Частное учреждение образования

Колледж бизнеса и права

|  |
| --- |
| УТВЕРЖДАЮ  Ведущий методист колледжа  \_\_\_\_\_\_\_\_\_\_\_Е.В. Паскал  «\_\_\_» 2023 |
| Специальность: 2-40 01 01 «Программное обеспечение информационных технологий» | Учебная дисциплина: «Защита компьютерной информации» | |

# Лабораторная работа №20

Инструкционно-технологическая карта

Тема: Применение ПС для анализа трафика в сети. Классификация расходов трафика.

Цель: научиться исследовать и применять программные системы для анализа трафика в сети с целью классификации его расходов.

Время выполнения: 2 часа.

СОДЕРЖАНИЕ РАБОТЫ

1. Теоретические сведения для выполнения работы
2. Практические задания
3. Контрольные вопросы
4. Литература
5. ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ ДЛЯ ВЫПОЛНЕНИЯ РАБОТЫ

## Водная информация

Трафик сетей в интернете представляет собой обмен данных, информации и пакетов, который происходит между различными узлами и устройствами в глобальной компьютерной сети. Этот трафик может включать передачу веб-страниц, электронной почты, файлов, потокового видео, голосовых вызовов и других типов информации, передаваемых через различные протоколы, такие как HTTP, FTP, SMTP, TCP/IP и другие.

Один из важных аспектов, связанных с анализом трафика, — это обнаружение и анализ аномального сетевого поведения. Аномалии в сетевом трафике могут указывать на нарушения безопасности, сетевые проблемы или ненормальное функционирование сетевых устройств.

Обнаружение аномального сетевого поведения включает в себя анализ и сравнение текущего трафика с нормальными или ожидаемыми моделями поведения. Это может включать мониторинг аномального объема трафика, необычных паттернов передачи данных, подозрительных запросов или необычной активности в сети.

Для обнаружения аномалий в трафике могут использоваться различные методы, включая статистический анализ, машинное обучение и анализ содержимого пакетов.

Существует несколько распространенных классификаций расходов трафика в сети, которые позволяют идентифицировать различные типы сетевых приложений, протоколов или сервисов. Некоторые из них включают:

* классификация по типу протокола: эта классификация основана на идентификации используемого протокола в сетевом трафике. Например, можно выделить HTTP-трафик, FTP-трафик, DNS-трафик и т.д. Это позволяет анализировать и понимать, какие протоколы преобладают в сети и как они влияют на расход ресурсов;
* классификация по типу приложения: здесь трафик классифицируется по типу сетевого приложения или сервиса, генерирующего этот трафик. Например, можно выделить трафик видео-стриминга, голосовых вызовов, онлайн-игр, социальных сетей и т.д. Это помогает определить, какие типы приложений потребляют большую часть сетевых ресурсов;
* классификация по содержимому: в этой классификации трафик анализируется на основе содержимого данных, передаваемых в сети. Например, можно классифицировать трафик на основе ключевых слов, шаблонов или сигнатур определенных типов данных или протоколов. Это может быть полезно для обнаружения и фильтрации нежелательного или вредоносного трафика;
* классификация по направлению или источнику: здесь трафик классифицируется на основе источника или назначения данных. Например, можно выделить входящий и исходящий трафик, трафик между определенными сегментами сети или трафик между конкретными узлами. Это позволяет анализировать направления коммуникации и оценивать трафик внутри сети;
* классификация расходов трафика позволяет лучше понимать характеристики и особенности сетевой активности, а также принимать решения о ресурсах, оптимизации сети и обеспечении безопасности.

Wireshark — это мощный инструмент сетевого анализа, который позволяет захватывать и анализировать сетевой трафик в реальном времени. Он может быть использован для различных целей, таких как отладка сетевых проблем, анализ безопасности, анализ протоколов и многое другое.

Протокол — это набор правил и соглашений, которые определяют формат и последовательность обмена данными между устройствами в сети. Он определяет, как данные должны быть упакованы, переданы и интерпретированы на отправителе и получателе.

