



# 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 sniffеров

В основе многих sniffеров 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 sniffеров

Вскоре sniffеры 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 - sniffеров было уделом квалифицированных специалистов. С появлением Windows2000 создать программу для прослушивания сегмента сети стало совсем просто.

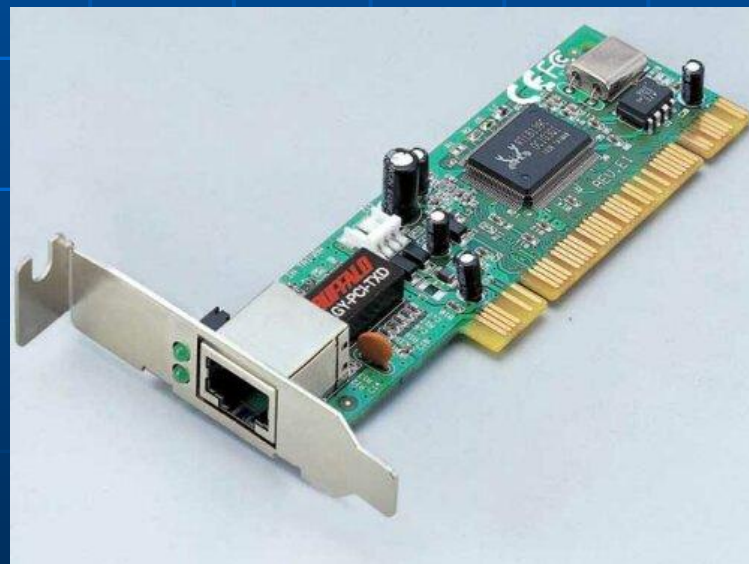
# Принцип работы снифферов

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





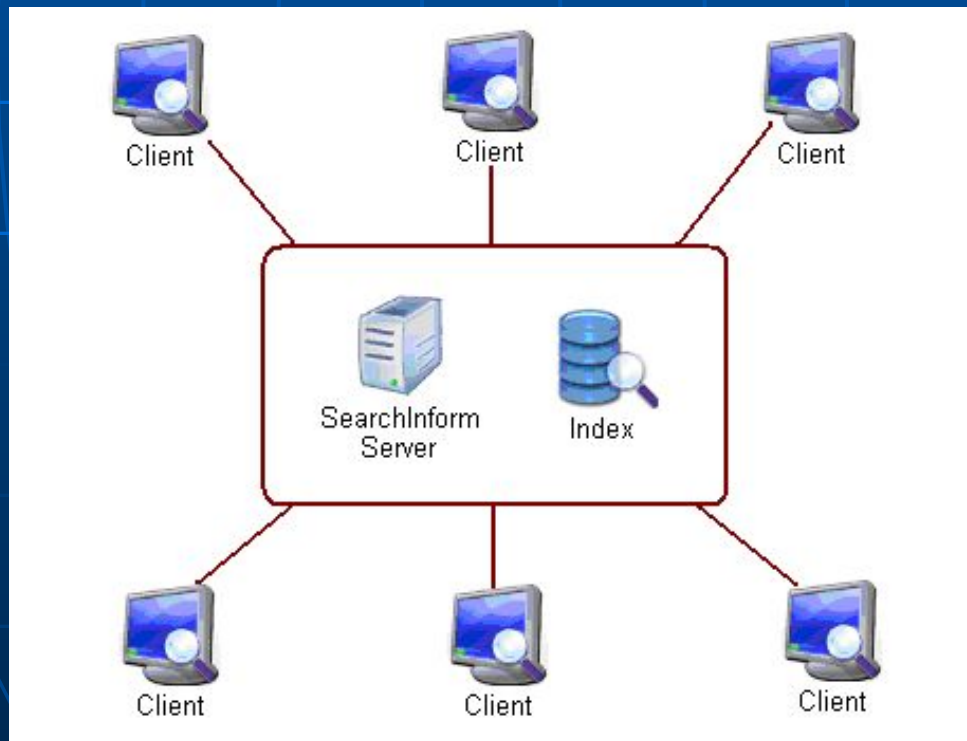
Снифферы ставят сетевую карту в прослушивающий режим (PROMISCUOUS mode - Promiscuous (англ.) – неразборчивый, смешанный.). Они получают все пакеты. В локальной сети можно перехватывать все отправляемые пакеты со всех машин.



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 передается 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.

The screenshot shows the IcqSnif application interface. On the left, there is a list of IP addresses from 192.168.8.127 to 192.168.8.158, each with a checkbox and a small computer icon. The main area is divided into three tabs: Log, Status Log, and Statistics. The Log tab is active, displaying a list of captured messages. The messages are in Russian and appear to be a private conversation. The IP addresses in the log are partially obscured by black redaction boxes.

