Безопасность сетей

- снифферы (sniffer) -

Проблема

Каждый из нас хочет быть защищенным при посещении Интернета и использования локальных сетей. Для таких целей существует множество программ, антивирусы и фаерволы, но что делать, если ваш трафик перехватывают вне вашего компьютера?

Цель работы

Рассмотреть способы защиты информации от несанкционированного доступа, создать свой метод защиты.

Задачи

1. Выяснить, что такое программы - анализаторы работы компьютерных сетей
2. Изучить как они развивались со времени своего появления и для чего применяются в данный момент
3. Представить способы защиты от применения снифферов злоумышленниками

- Снифферы (sniffer) -

Sniff (англ.) – нюхать, фыркать, втягивать носом.

Слово sniffer зарегистрировала американская фирма Network Associates. Оно является торговой маркой, под которой распространяется программа - анализатор работы компьютерной сети.

Немного из истории снифферов

В основе многих снифферов были и есть сетевые драйверы и библиотеки (libpcap, libnet), которые осуществляют большую часть работы. Для переключения сетевой платы в promiscuous mode требуется низкоуровневое программирование её портов. В многозадачной ОС такую работу могут выполнить только драйверы уровня ядра системы (kernel-mode drivers). Первые программы такого типа были созданы для операционных систем Unix.

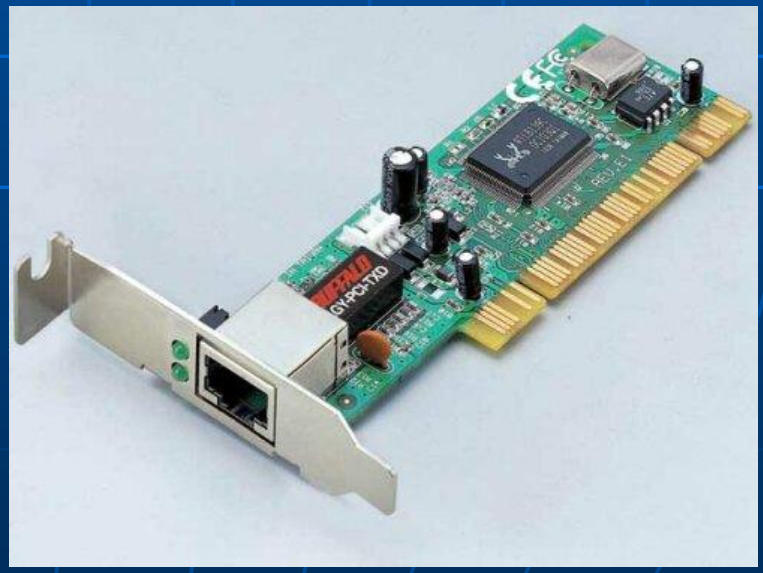
Немного из истории снифферов

Вскоре снифферы перебрались в популярную ОС Windows, но их работа в этой системе также требовала сетевого драйвера, который переключал сетевую плату (NIC – network interface card) в специальный режим. До недавнего времени создание программ - снифферов было уделом квалифицированных специалистов. С появлением Windows2000 создать программу для прослушивания сегмента сети стало совсем просто.

