МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное

образовательное учреждение высшего образования

«Юго-Западный государственный университет»

(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
_____О.Г. Локтионова
«___»_____2017 г.

АНАЛИЗ ТРАФИКА В СЕТЯХ ETHERNET

Методические указания по выполнению лабораторной и практической работы по дисциплинам «Сети и системы передачи информации», «Безопасность систем и сетей передачи данных», «Сети и системы передачи информации (специальные разделы)», «Администрирование вычислительных сетей», «Администрирование защищенных телекоммуникационных систем» для студентов укрупненной группы специальностей и направлений подготовки 10.00.00.

Курск 2017

УДК 004

Составители: И.В. Калуцкий, А.Г. Спеваков, А.А. Асютиков, К.О. Хохлач.

Рецензент
Кандидат технических наук, доцент кафедры
«Информационная безопасность» *М.О. Таныгин*

Анализ трафика в сетях Ethernet: методические указания к выполнению лабораторных и практических работ по дисциплинам / Юго-Зап. гос. Ун-т; сост. И.В. Калуцкий, А.Г. Спеваков, А.А. Асютиков, К.О. Хохлач. Курск, 2017, 12 с.: ил. 9.; Библиогр.: с. 12.

Содержат сведения по вопросам анализа трафика в сетях Ethernet. Указывается порядок выполнения лабораторных и практических работ, правила оформления, содержание отчета.

Методические указания по выполнению лабораторной и практической работы по дисциплинам «Сети и системы передачи информации», «Безопасность систем и сетей передачи данных», «Сети и системы передачи информации (специальные разделы)», «Администрирование вычислительных сетей», «Администрирование защищенных телекоммуникационных систем» для студентов укрупненной группы специальностей и направлений подготовки 10.00.00.

Текст печатается в авторской редакции

Подписано в печать Формат 60х84 1/16.
Усл. печ. л. 0,69. Уч. –изд.л. 0,63. Тираж 30 экз. Заказ . Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Локальная сеть — семейство технологий пакетной передачи данных между устройствами для компьютерных и промышленных сетей.
Стандарты Ethernet определяют проводные соединения и электрические сигналы на физическом уровне, формат кадров и протоколы управления доступом к среде — на канальном уровне модели OSI. Ethernet стал самой распространённой технологией ЛВС в середине 1990-х годов, вытеснив такие устаревшие технологии, как Token Ring, FDDI и ARCNET.
Название «Ethernet» (буквально «эфирная сеть» или «среда сети») отражает первоначальный принцип работы этой технологии: всё, передаваемое одним узлом, одновременно принимается всеми остальными (то есть имеется некое сходство с радиовещанием). В настоящее время практически всегда подключение происходит через коммутаторы (switch), так что кадры, отправляемые одним узлом, доходят лишь до адресата — это повышает скорость работы и безопасность сети.

ЦЕЛЬ РАБОТЫ

Цель лабораторной работы – определение основных понятий, которые изучает предмет передачи информации, изучение трафика в сетях Ethernet.

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1. Получить задание
2. Изучить теоретическую часть
3. Выполнить практическое задание
4. Сделать вывод

СОДЕРЖАНИЕ ОТЧЕТА

1. Титульный лист
2. Задание в соответствии с вариантом
3. Выполненное задание
4. Вывод

ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

Анализ сетевого трафика и пакетов с использованием сниффера «Ethereal»

Sniffer (от англ. to sniff – нюхать) – это сетевой анализатор трафика, программа или программно-аппаратное устройство, предназначенное для перехвата и последующего анализа, либо только анализа сетевого трафика, предназначенного для других узлов.

Перехват трафика может осуществляться:

- обычным «прослушиванием» сетевого интерфейса (метод эффективен при использовании в сегменте концентраторов (хабов) вместо коммутаторов (свичей), в противном случае метод малоэффективен, поскольку на сниффер попадают лишь отдельные фреймы);
- подключением сниффера в разрыв канала;
- ответвлением (программным или аппаратным) трафика и направлением его копии на сниффер;
- через анализ побочных электромагнитных излучений и восстановление таким образом прослушиваемого трафика;
- через атаку на канальном (2-й) или сетевом (3-й) уровне, приводящую к перенаправлению трафика жертвы или всего трафика сегмента на сниффер с последующим возвращением трафика в надлежащий адрес.

