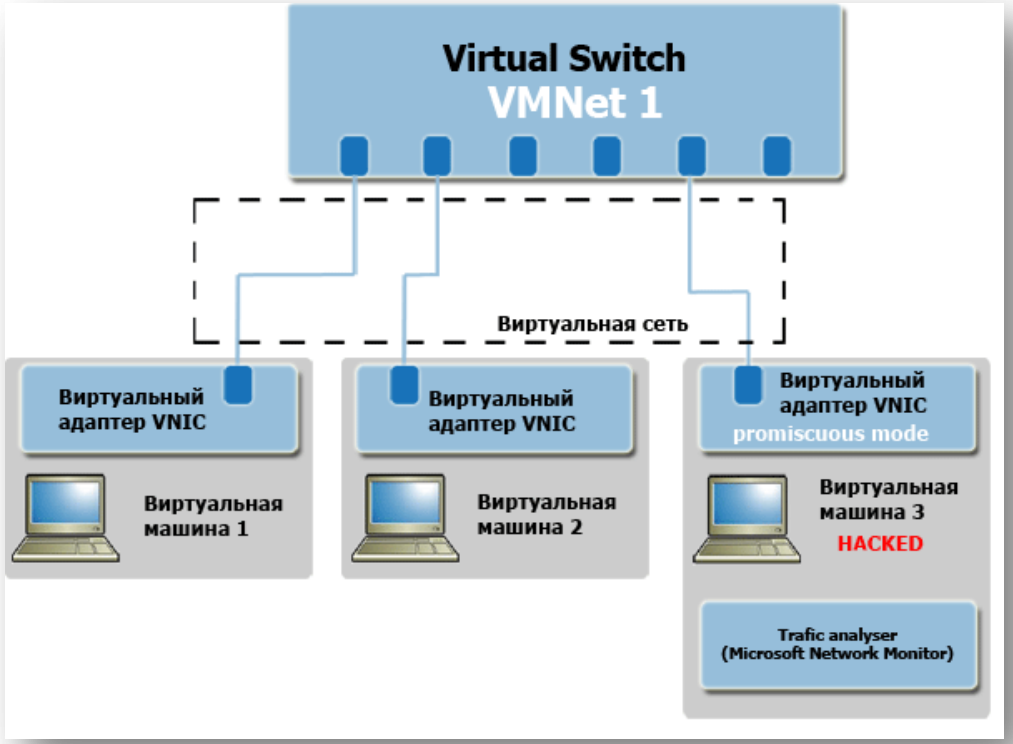
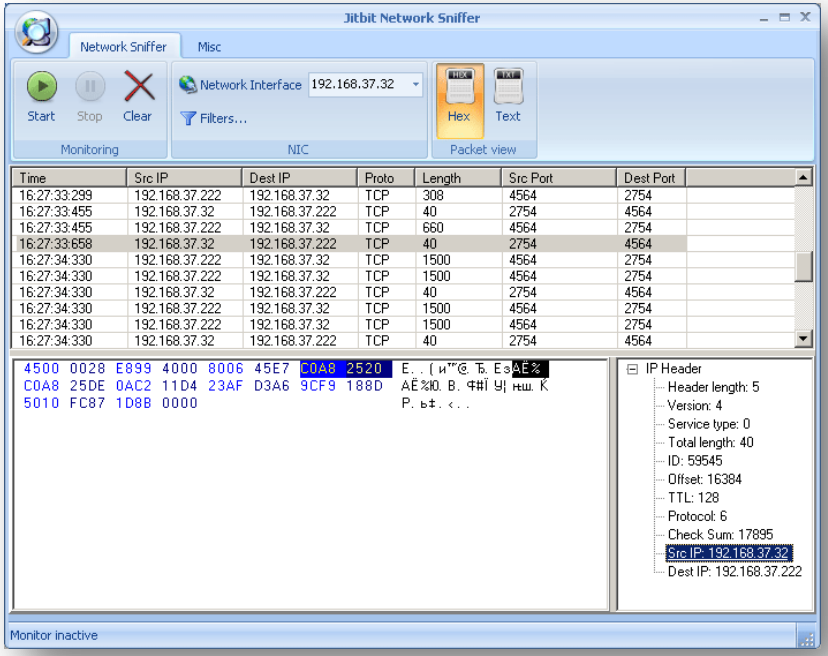
Анализаторы сетевых пакетов