Log	Status Log	Statistics
23.02.2009 17:39:46	ТигрА[192.168.127]->ТигрА[192.168.127]	ты можешь мне песенки скачать
23.02.2009 17:39:46	Кайт[192.168.127]->ТигрА[192.168.127]	ты можешь мне песенки скачать
23.02.2009 17:39:48	ТигрА[192.168.127]->ТигрА[192.168.127]	группы
23.02.2009 17:39:50	Кайт[192.168.127]->ТигрА[192.168.127]	группы
23.02.2009 17:39:50	ТигрА[192.168.127]->Кайт[192.168.127]	какие?
23.02.2009 17:39:56	ТигрА[192.168.127]->ТигрА[192.168.127]	ну помнишь которую пи диди создавал
23.02.2009 17:39:58	ТигрА[192.168.127]->ТигрА[192.168.127]	?
23.02.2009 17:40:01	ТигрА[192.168.127]->ТигрА[192.168.127]	ща
23.02.2009 17:40:01	Кайт[192.168.127]->ТигрА[192.168.127]	ну помнишь которую пи диди создавал
23.02.2009 17:40:01	Кайт[192.168.127]->ТигрА[192.168.127]	?
23.02.2009 17:40:01	Кайт[192.168.127]->ТигрА[192.168.127]	ща
23.02.2009 17:40:01	ТигрА[192.168.127]->Кайт[192.168.127]	эмм
23.02.2009 17:40:02	ТигрА[192.168.127]->ТигрА[192.168.127]	напишу
23.02.2009 17:40:04	Кайт[192.168.127]->ТигрА[192.168.127]	напишу
23.02.2009 17:40:04	ТигрА[192.168.127]->Кайт[192.168.127]	пиши)
23.02.2009 17:40:54	ТигрА[192.168.127]->ТигрА[192.168.127]	danity kane



# 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.

0x4553-Interceptor 0.7.1

Network Adapter: Realtek RTL8139/810x Family Fast Ethernet NIC (Microsoft's Packet Scheduler) on local host: 192.168.8

Protocol	Time/Date	To/From	Host	Username	Password
HTTP Auth	18:23:13...	194.67.57.50:80/172...	win.mail.ru	med[REDACTED]	050[REDACTED]
MRA Auth	18:22:29...	94.100.181.53:2041/1...		[REDACTED]@mail.ru	[REDACTED]595
FTP Auth	18:21:06...	192.168.5.222:21/192...		[REDACTED]nous	[REDACTED]@lantricks.com
Web Site visit...	18:19:25...	87.242.126.158:80/17...	172.16.0.37	[REDACTED].ru	

Remote Capture: rpcap://192.168.0.1 | not hos  On

ARP Poison

From: 192 . 168 . 8 . 1

To: 192 . 168 . 8 . 255

Add Delete

192.168.8.1 -> 192.168.8.255  
192.168.8.255 -> 192.168.8.1



# Защита

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



**Ваш компьютер не защищен от атак извне.**

Щелкните "Активировать защиту", чтобы защитить свой компьютер. Вам потребуется перезагрузить компьютер после этого для активации защиты.

# Способ №1

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



Защита в ритме прогресса

# Способ №1

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



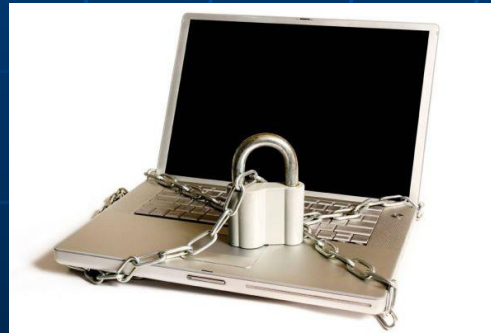
# Способ №1

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:  
IsqSnif 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 // "Сети", 1995, N4, сс. 60-70
  - Информация об информационном праве
  - Борис Леонтьев. Хакеры, взломщики и другие информационные убийцы
  - Ярослав Ключкин. Обнаружение пакетных sniffеров
  - <http://www.law.net.ru/index.htm>
  - <http://www.securitylab.ru/software/1220/>
  - <http://sniffs.narod.ru/aneksniiff/sniffer3.html>
  - [http://www.inattack.ru/cat\\_program/2.html](http://www.inattack.ru/cat_program/2.html)
  - <http://www.shram.kiev.ua/progs/sniff.shtml>