В начале 1990-х широко применялся хакерами для захвата пользовательских логинов и паролей. Широкое распространение хабов позволяло захватывать трафик без больших усилий в больших сегментах сети.

Снифферы применяются как в благих, так и в деструктивных целях. Анализ прошедшего через сниффер трафика, позволяет:

- Отслеживать сетевую активность приложений.
- Отлаживать протоколы сетевых приложений.
- Локализовать неисправность или ошибку конфигурации.
- Обнаружить паразитный, вирусный и закольцованный трафик, наличие которого увеличивает нагрузку сетевого оборудования и каналов связи.

- Выявить в сети вредоносное и несанкционированное ПО, например, сетевые сканеры, флудеры, троянские программы, клиенты пиринговых сетей и другие.
- Перехватить любой незашифрованный (а порой и зашифрованный) пользовательский трафик с целью узнавания паролей и другой информации.

Постепенно из инструментов, предназначенных только для диагностики, сниферы постепенно превратились в средства для исследований и обучения. Например, они постоянно используются для изучения динамики и взаимодействий в сетях. В частности, они позволяют легко и наглядно изучать тонкости сетевых протоколов. Наблюдая за данными, которые посылает протокол, вы можете глубже понять его функционирование на практике, а заодно увидеть, когда некоторая конкретная реализация работает не в соответствии со спецификацией.

На сегодняшний момент существует достаточно большое количество хороших реализаций снифферов. Некоторое из них:

- Tcpdump – консольный вариант сниффера. Портирован почти подо все наиболее распространенные ОС;
- Wireshark до недавнего момента был известен под названием Ethreal;
- WinDump

Сниффер Wireshark

Программа Wireshark является одной из самых удобных реализаций снифферов. Портирована на большое количество платформ.

Базовый принцип работы снифферов

На рисунке 1 изображена схематично структура сетевой подсистемы ОС. Вся базовая инфраструктура реализована в виде драйверов и работает в режиме ядра. Пользовательские процессы и реализации прикладных протоколов, в частности интерфейс сниффера работают в пользовательском режиме.

На рисунке отображены 2 пользовательских процесса («сетевой процесс «1» и «сетевой процесс 2»).

