IP-адресу со следующими особенностями:
7. Позволяет создать любые необходимые для dos-атаки пакеты.
8. Имеет консольный интерфейс.
9. Поддерживается как на Linux, так и на Windows.
10. Может генерировать случайные IP источника, но не во время атаки (один раз генерирует случайный IP для всех пакетов), из-за чего сильно уменьшается скорость подачи пакетов.
11. Можно управлять количеством и скоростью подачи TCP пакетов, но нельзя для ICMP.
12. Можно не генерировать каждое поле пакета (в таком случае заполнится случайными значениями).
13. Colasoft Packet Builder:
14. Позволяет создавать любые пакеты, кроме ICMP.
15. Графический интерфейс.
16. Можно выбрать карту, с которой будет вестись передача.
17. Имеет встроенный HEX-редактор.
18. Только для Windows.
19. Нельзя генерировать случайный IP источника.
20. Можно настроить количество и скорость передачи пакетов.
21. Можно сохранять конфигурации.
22. Требует ручной настройки многих полей пакета.
23. PACKETH:
24. Позволяет создавать любы пакеты.
25. Графический интерфейс.
26. Можно сохранять конфигурации.
27. Только Linux.
28. Позволяет во время атаки генерировать случайный IP, mac адрес.
29. Можно выбирать скорость и количество передаваемых пакетов.
30. Во время атаки в случайный момент времени вылетает с ошибками или вовсе не начинает атаку, а вылетает.
31. Почти не требует ручной настройки полей пакета.
32. Ostinato:
33. Позволяет создавать любые пакеты.
34. Не поддерживает TCP-соединения с отслеживанием соединения.
35. Графический интерфейс.
36. Имеет бесплатную версию на Linux, платный на Windows.
37. Позволяет сохранять конфигурации.
38. Удобный процесс остановки и продолжения атаки.
39. Позволяет генерировать IP адреса во время атаки (список получается до атаки).
40. Очень долгий процесс загрузки конфигурации при генерации огромного количества случайных IP (вплоть до 30 минутного ожидания).
41. Почти не требует ручного заполнения полей пакета.
42. Можно выбирать скорость и количество передаваемых пакетов.
43. **Ход работы**

Для тестирования атак будет использоваться web-сервер Apache2, установленный на операционную систему Ubuntu. Сначала смоделируем SYN-flood атаку с помощью утилиты hping3 (рис. 1). В команде мы прописываем тип пакета (в данном случае это SYN), мнимый адрес отправителя, скорость отправки пакетов и адрес сервера. 

Рис. 1

При такой атаке на сервер поступает большое количество запросов на подключение с несуществующего ip адреса, на которые сервер не может ответить. В итоге канал заполняется пакетами, и к серверу становится невозможным подключиться.

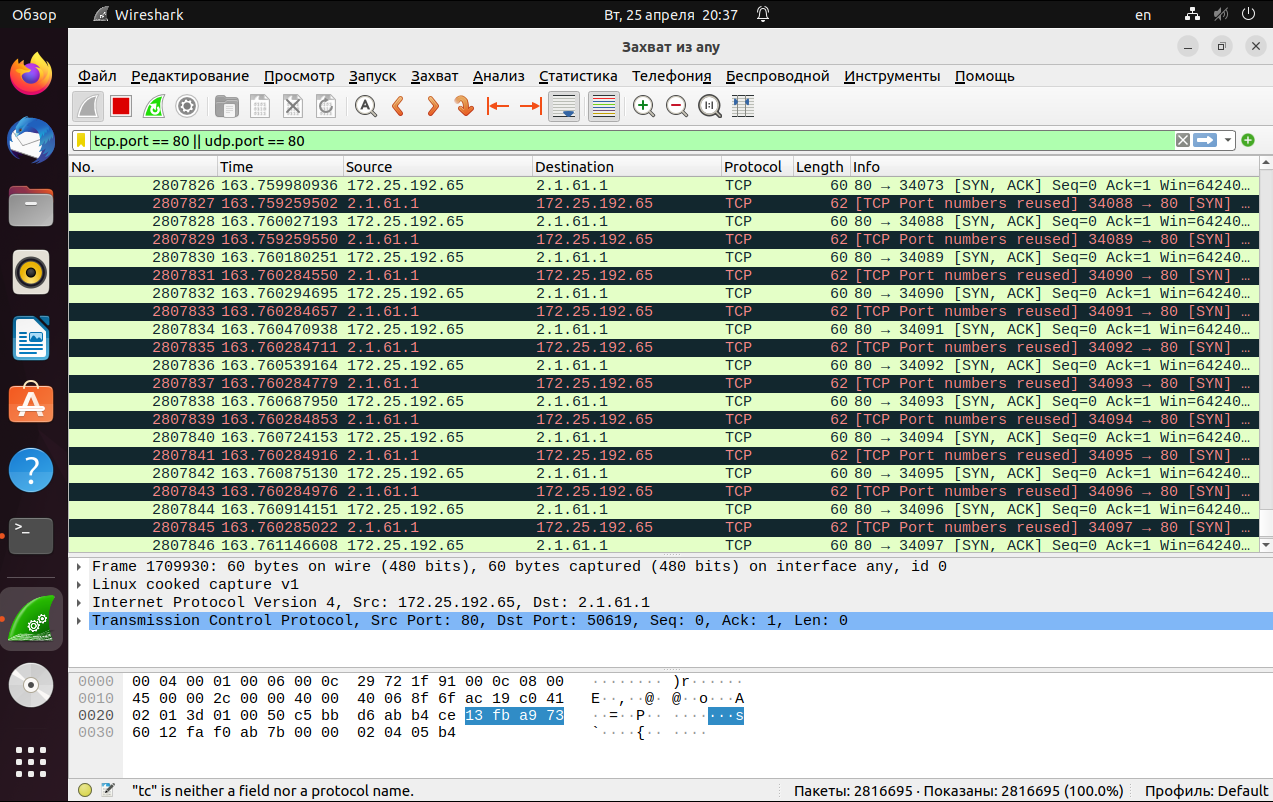
Атака прошла успешно, когда количество пакетов достигло 2816695 сервер перестал отвечать на сообщения. Время между запросами составило 0.00006 секунды. Скорость составила 17146 пакета в секунду. (рис. 2) 