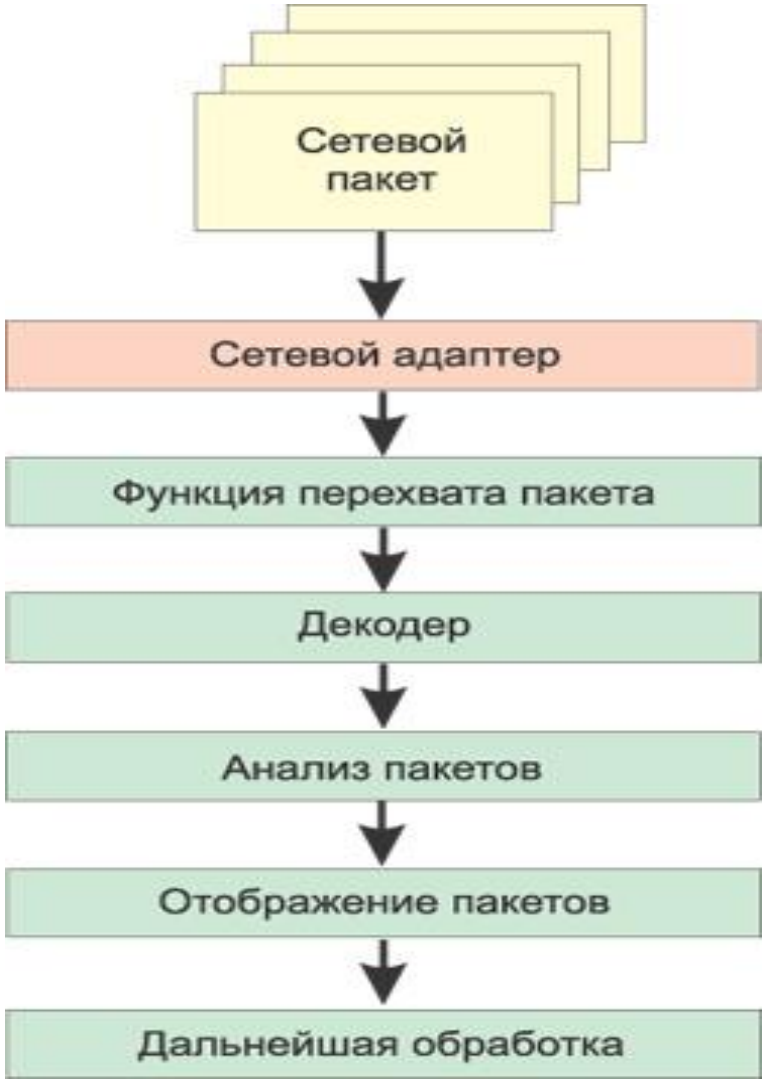


СНИФФЕРЫ

- Анализаторы сетевых пакетов, или снифферы, первоначально были разработаны как средство решения сетевых проблем.
- Они умеют перехватывать, интерпретировать и сохранять для последующего анализа пакеты, передаваемые по сети.