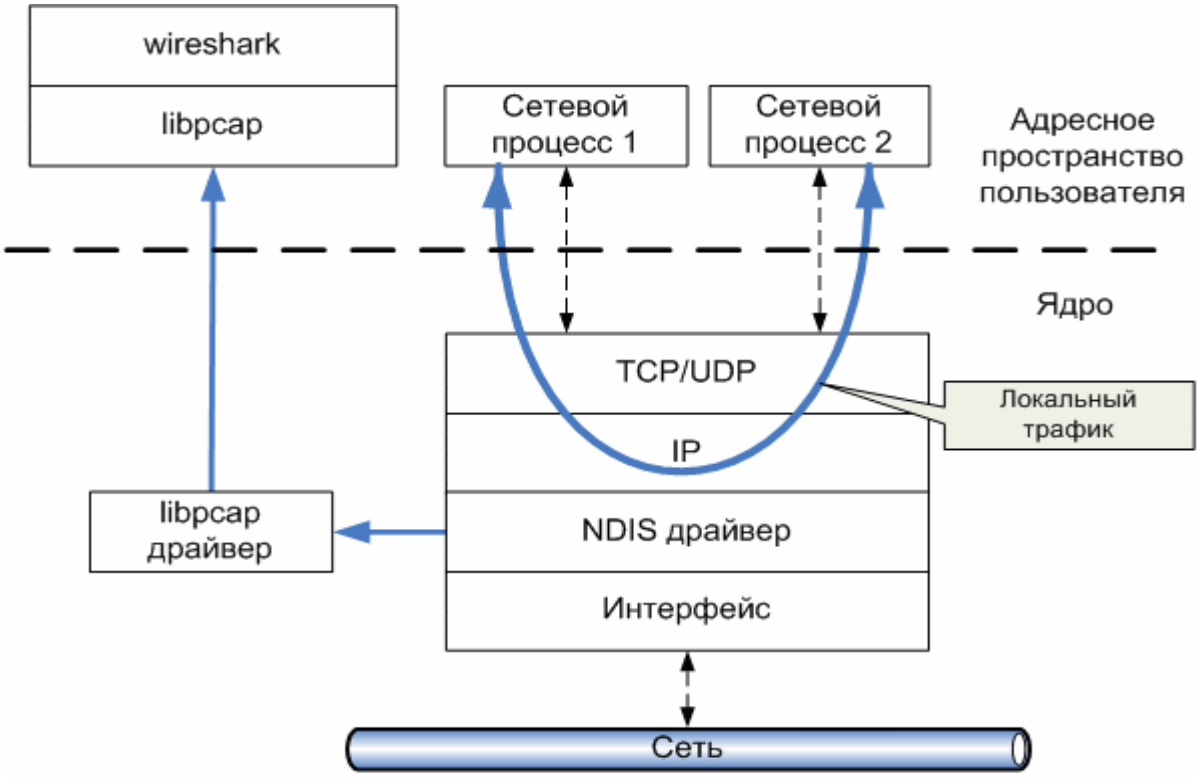

Рисунок 1 – Принцип «захвата» сниффером сетевого трафика

Основными компонентами сниффера являются: драйвер для захвата пакетов (libpcap драйвер), интерфейсная библиотека (libpcap) и интерфейс пользователя (Wireshark). Библиотека libpcap (реализация под ОС Windows носит название WinPcap – универсальная сетевая библиотека, самостоятельно реализующая большое количество сетевых протоколов и работающая непосредственно с NDIS (Network Driver Interface Specification) драйверами сетевых устройств. На базе данной библиотеки реализовано большое количество сетевых программ, в частности сниффер Wireshark.

Основной нюанс использования сниффера заключается в том, что он не позволяет производить анализ локального трафика, т.к. он не проходит через драйвер сетевого устройства. Т.е., если вы захотите проанализировать сниффером трафик между 2-ми сетевыми процессами на локальной машине (например, ftp-сервер и ftp-клиент), то у вас ждет разочарование. Однако, например при использовании виртуальных

машин, сниффер будет работать без проблем, т.к. виртуальные машины эмулируют реальную среду и сетевые адаптеры, поэтому трафик идет через драйвера как и в нормальной ситуации при взаимодействии с другими физическими сетевыми машинами.

Также к недостаткам большинства снифферов стоит отнести и тот факт, что, позволяя анализировать трафик, проходящий через сетевой интерфейс, они не могут указать, какое именно приложение генерирует или получает его. Это объясняется те, что информация об этом хранится на сетевом (например, IP) уровне сетевого стека, а большинство снифферов использует собственную реализацию стека протоколов (например, библиотеку WinPcap), которая (как уже было показано) работает непосредственно с драйверами устройств.

Использование программы Wireshark

Данный сниффер позволяет в режиме реального времени захватывать пакеты из сети, и анализировать их структуру. Также можно анализировать структуру пакетов из файла, содержащего трафик, полученный, например, программой «tcpdump» (unix/linux).

В стандартном режиме окно снифферa делится на 3 фрейма (панели): список захваченных пакетов, «анализатор» протоколов и исходные данные пакетов. Размер каждого фрейма можно менять по своему усмотрению.
Рассмотрим эти панели подробнее:
Верхняя панель содержит список пакетов, захваченных из сети. Список можно отсортировать по любому полю (в прямом или обратном порядке) – для этого нажать на заголовок соответствующего поля.

Каждая строка содержит следующие поля (по умолчанию):

- порядковый номер пакета (No.);
- время поступления пакета (Time);
- источник пакета (Source);
- пункт назначения (Destination);
- протокол (Protocol);
- информационное поле (Info).

Список отображаемых полей настраивается в Edit/Perferencis/Columns. Для того, чтобы изменения возымели эффект необходимо перезапустить программу, предварительно нажав кнопку Save.
Средняя панель содержит т.н. «дерево протоколов» для выбранного в верхнем окне пакета. В этой панели в иерархическом виде для выбранного в верхнем окне захваченного пакета отображается вложенность протоколов в соответствии с моделью взаимодействия открытых систем OSI. По нажатию на правую кнопку мыши вызывается контекстное меню. При «раскрытии» каждого из протокола нажатием на значек «+» слева, выводятся поля данных соответствующих протоколов.
Нижняя панель содержит шестнадцатеричное представление выбранного пакета. При выборе того или иного поля в средней панели автоматически будет подсвечиваться соответствующий участок 16-ого представления.