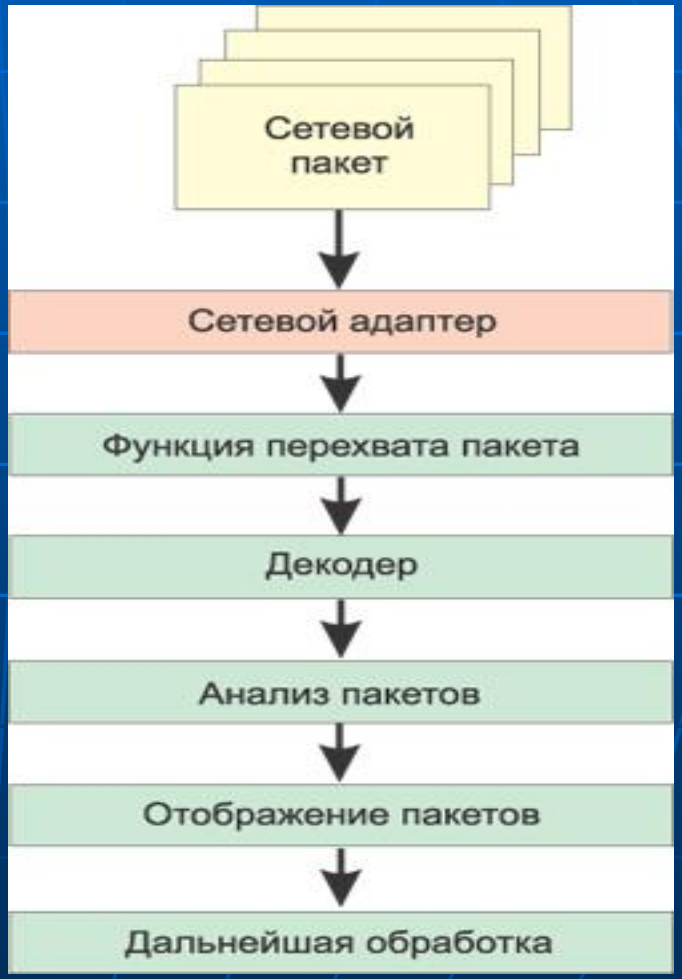
Принцип работы снифферов

Снифферы - это программы, которые перехватывают весь сетевой трафик. Снифферы полезны для диагностики сети (системные администраторы) и для перехвата паролей (хакеры)

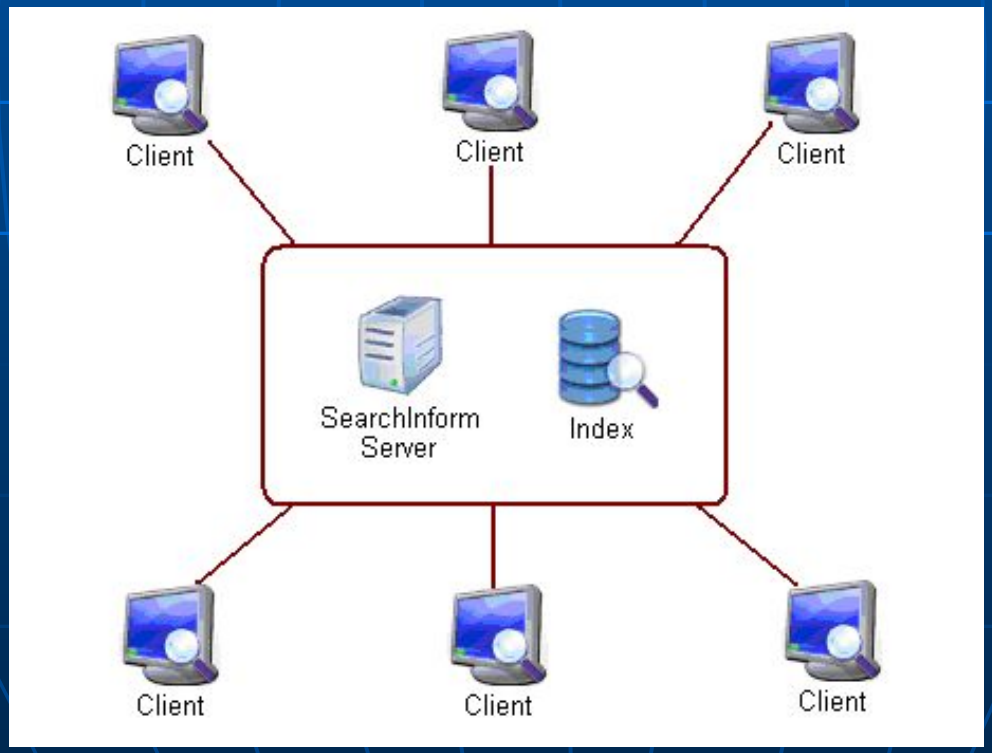
Снифферы ставят сетевую карту в прослушивающий режим (PROMISCUOUS mode - Promiscuous (англ.) – неразборчивый, смешанный.). Они получают все пакеты. В локальной сети можно перехватывать все отправляемые пакеты со всех машин.