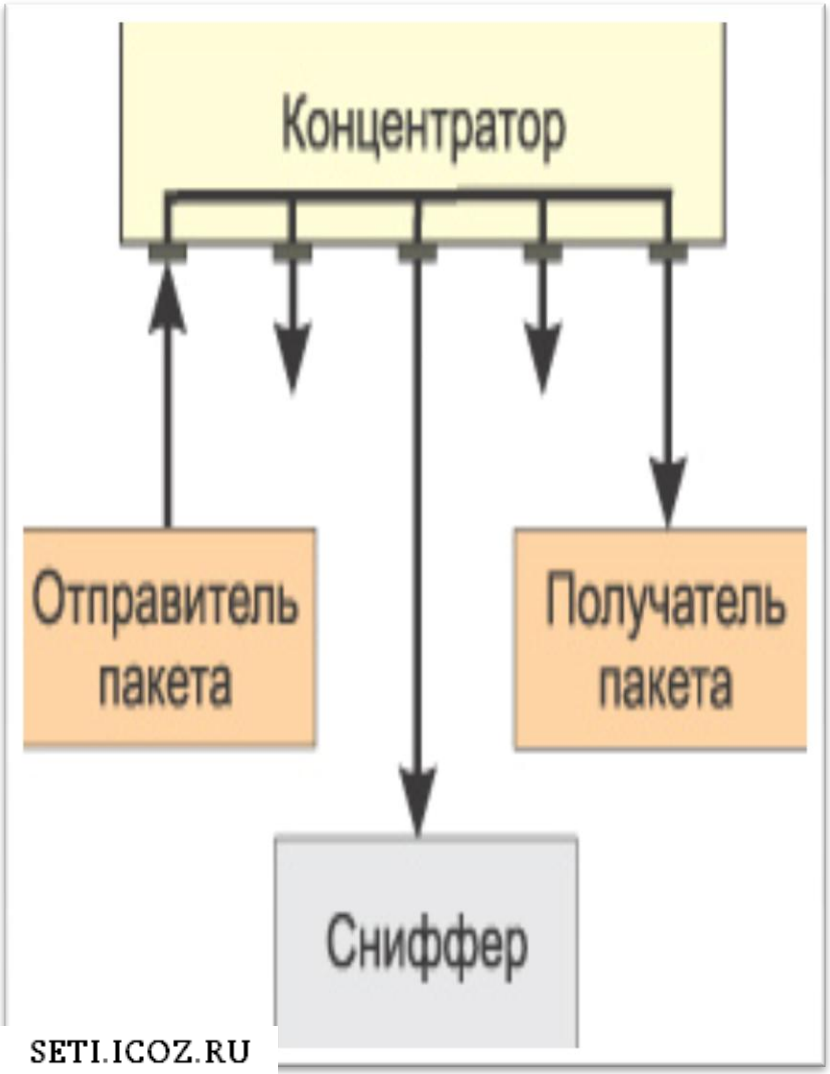


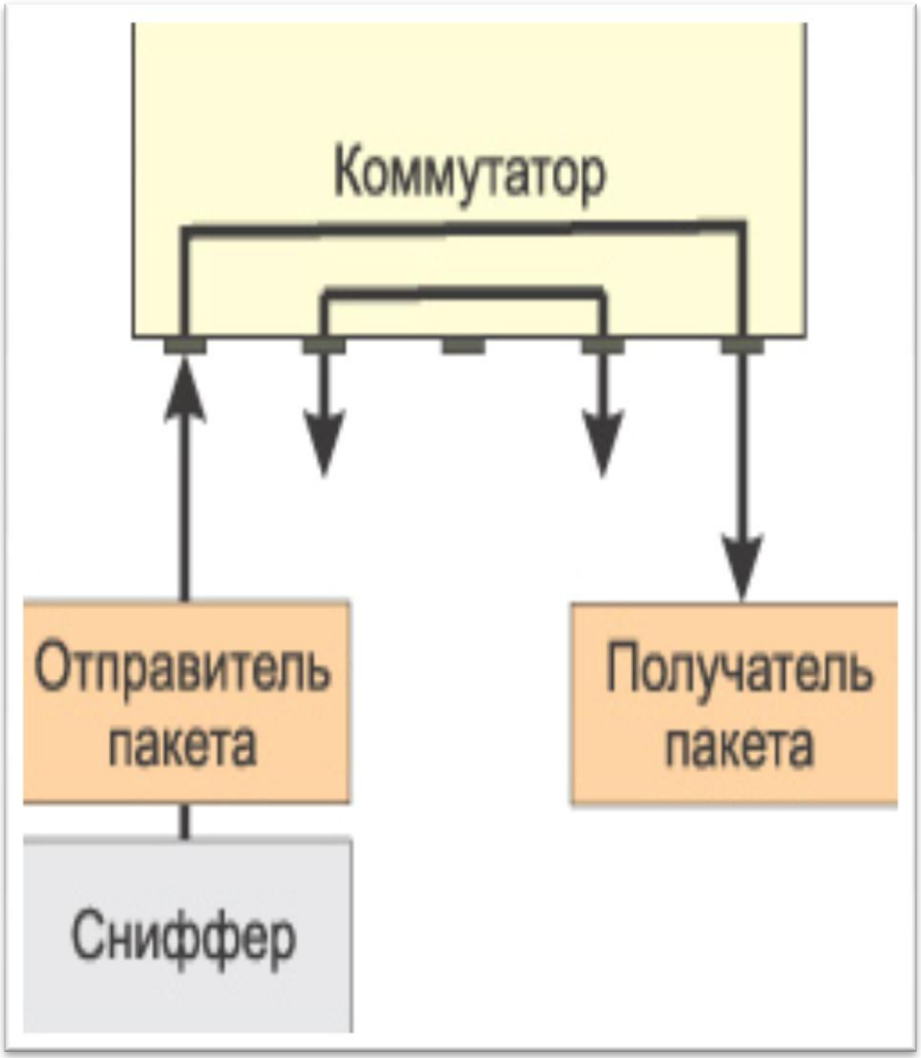
Принципы работы пакетных снифферов



Сниффер — это программа, которая работает на уровне сетевого адаптера NIC (Network Interface Card) (канальный уровень) и скрытым образом перехватывает весь трафик.