Рис. 2

Организуем элементы защиты от SYN-атаки. Для этого, согласно учебному пособию по Основам информационной безопасности, нужно отключить очередь “полуоткрытых” TCP-соединений командой:

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

Повторим SYN-атаку. Атака также прошла успешно, незначительно изменилось лишь количество пакетов, которое было отправлено на сервер. (рис. 3). Защита не показала хороших результатов.

Изображение выглядит как текст

Автоматически созданное описание

Рис. 3

Теперь смоделируем ICMP-атаку, суть которой заключается в “забрасывании” сервера пакетами типа ICMP (рис.4).

Рис. 4

Как мы видим количество времени ожидания ответа увеличилось (Рис. 5). Это значит, что атака прошла успешно. Для заполнения канала хватило 88331 пакета. Скорость передачи составила 4496 пакетов в секунду. Интервал между пакетами – 0.0002 секунды. (Рис. 6)

Изображение выглядит как текст

Автоматически созданное описание

Рис. 5Изображение выглядит как стол

Автоматически созданное описание

Рис. 6

Теперь организуем элементы защиты от ICMP-атаки. (рис. 7)

Рис. 7

Защита оказалась успешной, сервер можно было открыть в браузере.

1. **Ответы на контрольные вопросы**

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

Общий принцип проведения DoS-атак заключается в организации большого количества пакетов (flood), отправляемых на сервер, который постепенно исчерпает свои ресурсы и перестанет отвечать.

2. Какие способы защиты от DoS-атак существует?

Способы защиты от DoS-атак отличаются в зависимости от типа атаки. Так, например, для защиты от SYN-flood необходимо очистить очередь «полуоткрытых» TCP-соединений; для защиты от ICMP-flood необходимо отключить ответы на запросы IMCP echo; для защиты от

HTTP-flood необходимо увеличить максимальное количество одновременных подключений; для защиты от UDP-flood необходимо отключить UDP-сервисы и установить ограничение на число соединений с DNS-сервером.

3. В чем заключается работа генератора пакетов? Какие настройки можно установить при генерации пакетов?

Работа генератора пакетов заключается в создании пактов с различными параметрами и их последующей отправке в сеть. При генерации пакетов можно установить количество и тип пакетов, адреса отправителя и получателя и параметры отправки.

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

Структурно UDP-пакет состоит из четырехпольного заголовка, каждое поле которого занимает 16 бит (на порт отправителя, порт получателя, длину датаграммы и контрольную сумму).

Проведение DoS-атаки на уровне UDP-трафика возможно благодаря отсутствию механизма предотвращений перегрузок, что обеспечивает быстрый захват всей полосы пропускания паразитному трафику, что оставляет полезному трафику ничтожно малую часть.

5. За счет чего отключение ответов на запросы ICMP позволяет решить проблему ICMP-flood?

Отключение ответов на запросы ICMP позволяет решить проблему ICMP-flood за счет прекращения создания ответных пакетов, отсутствие которых повышает пропускную способность канала.

1. **Выводы**

В ходе проведения лабораторной работы были получены знания о том, как организовывать SYN и ICMP атаки и как защищаться от ICMP атаки. Из результатов атак можно сделать вывод о том, что средств защиты, предложенных учебным пособием недостаточно, и необходимо организовывать дополнительные меры по защите сервера от SYN-атаки.