Графически показать принцип работы сниффера можно примерно так:



Прослушивание возможно благодаря особенности архитектуры сети Ethernet (IEEE 802.3). Архитектура большинства локальных сетей основана на технологии Ethernet (ether – эфир, network – сеть), в которой все устройства подключены к одной среде передачи данных и совместно её используют. Топология сети Ethernet – линейная или звездообразная, а скорость передачи данных 10, 100 и 1000 Мбит/сек.



Ethernet – это широковещательная сеть, в которой все узлы могут принимать сообщения через единую магистраль. При использовании этой особенности Ethernet отпадает необходимость несанкционированного подключения к сегменту сети, т.е. не требуется резать кабели. Компьютер, с которого предполагается прослушивать, уже подключен к некоторому сегменту сети.

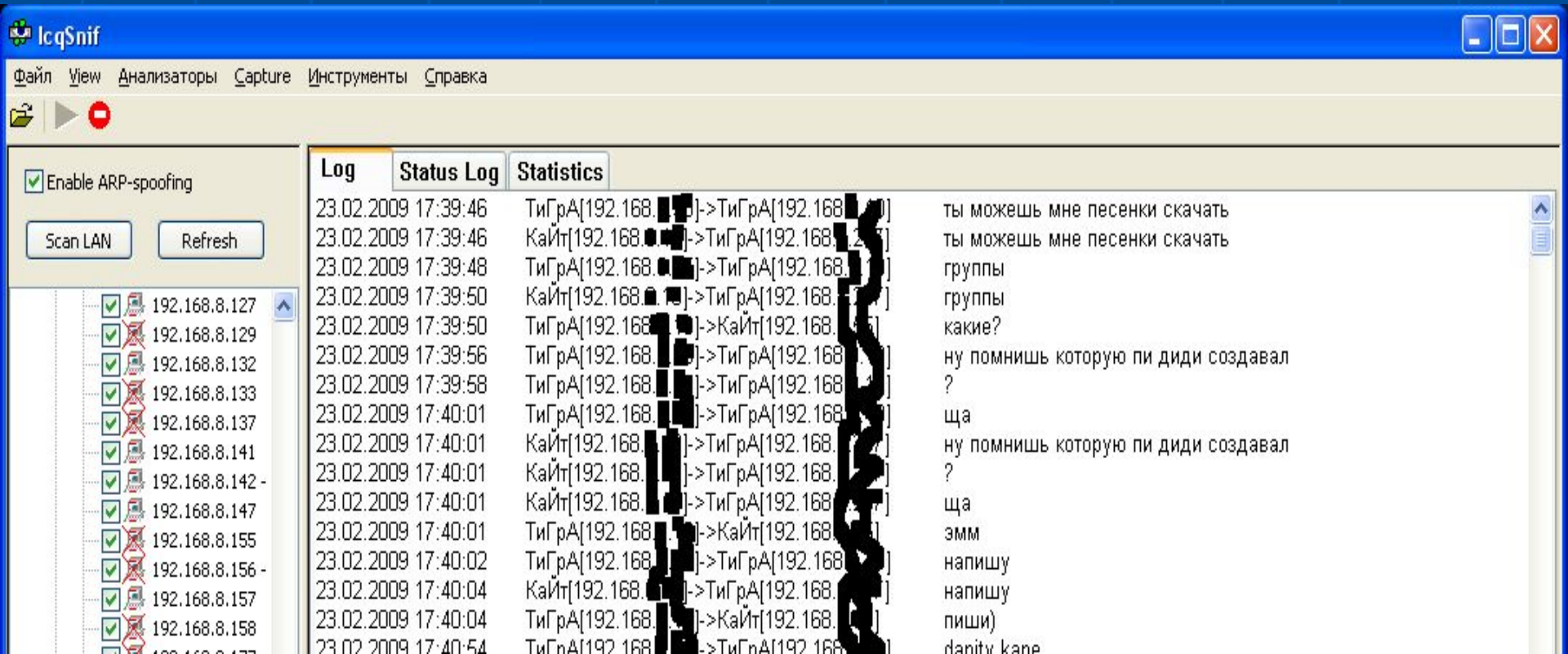
Прослушивающие программы или пакетные анализаторы относятся к классу утилит двойного назначения. С одной стороны, снифферы – мощное оружие, с помощью которого можно осуществить пассивную сетевую атаку. Эти программы могут представлять собой серьезную угрозу, поскольку могут перехватывать и расшифровывать имена и пароли пользователей, конфиденциальную информацию, нарушать работу отдельных компьютеров и сети в целом. Известно, что в большинстве протоколов передачи данных (FTP, POP, HTTP, telnet) секретная информация между клиентом и сервером передаётся открытым текстом.