Протоколы необходимы для обеспечения стандартизированного и надежного обмена данными между различными устройствами и приложениями в компьютерных сетях. Они определяют, как устройства должны устанавливать соединения, передавать информацию, обрабатывать ошибки и завершать коммуникацию.

HTTP (Hypertext Transfer Protocol) — это протокол передачи данных, который используется для обмена информацией между веб-серверами и клиентами. Он является основным протоколом для доступа к веб-страницам в интернете и обеспечивает запросы и передачу гипертекстовых документов, таких как HTML.

FTP (File Transfer Protocol) — это протокол передачи файлов, который используется для передачи файлов между клиентом и сервером. FTP позволяет пользователю загружать файлы на сервер и скачивать файлы с сервера, а также выполнять другие операции с файлами, такие как удаление и переименование.

SMTP (Simple Mail Transfer Protocol) — это протокол передачи почты, который используется для отправки электронных писем между почтовыми серверами. SMTP обеспечивает доставку электронной почты от отправителя к получателю, а также управление очередью и маршрутизацию сообщений.

При передаче данных протоколы указывают на:

* формат данных: Протоколы определяют, как данные должны быть структурированы и упакованы перед отправкой. Это включает в себя определение заголовков, полей и структуры пакетов данных;
* маршрутизацию: Протоколы указывают, как данные должны быть направлены от отправителя к получателю через различные сетевые узлы. Это включает в себя определение адресации и маршрутизации данных в сети;
* управление сеансом: Протоколы обеспечивают установление, поддержание и завершение соединений между устройствами. Они определяют процедуры управления сеансом, такие как установка соединения, проверка целостности данных и разрыв соединения;
* контроль ошибок: Протоколы включают механизмы для обнаружения и восстановления от ошибок, возникающих во время передачи данных. Они обеспечивают проверку целостности данных, повторную передачу потерянных пакетов и управление потоком данных;
* управление ресурсами: Протоколы определяют, как должны быть распределены и управляться ресурсы сети, такие как полоса пропускания, приоритеты и задержки передачи данных.

Что обозначают столбики и какую информацию можно получить исходя из этих столбиков:

* No. (Номер): порядковый номер пакета в списке захвата трафика;
* Time (Время): отображает время захвата пакета. Включает информацию о точном моменте времени и временных отметках относительно предыдущих пакетов;
* Source (Источник): IP-адрес или имя устройства, отправляющего пакет;
* Destination (Получатель): IP-адрес или имя устройства, принимающего пакет;
* Protocol (Протокол): определяет протокол, используемый в пакете, такой как TCP, UDP, ICMP, DNS и другие;
* Length (Длина): указывает длину пакета в байтах;
* Info (Информация): содержит краткое описание пакета или информацию о его содержимом. Включает различные сведения о протоколе и действиях, связанных с пакетом;
* Source Port (Исх. порт): порт отправителя, используемый для идентификации конкретного приложения или службы на отправителе;
* Destination Port (Получ. порт): Порт получателя, используемый для идентификации конкретного приложения или службы на получателе;
* Flags (Флаги): дополнительная информация о флагах, связанных с протоколами, такими как TCP, где флаги могут указывать на установку соединения, закрытие, сброс и другие события;
* Info column (Столбец информации): отображает более подробную информацию о пакете, включая различные события и действия, связанные с протоколом.

Кроме указанных столбцов, Wireshark также предоставляет возможность настроить отображение дополнительных столбцов, чтобы увидеть другую информацию о пакетах. Эти столбцы могут включать информацию о MAC-адресах, версии протоколов, кодах состояния и других атрибутах, в зависимости от типа пакета и протокола.

**Как уставить Wireshark?**

Шаги по установке Wireshark могут незначительно отличаться в зависимости от операционной системы, которую вы используете. Вот общая пошаговая инструкция для установки Wireshark:

Шаг 1: загрузите Wireshark

* посетите официальный веб-сайт Wireshark по адресу https://www.wireshark.org/;
* на главной странице найдите раздел загрузки (Download) и выберите соответствующую операционную систему.

