Лабораторная работа №7

Доступность информации. Анализ сетевого трафика. Снифферы.

В данной работе предполагается рассмотрение методов обеспечения доступности информации, а также возможности анализа сетевого трафика на примере снифферов.

Что такое IPv4?

IPv4 — это аббревиатура от Internet Protocol version 4 (интернет-протокол версии 4) – представляет собой основной тип адресов, используемый на сетевом уровне модели OSI, для осуществления передачи пакетов между сетями. IP-адреса состоят из четырех байт, к примеру 192.168.100.111.

Присвоение IP-адресов хостам осуществляется:

- вручную, настраивается системным администратором во время настройки вычислительной сети;
- автоматически, с использование специальных протоколов (в частности, с помощью протокола DHCP - Dynamic Host Configuration Protocol, протокол динамической настройки хостов).

Протокол IPv4 разработан в сентябре 1981 года и работает на межсетевом (сетевом) уровне стека протокола TCP/IP. Основной задачей протокола является осуществление передачи блоков данных (дейтаграмм) от хоста-отправителя, до хоста-назначения, где отправителями и получателями выступают вычислительные машины, однозначно идентифицируемые адресами фиксированной длины (IP-адресами). Также интернет-протокол IP осуществляет, в случае необходимости, фрагментацию и сбору отправляемых дейтаграмм для передачи данных через другие сети с меньшим размером пакетов.

Пакеты на уровне IP называются дейтаграммами. Рис. 1 показан формат IP-дейтаграммы.

Октет	0 1 2 3 4 5 6 7	8 9 10 11 12 13 14 15	16 17 18 19 20 21 22 23	24 25 26 27 28 29 30 31
0	Версия	IHL	Тип обслуживания	Длина пакета
4	Идентификатор		Флаги	Смещение фрагмента
8	Время жизни		Протокол	Контрольная сумма заголовка
12	IP-адрес отправителя			
16	IP-адрес получателя			
20	Параметры от 0-я до 10-и 32-х битовых слов			
	Данные			

Рис.1. Формат IP-дейтаграммы.

Перехваченный IPv4 пакет с помощью сниффера Wireshark изображен на рис.2.

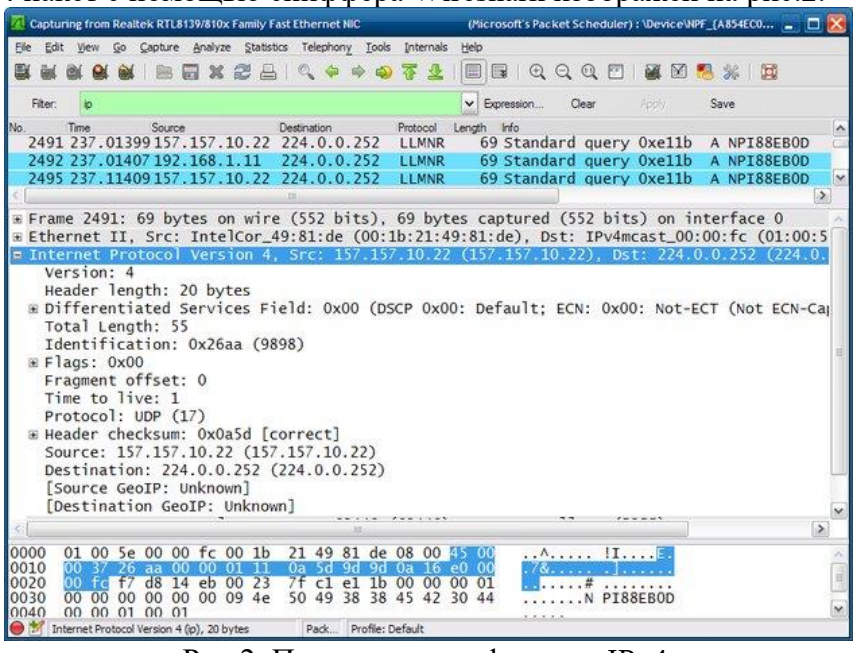

Рис.2. Пример пакета формата IPv4.

"Прослушивание" сетевого трафика

В некоторых случаях для обнаружения проблем функционирования сетевого стека узла и сегментов сети используется анализ сетевого трафика. Существуют средства, которые позволяют отобразить (прослушать) и проанализировать работу сети на уровне передаваемых фреймов, сетевых пакетов, сетевых соединений, датаграмм и прикладных протоколов.