Захват пакетов

Для начала захвата пакетов необходимо задать параметры захвата. В частности, указать сетевой интерфейс, с которого и будет осуществляться захват пакетов. Это действие доступно через меню как «Capture–>Options» или комбинации клавиш CTRL+K (см. рис. 2). Интерфейс, задаваемый в поле ***«Interface:»*** можно выбрать из соответствующего поля. В примере на рис. 2. Показано, что доступны 3 интерфейса: физический сетевой адаптер («Marvel…»), и интерфейсы для виртуальных каналов, в частности, установленного VPN-соединения («WAN (PPP/SLIP)…»). В большинстве случае подходит выбор интерфейса сетевого адаптера.

В качестве дополнительных параметров захвата можно указать следующие:

- ***«Capture Filter»*** – фильтр захвата (будем рассматривать далее). По нажатию на соответствующую кнопку можно применить тот или иной фильтр отбора (из ранее сохраненных). Если таковых не имеется, его можно указать явно в строке редактирования.
- ***«Update list of packets in real time»*** **–** обновление списка захваченных пакетов в режиме реального времени.

- ***«Stop Capture»*** – набор параметров, позволяющих задать то или иное значение при достижении, которого процесс захвата пакетов прекратится.
- ***«Name Resolution»*** – набор параметров разрешения имен позволяет определить какие из способов разрешения имен должны использоваться.