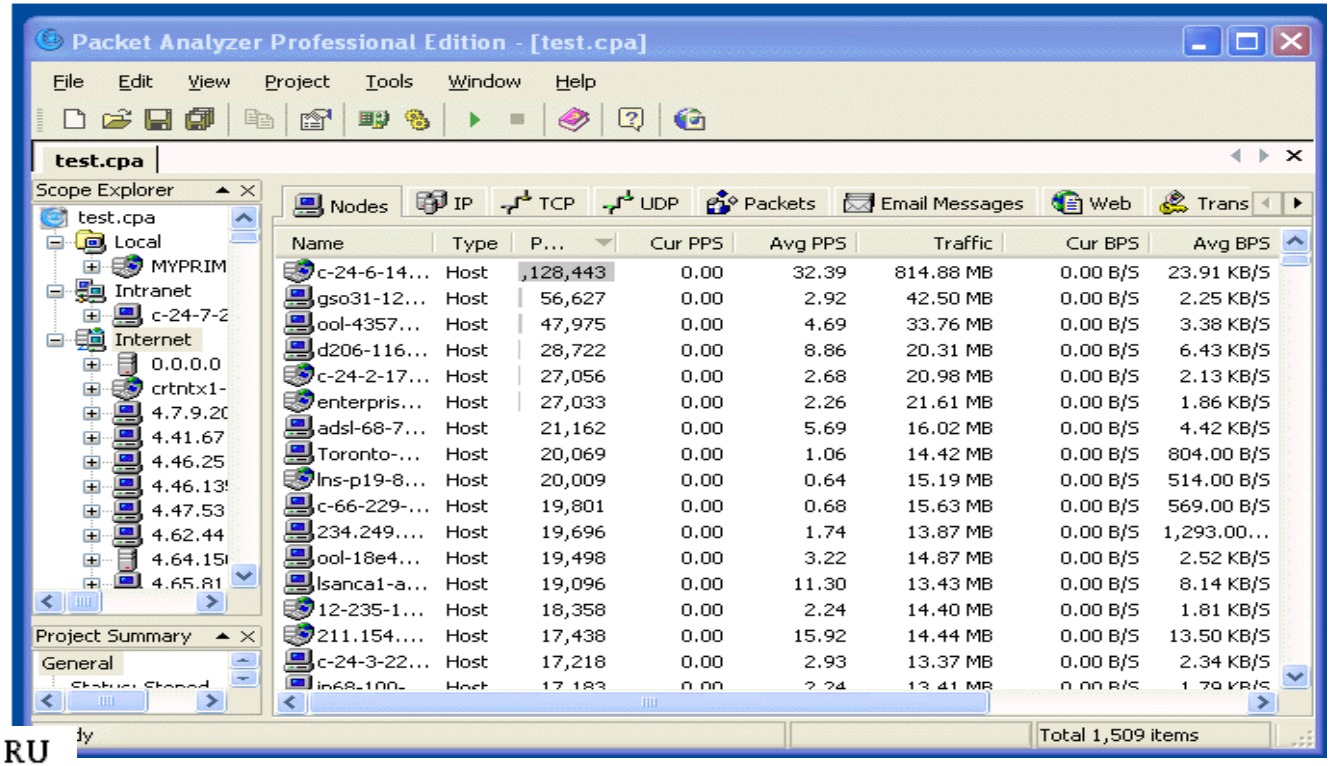
ИСПОЛЬЗОВАНИЯ СНИФФЕРОВ





Методы перехвата сетевого трафика

- Прослушивание сети с помощью программ сетевых анализаторов, является первым, самым простым способом перехвата данных.