Шаг 2: выберите версию Wireshark для загрузки

* в разделе загрузки вы увидите доступные версии Wireshark для вашей операционной системы;
* рекомендуется загрузить последнюю стабильную версию, если она доступна.

Шаг 3: загрузите установочный файл

* щелкните по ссылке загрузки для выбранной версии Wireshark;
* подтвердите сохранение файла на ваш компьютер.

Шаг 4: запустите установку

* найдите загруженный установочный файл Wireshark на вашем компьютере и запустите его;
* если требуется, подтвердите действие администратора для продолжения установки.

Шаг 5: выберите опции установки

* при запуске установщика вам может быть предложено выбрать опции установки;
* ознакомьтесь с предлагаемыми опциями и выберите необходимые параметры, если есть такая возможность.

Шаг 6: примите лицензионное соглашение

* прочтите лицензионное соглашение (EULA) и примите его условия, чтобы продолжить установку.

Шаг 7: укажите путь установки

* если требуется, выберите папку или директорию, в которую будет установлен Wireshark. Обычно используется предлагаемый по умолчанию путь.

Шаг 8: завершение установки

* дождитесь завершения установки Wireshark на вашем компьютере;
* после завершения установки может потребоваться перезагрузка системы.

Это общая пошаговая инструкция по установке Wireshark, рекомендуется оставить те же настройки рекомендованные для установки ПС «Wireshark». Обратите внимание, что некоторые шаги могут отличаться в зависимости от вашей операционной системы или версии Wireshark.

**Как работать?**

Шаг 1: запустите Wireshark Запустите приложение Wireshark на вашем компьютере. Обычно после установки Wireshark его можно найти в меню "Пуск" (Windows) или в папке "Программы" (macOS).

Шаг 2: Выберите сетевой интерфейс Wireshark покажет список доступных сетевых интерфейсов на вашем компьютере. Выберите интерфейс, который вы хотите использовать для захвата сетевого трафика. Например, это может быть ваша сетевая карта Ethernet или беспроводной адаптер Wi-Fi.

Шаг 3: захватите пакеты. Нажмите кнопку "Захват" или "Start" (начать) для начала процесса захвата пакетов на выбранном интерфейсе. Wireshark начнет записывать все пакеты, проходящие через выбранный интерфейс.

Шаг 4: Анализируйте пакеты. После начала захвата пакетов Wireshark будет отображать захваченные пакеты в реальном времени в основном окне программы. Вы можете щелкнуть на каждом пакете, чтобы увидеть его подробности, включая заголовки протоколов и данные.

Шаг 5: примените фильтры Wireshark предоставляет мощные возможности фильтрации, которые позволяют вам сузить область анализа и сконцентрироваться только на интересующих вас пакетах. Вы можете использовать фильтры по протоколам, адресам и другим параметрам, чтобы отобразить только необходимую информацию.

Шаг 6: Используйте дополнительные функции Wireshark предлагает множество дополнительных функций, которые могут быть полезными при анализе сетевого трафика. Это включает в себя генерацию статистики, отслеживание потоков данных, поиск конкретных событий, экспорт данных для дальнейшего анализа и многое другое. Изучите возможности Wireshark и экспериментируйте с ними.

Шаг 7: завершите захват и сохраните данные. Когда вы завершите анализ или достигнете нужных результатов, остановите захват пакетов, нажав кнопку "Stop" (остановить) или аналогичную. После этого вы можете сохранить записанные пакеты для будущего использования или обработки.

Пример.

Условие задачи: исследование HTTP-запросов и ответов

Описание: захватите сетевой трафик с помощью Wireshark во время веб-серфинга. Используйте фильтр Wireshark для отображения только пакетов протокола HTTP. Изучите заголовки запросов и ответов, анализируйте параметры запросов (URL, методы, заголовки) и содержимое ответов (статусы, заголовки, содержимое страниц). Попробуйте определить, какие веб-сайты посещены и какие данные передаются.