В зависимости от ситуации для диагностики может быть доступен как трафик узла, на котором производится прослушивание сетевого трафика, так и трафик сетевого сегмента, порта маршрутизатора и т. д. Расширенные возможности для перехвата трафика основаны на "беспорядочном" (promiscuous) режиме работы сетевого адаптера: обрабатываются все фреймы (а не только те, которые предназначены данному MAC-адресу и широковещательные, как в нормальном режиме функционирования).

В сети Ethernet существуют следующие основные возможности прослушивания трафика:

- В сети на основе концентраторов весь трафик домена коллизий доступен любой сетевой станции.
- В сетях на основе коммутаторов сетевой станции доступен ее трафик, а также весь широковещательный трафик данного сегмента.
- Некоторые управляемые коммутаторы имеют функцию копирования трафика данного порта на порт мониторинга ("зеркалирование", мониторинг порта).
- Использование специальных средств (ответвителей), включаемых в разрыв сетевого подключения и передающих трафик подключения на отдельный порт.
- "Трюк" с концентратором — порт коммутатора, трафик которого необходимо прослушать, включают через концентратор, подключив к концентратору также узел-монитор (при этом в большинстве случаев уменьшается производительность сетевого подключения).

Существуют программы (сетевые мониторы или анализаторы, sniffer), которые реализуют функцию прослушивания сетевого трафика (в т.ч. в беспорядочном режиме), отображения его или записи в файл. Дополнительно ПО для анализа может фильтровать трафик на основе правил, декодировать (расшифровать) протоколы, считать статистику и диагностировать некоторые проблемы.

Примечание: Хорошим выбором базового инструмента для анализа сетевого трафика в графической среде является бесплатный пакет wireshark , доступный для Windows и в репозиториях некоторых дистрибутивов Linux.

Задание 1.

На коммутаторах D-Link реализована поддержка функции Port Mirroring ("Зеркалирование портов"), которая полезна администраторам для мониторинга и поиска неисправностей в сети.

Функция Port Mirroring позволяет отображать (копировать) кадры, принимаемые и отправляемые портом-источником (Source port) на целевой порт (Target port) коммутатора, к которому подключено устройство мониторинга (например, с установленным анализатором сетевых протоколов) с целью анализа проходящих через интересующий порт пакетов.

В настоящее время анализаторы сетевых протоколов эффективно используются IT-отделами и отделами информационной безопасности для решения широкого круга задач. С их помощью можно быстро определить причину медленной работы IT-сервиса или бизнес-приложения. Они позволяют документировать сетевую активность пользователей и использовать полученные данные, например, для определения источника утечки информации.

Задание 1

1. Запустите анализатор трафика Wireshark.
2. Включите захват пакетов на вашей рабочей станции.
3. Зайдите на сайт с HTTP соединением, например http://phys.asu.ru
4. Проанализируйте полученный трафик, найдите пакеты протокола HTTP.
5. Вставьте в отчет скриншот одного из пакетов. В каком виде передаются данные?
6. Перейдите на сайт с HTTPS соединением.
7. Вставьте в отчет скриншот одного из пакетов. В каком виде передаются данные?

Задание 2

Оборудование:

DES-3200 1 шт.
Рабочая станция 3 шт.
Кабель Ethernet 3 шт.

1. Зайдите через браузер в web-интерфейс коммутатора D-link DES 3200. По умолчанию коммутатор имеет IP адрес 10.90.90.90. Первоначально дайте своему компьютеру адрес в диапазоне 10.90.90.1-255 с маской подсети 255.255.255.0.
2. Изучите настройки коммутатора, вставьте в отчет описание не менее двух пунктов меню со скриншотами.
3. Подключите к коммутатору ещё два компьютера, присвойте им адреса из того же диапазона (примерный вид сети изображен на рис. 3)

Рис.3. Примерная схема локальной сети.

4. Настройте на первый ПК «зералирование», например, подключившись к нему через консоль (возможна команда telnet), можно попробовать настройку через Web-интерфейс.
5. Включите на первом ПК Wireshark.
6. На втором ПК попробуйте команду ping к третьему ПК.
7. Проследите за появлением новых пакетов в программе Wireshark. Пакеты какого протокола захвачены анализатором? Вставьте скриншот в отчёт.

Содержание отчёта:

1. Титульный лист.
2. Скриншоты выполненных заданий с описанием к ним.
3. Вывод.
4. Ответ на контрольные вопросы:
   a. «Человек посередине» — это кто?
   b. Какие снифферы бывают?
   c. Возможен ли перехват трафика в беспроводной сети?