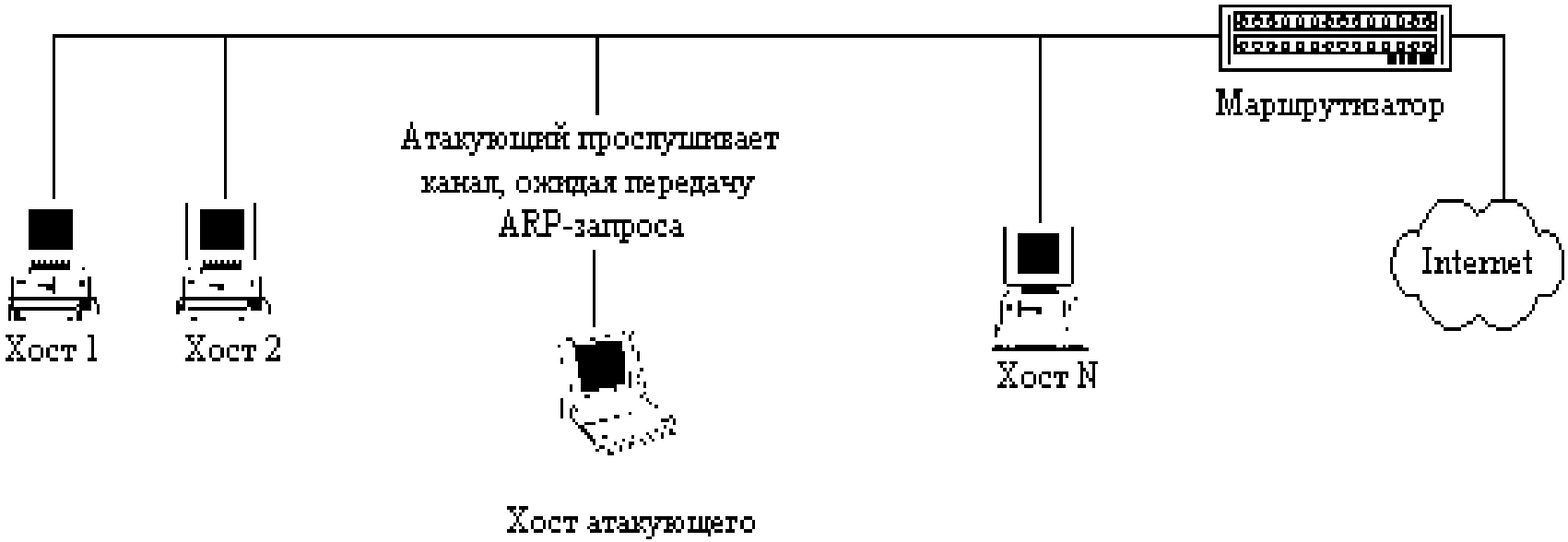
- Для защиты от прослушивания сети применяются специальные программы, например, **AntiSniff** , которые способны выявлять в сети компьютеры, занятые прослушиванием сетевого трафика.

- Программы-антисниферы для решения своих задач используют особый признак наличия в сети прослушивающих устройств - сетевая плата компьютера-снифера должна находиться в специальном режиме прослушивания.

- Находясь в режиме прослушивания, сетевые компьютеры особенным образом реагируют на IP-дейтаграммы, посылаемые в адрес тестируемого хоста.