Злоумышленнику не составляет большого труда получить доступ к чужой информации. Достаточно раздобыть программу - сниффер, настроить её фильтры и ждать, когда жертва будет подключаться к серверу.

С другой стороны, снифферы помогают системным администраторам осуществлять диагностику сети и отслеживать атаки компьютерных хулиганов. Кроме того, они служат для проверки и детального анализа правильности конфигурации сетевого программного обеспечения. Проще сказать, снифферы можно использовать как оружие и как помощь.

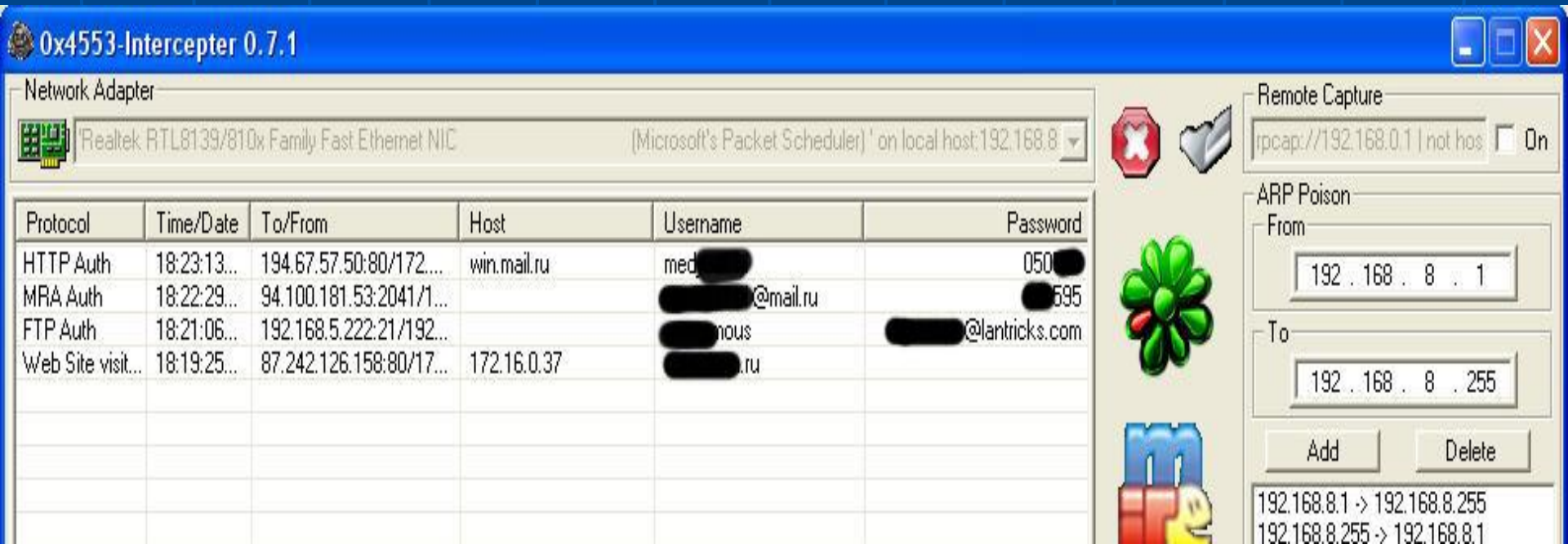
Примеры

Через сниффер возможно перехватить приватную переписку по IRC и Icq. Например, «приват» по IRC в локальной сети г. Шимановска.