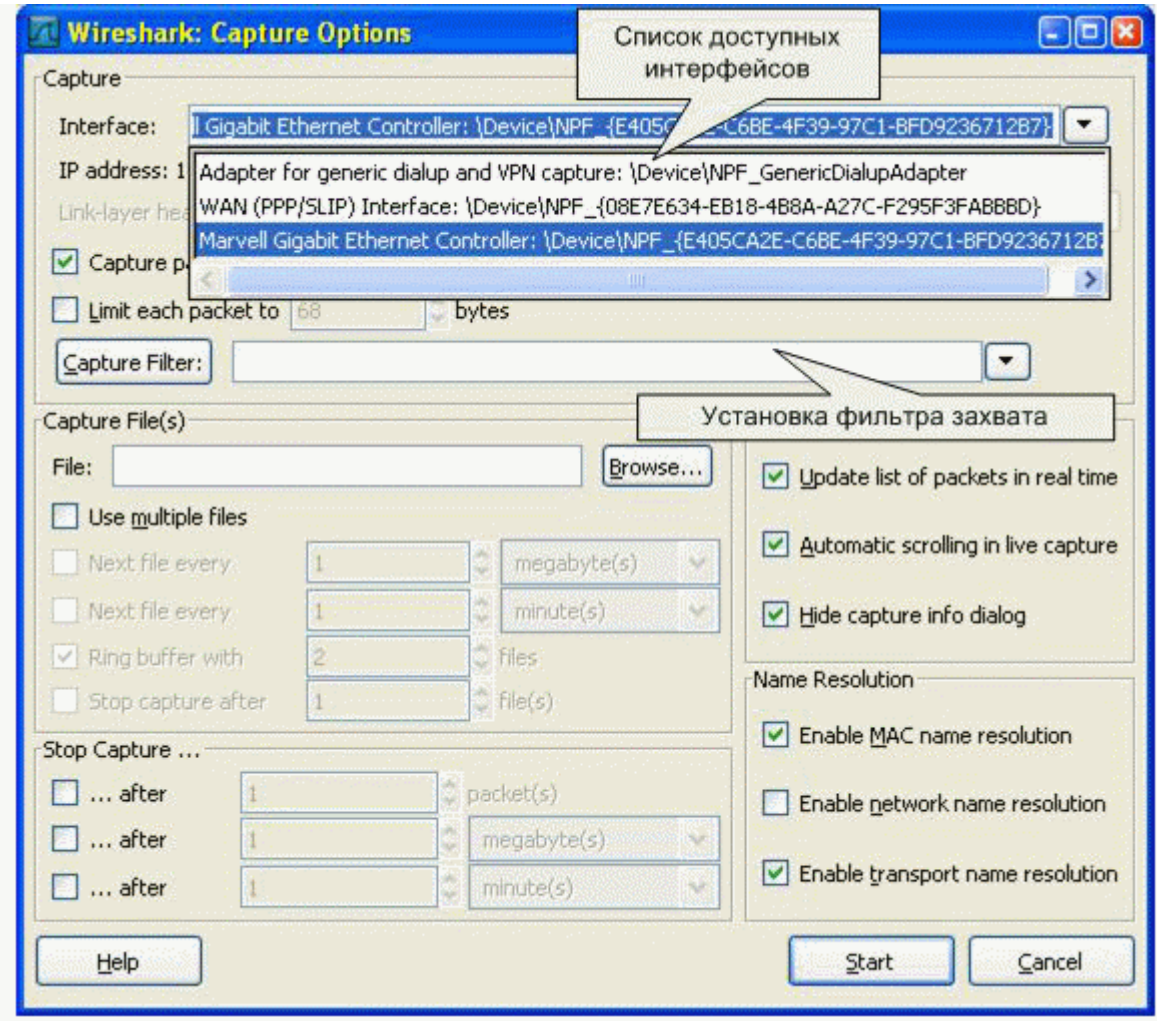

Рисунок 2 – Выбор Интерфейса и параметров захвата пакетов

Если запустить сниффер без дополнительных настроек, он будет «захватывать» все пакеты, проходящие через сетевые интерфейсы (см. рис. 1). Вообще, для общего ознакомления с процессами, происходящими в сети, очень полезно пронаблюдать активность сетевых протоколов в реальных условиях работы системы в сети. Пронаблюдать все разнообразие протоколов, запросов, ответов и др. событий.

При целенаправленном использовании сниффера очень часто необходимо выборочно отображать или захватывать пакеты по некоторым заданным критериям. Для этих целей служат фильтры отображения и захвата,

соответственно.

Типы фильтрации трафика

Существует два варианта фильтрации пакетов: на этапе захвата и на этапе отображения пользователю. В первом случае эффективность работы сниффера и потребляемые им системные ресурсы значительно ниже, нежели во втором случае. Это объясняется тем, что при достаточно интенсивном сетевом трафике и и продолжительном времени захвата все пакеты должны бить захвачеты и сохранены либо в память, либо на дисковое устройство. Самые простые подсчеты могу показать, что даже для 100-мегабитной сети системных ресурсов хватит на непродолжительное время. Фильтрация захвата уже на момент получения пакета гораздо эффективнее, однако в таком случае она должна быть реализована на уровне самих драйверов захвата. Данный факт, естественно, усложняет реализацию сниффера. Wireshark поддерживает оба варианта фильтрации. Рассмотрим

ЗАДАНИЕ:

1. Установить на компьютер программу WinPcap и оболочку к ней Wireshark. Запустить сеанс перехвата пакетов. Запустить для интенсивной генерации кадров браузер и откройте в нем любой сайт по выбору.
2. Установить какой тип кадров Ethernet в данной сети.
3. На основании собранной статистики определить к коммутационному оборудованию какого типа подключен ваш компьютер.
4. Определить, какие типы оборудования могут в принципе использоваться в вашей сети.
5. Рассортировать пакеты по адресам отправителя и получателя. Определите, какие группы кадров по адресам присутствуют в собранной статистике.
6. Найти широковещательные кадры и пакеты. Изучить их заголовки.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Какие типы кадров Ethernet бывают, в чем их отличие?
2. Какой тип кадров Ethernet кадров используется? Почему именно он?
3. Какой тип коммутационного оборудования используется? Обоснуйте ваше мнение.

4. На какой канальный адрес осуществляются широковещательные рассылки?
5. Для чего применяются перехваченные вами широковещательные рассылки?

СПИСОК ИНФОРМАЦИОННЫХ ИСТОЧНИКОВ

1. Сергеев А.Н. Основы локальных компьютерных сетей [Текст]/ А.Н. Сергеев, Изд.: «Лань», 2016. 184 с.
2. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы [Текст]/В.Г. Олифер, Н.А. Олифер. 4-е изд. – СПб.: Питер 2010 -958с.
3. Анализ сетевого трафика как метод диагностики сети. [Электронный ресурс]: / Internet.-http://www.intuit.ru/studies/courses/681/537/lecture/12115 (14.09.2017)
4. Официальный сайт WinPcap. [Электронный ресурс]: / Internet.-https://www.winpcap.org/ (15.09.2017)