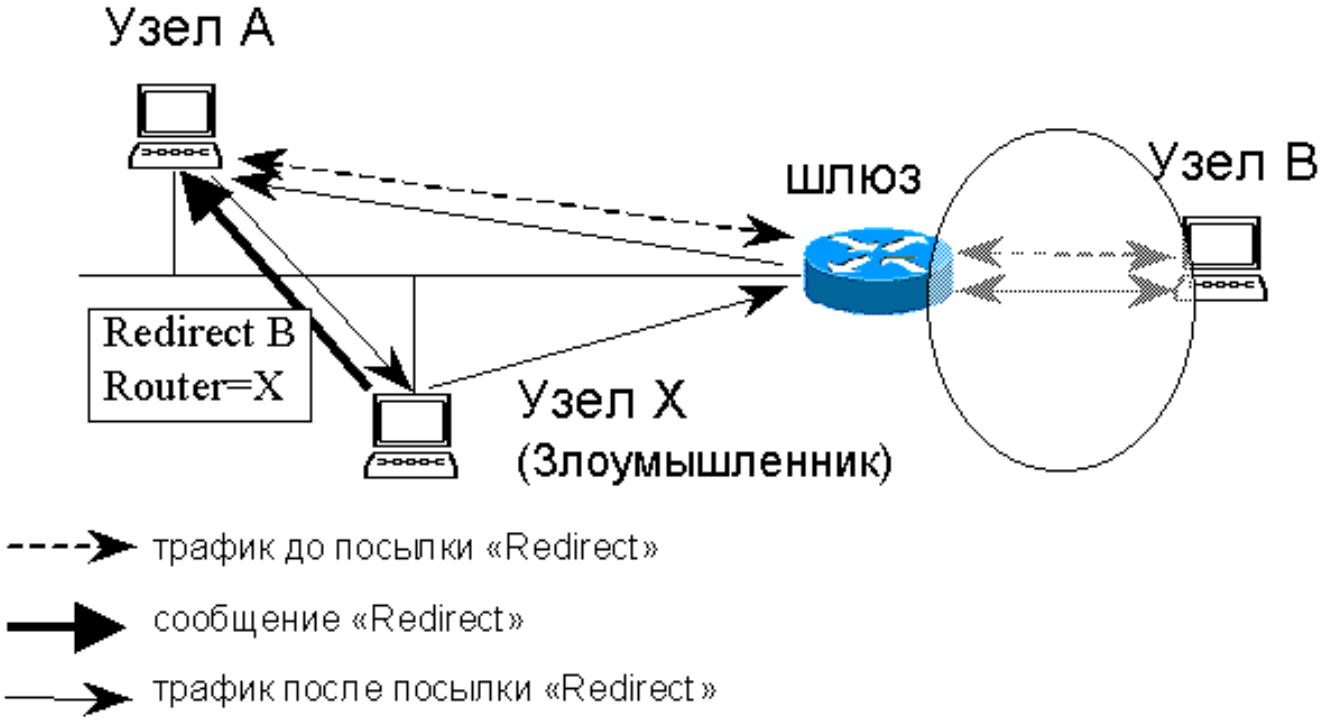
Ложные запросы ARP

- Чтобы перехватить и замкнуть на себя процесс сетевого взаимодействия между двумя хостами A и B злоумышленник может подменить IP-адреса взаимодействующих хостов своим IP-адресом, направив хостам A и B фальсифицированные сообщения ARP (Address Resolution Protocol - Протокол разрешения адресов).



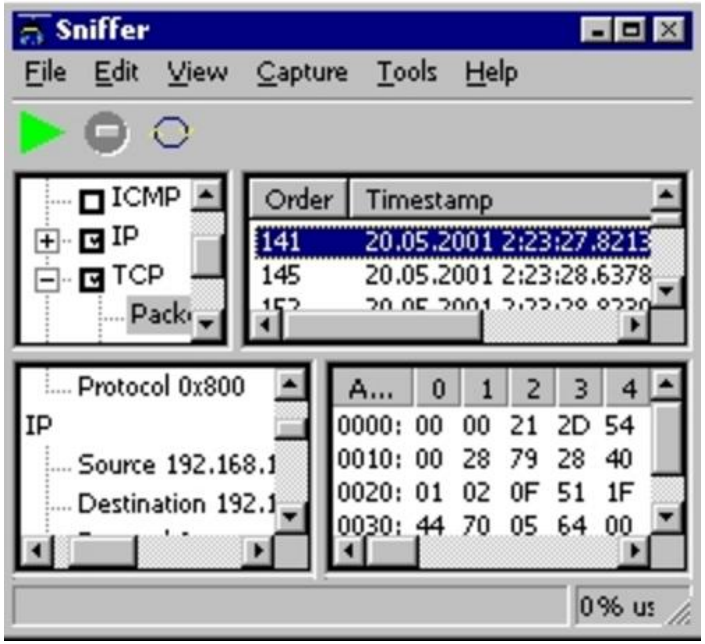
ЛОЖНАЯ МАРШРУТИЗАЦИЯ

- Чтобы перехватить сетевой трафик, злоумышленник может подменить реальный IP-адрес сетевого маршрутизатора своим IP-адресом, выполнив это, например, с помощью фальсифицированных ICMP-сообщений Redirect.



