УДК 004 **Технические науки**

Хомякова Ника Александровна, *студент*

Астраханский государственный университет им. В. Н. Татищева,

г. Астрахань, Россия

Email: tfrbdv@bk.ru

АНАЛИЗ СЕТЕВОГО ТРАФИКА С ЦЕЛЬЮ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация: Стремительное развитие информационных технологий вызвало проблемы защиты информации, которые столь же важны и остры, как и влияние информационных технологий на все общество. Сетевые атаки, сбои и отказы сетевого оборудования являются основными факторами, влияющими на безопасность передачи информации в распределенных сетях. Поэтому анализ сетевого трафика является очень важной частью процесса обеспечения информационной безопасности.

Ключевые слова: информационная безопасность, защита, информационная среда, оборудование.

Abstract: The rapid development of information technologies has caused problems of information protection, which are as important and acute as the impact of information technologies on the whole society. Network attacks, failures and failures of network equipment are the main factors affecting the security of information transmission in distributed networks. Therefore, network traffic analysis is a very important part of the information security process.

Keywords: information security, protection, information environment, equipment.

Современный мир невозможно представить без использования

компьютерных сетей. Сети обеспечивают быстрый доступ к информации, упрощают работу и повышают эффективность бизнес-процессов. Однако, с увеличением количества информации, передаваемой по сети, растет и угроза нарушения информационной безопасности.

Один из способов защиты информации - это анализ сетевого трафика. Анализ сетевого трафика позволяет выявить подозрительную активность, установить источник атаки и предпринять меры по защите системы.

Анализ сетевого трафика состоит из нескольких этапов. Сначала необходимо собрать данные о трафике, который передается по сети. Для этого используются специальные программы - снифферы. Снифферы могут работать на уровне сетевого интерфейса или захватывать трафик на уровне приложений. Собранные данные сохраняются в файлы, которые затем анализируются.

Далее, данные обрабатываются с помощью специальных программ, которые позволяют выделить основные характеристики трафика, такие как размер пакетов, время задержки, тип протокола и т.д. Анализ этих характеристик позволяет выявить аномалии в сетевом трафике.

Кроме того, при анализе сетевого трафика можно выявить попытки несанкционированного доступа к сети. Например, если обнаружены попытки подбора паролей или сканирования портов, то это может указывать на наличие злоумышленников, пытающихся получить доступ к защищенным ресурсам.

В качестве механизма безопасности вы можете использовать программу Wireshark, предназначенную для перехвата и последующего анализа, или анализировать только сетевой трафик, используемый для других узлов.

При анализе сетевого трафика должны быть решены следующие задачи:

Захват трафика при передаче файлов и изображений;

Отменить информацию, содержащуюся в пакете захвата;

Быстрый анализ сеансов TCP: определение количества сеансов TCP в буфере захваченных пакетов; отображение статистики сеансов TCP;

Неверная идентификация ошибок в захваченных пакетах;

Мы делаем выводы о проделанной нами работе.

Чтобы захватить сетевой трафик, используйте меню Cupture-Options и получите дамп с захваченными пакетами, как показано на рисунке 1.

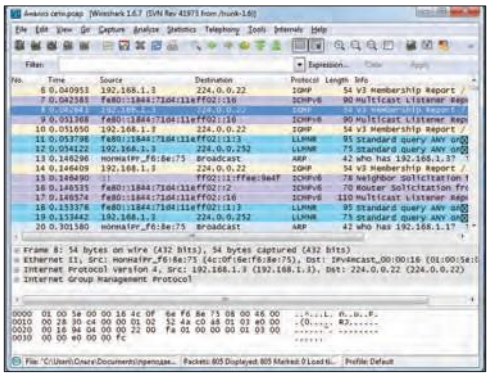

Рисунок 1-Дамп захваченных пакетов

Чтобы извлечь файлы или изображения из захваченных файлов, их необходимо отфильтровать с помощью пакетов протокола HTTP. Далее, чтобы извлечь информацию, перейдите к

Файл-Экспорт объекта-меню HTTP. Появится окно, в котором будут показаны все захваченные http-объекты - текстовые файлы, изображения и т.д. (Рисунок 2).

Рисунок 2 -Список захваченных файлов

Чтобы извлечь любой файл из этого списка, просто выберите его и нажмите "Сохранить как". С извлечением чертежа проблем нет (рис. 3). Потоковое видео / аудио может быть извлечено таким же образом.

Рисунок 3 - Извлеченный чертеж

Чтобы быстро просмотреть данные передачи в рамках определенного сеанса, пожалуйста, используйте команду меню Анализировать - Следовать потоку TCP. Чтобы использовать функцию отслеживания потока TCP, вам необходимо знать, что данные, которые вы ищете, находятся в определенном пакете. Вы можете определить это, "увидев" передачу данных в потоке TCP в виде пакета протокола FTP-data (рис. 4):

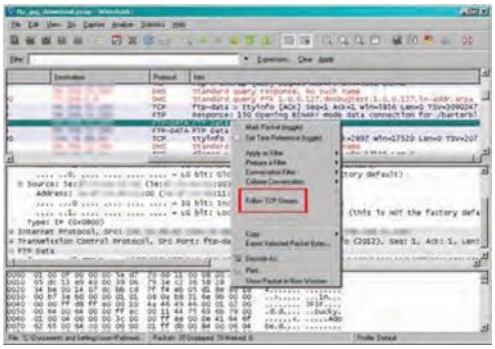

Рисунок 4 - Выбор пакета передачи данных

В появившемся окне выберите функцию "Сохранить" и сохраните данные на диск, используя расширение файла. Если вы не знаете точно расширение сохраненного файла, то заголовок файла может помочь вам "распознать" его – в нашем примере JFIF означает, что это файл jpg.