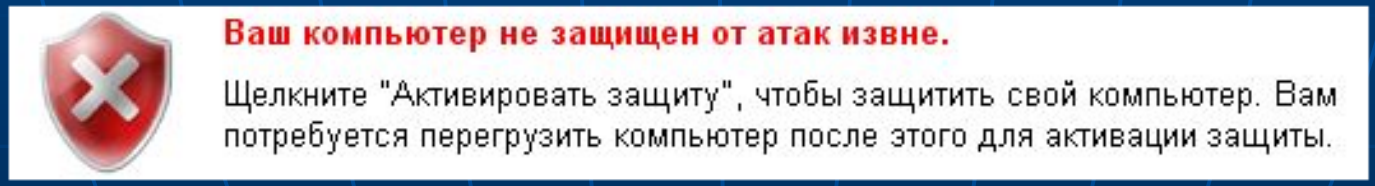
Примеры

Через сниффер возможно перехватить также пароли от разных сайтов и входа в интернет, ftp и т.п. . Например, информация, перехваченная сниффером в локальной сети г.Шимановска.



Защита

В большинстве случаев сниффер все же используют не по назначению, поэтому приходится применять некоторые способы защиты. Таких способов два.

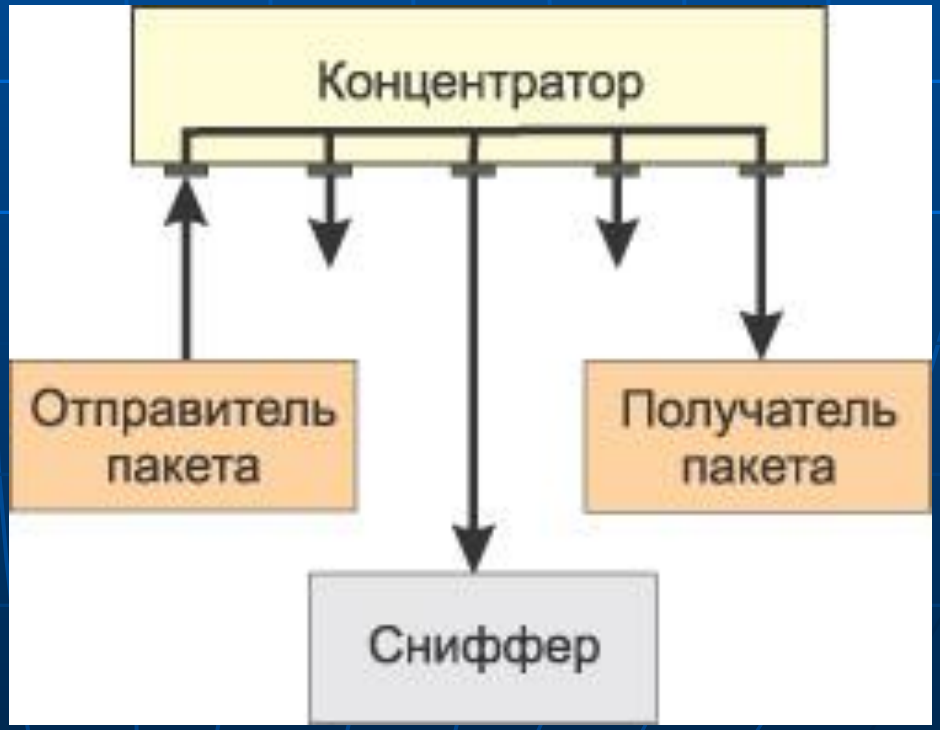


Способ №1

Установить вместо концентраторов (hub) дорогостоящие коммутаторы (switch).