ПЕРЕХВАТ TCP-СОЕДИНЕНИЯ

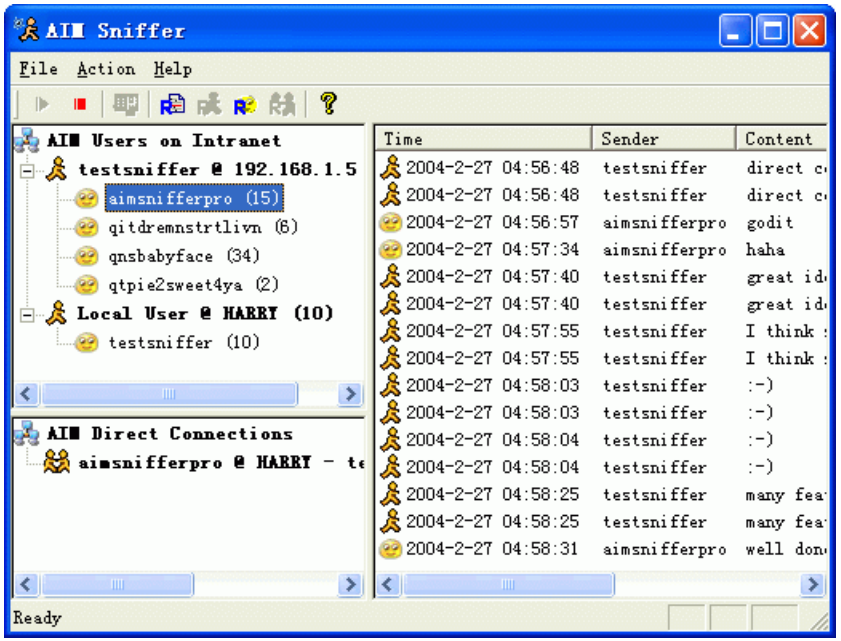
- Захват TCP-соединения (TCP hijacking) –это когда злоумышленник путем генерации и отсылки на атакуемый хост TCP-пакетов прерывает текущий сеанс связи с хостом. Далее, пользуясь возможностями протокола TCP по восстановлению прерванного TCP-соединения, хакер перехватывает прерванный сеанс связи и продолжает его вместо отключенного клиента.



Обзор программных пакетных снифферов

Категории программ-снифферов :

- снифферы, поддерживающие запуск из командной строки,
- снифферы, имеющие графический интерфейс.
- снифферы, которые объединяют в себе обе эти возможности



- Практически все пакетные снифферы позволяют производить анализ декодированных пакетов (именно поэтому пакетные снифферы также называют пакетными анализаторами, или протокольными анализаторами).

- Сниффер распределяет перехваченные пакеты по уровням и протоколам. Некоторые анализаторы пакетов способны распознавать протокол и отображать перехваченную информацию.

- Существуют программные снифферы, к которым в качестве плагинов или встроенных модулей прилагаются программные аналитические модули, позволяющие создавать отчеты с полезной аналитической информацией о перехваченном трафике.

- Другая характерная черта большинства программных анализаторов пакетов — возможность настройки фильтров до и после захвата трафика. Фильтры выделяют из общего трафика определенные пакеты по заданному критерию, что позволяет при анализе трафика избавиться от лишней информации.

Перечень учебных изданий, Интернет-ресурсов, дополнительной литературы использованной при создании презентации

- Учебный курс Основы сетевой инфраструктуры Windows Server 2008 [электронная версия]/ Academy, Softline- 139 с.
- Лимончелли, Т. Системное и сетевое администрирование. Практическое руководство[электронная версия]/ Т.Лимончелли, К. Хоган, С. Чейлап- 2-е издание. – Пер. с англ./– СПб: Символ-Плюс, 2009. – 944 с., ил.
- Журнал о компьютерных сетях и телекоммуникационных технологиях «Сети и системы связи» [Электронный ресурс]. — Режим доступа: URL: http://www.ccc.ru/ (дата обращения: 03.09.12).
- Национальный Открытый Университет «ИНТУИТ» [Электронный ресурс]. — Режим доступа: URL: http://www.intuit.ru/ (дата обращения: 03.09.12).
- Журнал CHIP [Электронный ресурс]. — Режим доступа: URL: http://www.ichip.ru/ (дата обращения: 03.09.12).
- Журнал "Computer Bild" [Электронный ресурс]. — Режим доступа: URL: http://www.computerbild.ru (дата обращения: 03.09.12).