Чтобы определить количество сеансов TCP в буфере захваченных пакетов, вам необходимо выполнить команду меню Статистика-Разговоры (рис. 5).

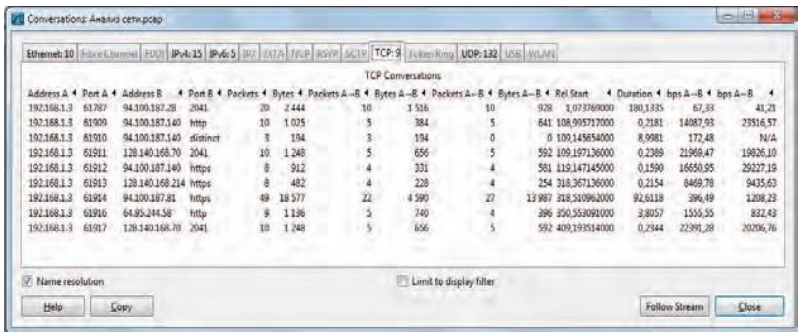

Рисунок 5 - Количество сеансов TCP

На рисунке 5 показано, что в буфере захваченного файла имеется 9 сеансов TCP. Выберите первый сеанс и щелкните правой кнопкой мыши, чтобы воспользоваться контекстным меню "Применить как выбранный фильтр-A<->B" (рис. 6).

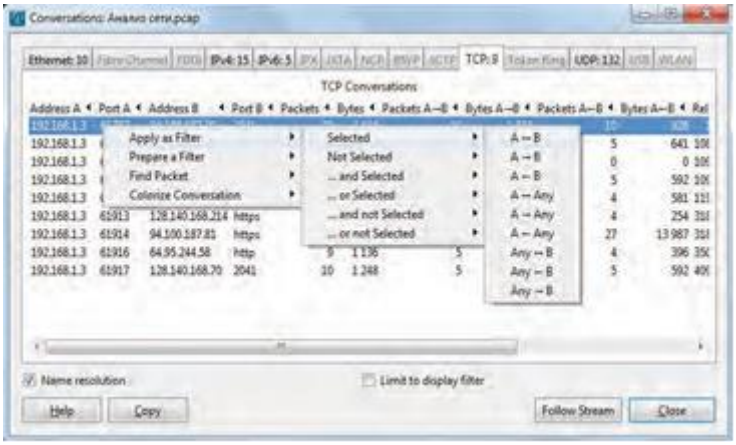

Рисунок 6-Кадр, показывающий только один сеанс

а) Клиент использует порт 61787, а сервер использует порт 2041;

б) Начальный серийный номер, выбранный клиентом, равен 122; в) Длина заголовка TCP составляет 60 байт.

Выбрав составное меню Analyze-Expert Info, мы извлекем сообщения об ошибках и предупреждающие знаки (например, отсутствующие сегменты или сегменты вне очереди) для быстрого обнаружения проблем, как показано на рисунке 6.

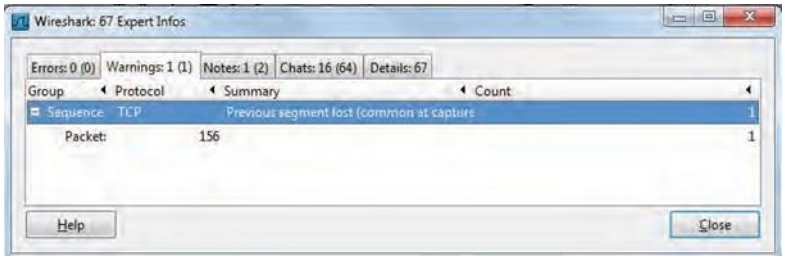

Рисунок 6 - Окно функции обнаружения ошибок

На рисунке 6 показано 16 чатов. Например, TCP–пакет с установленным флагом SYN; предупреждение - кодировка второго пакета протокола DHCP; предупреждение - предыдущий абзац потерян; и ошибка не была обнаружена.

Библиографический список:

1. Технологии слияния гетерогенной информации из разнородных источников (data fusion) Ананченко И.В., Гайков А.В., Мусаев А.А. Известия Санкт-Петербургского государственного технологического института (технического университета). 2013. №19 (45). с. 098-105.

2. The information infrastructure design of an educational organization using virtualization technologies. Musaev A.A., Gazul S.M., Anantchenko I.V. Известия Санкт-Петербургского государственного технологического института (технического университета). 2014. № 27 (53). с. 71-76.