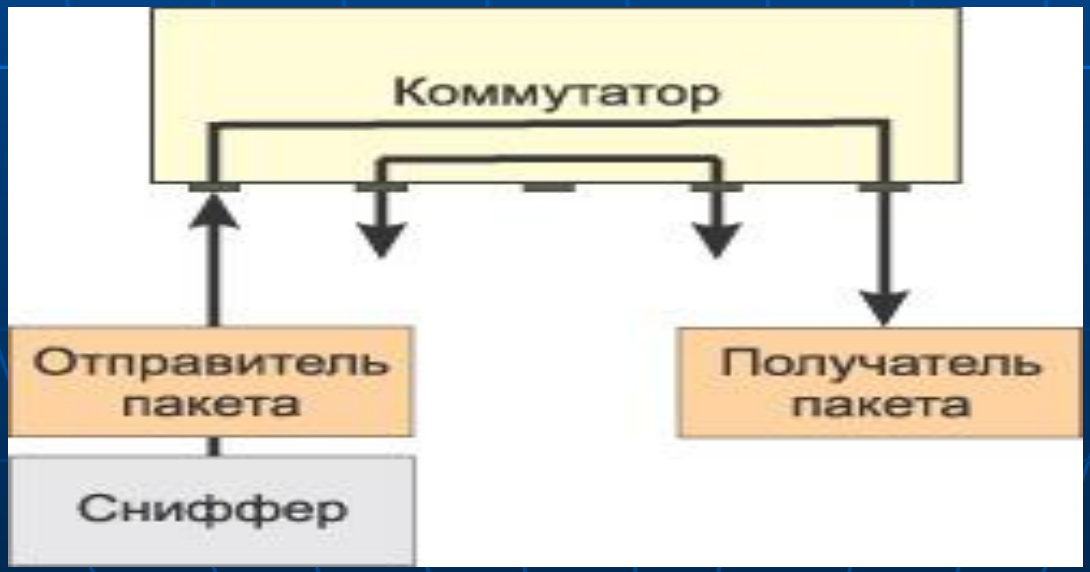
Способ №1

Если сеть основана на хабах (как, например, сеть г.Шимановска), то работа сниффера будет выглядеть примерно так:



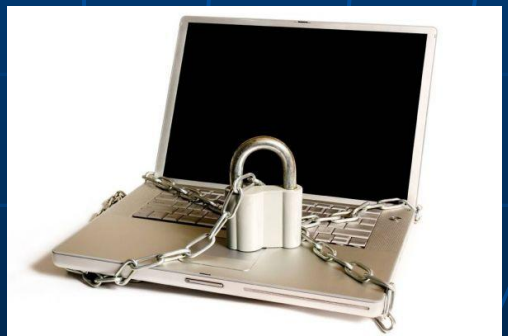
Способ №1

Если же сеть основана на свитчах, то все будет иначе, и пакет уже не будет перехвачен. Все это будет выглядеть примерно так:



Способ №2

Второй способ более надежный и менее дорогостоящий – это шифрование данных. В этом случае сниффер все-таки сможет перехватывать вашу информацию, но не сможет прочитать её. Шифровать можно с помощью технологии SSL (secure sockets layer), которая встроена почти во все браузеры. SSL часто используется в электронной коммерции и вполне надёжна. Но и у этого способа есть недостатки: чем выше будет уровень шифрования, тем меньше будет скорость вашего Интернета.



К сожалению, рядовые пользователи Интернета мало осведомлены, как об угрозе, которую представляют снифферы для их информационной безопасности, так и о способах защиты от них.

При создании данной работы тестировались программы:

IcqSnif v.2.2.5 (условно-бесплатная),

0x4553-Intercepter.v07 (бесплатная)

1. М. Рааб (M.Raab) Защита сетей: наконец-то в центре внимания // Компьютер Москва, 1994, с. 18
2. С.В. Сухова. Система безопасности NetWare // "Cemu", 1995, N4, сс. 6О-70
- Информация об информационном праве
- Борис Леонтьев. Хакеры, взломщики и другие информационные убийцы
- Ярослав Клюкин. Обнаружение пакетных снифферов
- http://www.law.net.ru/index.htm
- http://www.securitylab.ru/software/1220/
- http://sniffs.narod.ru/aneksniff/sniffer3.html
- http://www.inattack.ru/cat_program/2.html
- http://www.shram.kiev.ua/progs/sniff.shtml