Решение:   
Шаг 1: установите и запустите Wireshark

Загрузите и установите Wireshark с официального сайта (https://www.wireshark.org/).

Запустите программу Wireshark на вашем компьютере.

Шаг 2: Настройте захват сетевого трафика

Выберите сетевой интерфейс, через который вы хотите захватить трафик (например, Ethernet или Wi-Fi).

Нажмите на кнопку "Запуск" или "Старт" для начала захвата пакетов.

Шаг 3: Фильтрация пакетов HTTP

В поле "Фильтр" (Filter) введите "http" без кавычек и нажмите Enter.

Теперь Wireshark будет отображать только пакеты протокола HTTP.

Шаг 4: Изучение заголовков запросов и ответов

Выберите первый пакет в списке и раскройте его детали.

Изучите раздел "Hypertext Transfer Protocol" в раскрывающемся списке, чтобы увидеть заголовок запроса (Request).

Проанализируйте параметры запроса, такие как URL, метод (GET, POST и т.д.), заголовки и другие сведения.

Шаг 5: Анализ содержимого ответов

Раскройте раздел "Hypertext Transfer Protocol" в том же пакете, чтобы увидеть заголовок ответа (Response).

Изучите статус ответа (Status), заголовки и содержимое страницы или данных, передаваемых в ответе.

Шаг 6: Идентификация посещенных веб-сайтов и передаваемых данных

Продолжайте просматривать пакеты HTTP и анализировать заголовки запросов и ответов.

Обратите внимание на URL-адреса в запросах, чтобы определить посещаемые веб-сайты.

Анализируйте содержимое ответов, чтобы определить передаваемые данные, такие как HTML-страницы, изображения, файлы или другие типы информации.

Шаг 7: Проведение дополнительных анализов

По мере изучения пакетов HTTP, вы можете обратить внимание на необычные или аномальные запросы или ответы.

Используйте различные функции Wireshark, такие как фильтры, статистика и расширенный анализ, для более глубокого исследования сетевого трафика.

1. ПРАКТИЧЕСКИЕ ЗАДАНИЯ

Задание осуществляется на сайте КБиП, для выполнение требуется запустить Wireshark и выбрать сетевой адаптер.

Пошаговая инструкция для выполнения, следующая:

* запустить Wireshark;
* перейти на сайт КБиП;
* зайти в электронный журнал;
* вернуться в программу;
* ввести в строку фильтра http;
* выбрать любой пакет данных;
* изучить данные из выбранного пакета, из левого нижнего окна.

Расскажите любую дающую вам информацию по этим данным.

1. КОНТРОЛЬНЫЕ ВОПРОСЫ:
2. Что такое Wireshark? Для чего нужен?
3. Что собой представляет собой трафик сетей в интернете?
4. Какие типы информации могут быть переданы через сетевой трафик?
5. Какие методы использовать для обнаружения аномалий в трафике?
6. Что такое HTML, IP, FTP?
7. Что такое протокол и для чего нужен? При передаче данных, на что указывают протоколы?

4. ЛИТЕРАТУРА

1. Андресс Д. Защита данных. От авторизации до аудита – Питер, 2021.
2. Козлов С. Защита информации, устройства несанкционированного съема информации и борьба с ними - Академический проект, 2019.
3. М.В. Баранова и В.В. Кучеренко. Шифрование данных в информационных системах
4. А.А. Данилов, С.А. Копылова, И.В. Михайлов. Защита информации в компьютерных системах и сетях"

Преподаватель Д.А. Бунькевич

Рассмотрено на заседании цикловой комиссии

программного обеспечения информационных технологий

Протокол № \_\_\_\_ от «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_ 2023

Председатель ЦК \_\_\_\_\_\_\_\_\_\_\_ К.О.Якимович