Лабораторная работа № 1
Тема: Ознакомление с программой CommView Remote Agent

Краткие теоретические сведения

Программа CommView Remote Agent предназначена для наблюдения трафика в удалённой сети. Она позволяет пользователям программы CommView анализировать сетевой трафик на компьютере, где запущен Remote Agent, где бы физически этот компьютер ни был расположен.

Достаточно провести установку, несложную конфигурацию, и, CommView Remote Agent готов принять подключение со стороны CommView. Как только соединение будет установлено и произойдёт успешная проверка пароля, CommView Remote Agent сможет собирать трафик в своём сегменте сети и передавать его на CommView. Передаваемые пакеты "сжимаются" для уменьшения нагрузки на сеть и шифруются для обеспечения безопасной передачи по открытым сетям. Программа CommView оснащена гибким набором фильтров, чтобы отсеивать ненужные пакеты, минимизируя служебный TCP трафик между CommView и CommView Remote Agent.

CommView Remote Agent - незаменим для профессионалов в области сетевых технологий, программирования и безопасности, поможет решить широкий круг задач, таких как наблюдение многосегментных сетей или дистанционная отладка сетевых программ.

Порядок выполнения работы

Запустите VirtualBox. Включите виртуальный ПК с Windows XP.

1. **Установка и настройка**

CommView Remote Agent следует устанавливать на компьютер(ах), чей трафик вы намерены отслеживать. Как и CommView, он может захватывать пакеты, проходящие через любой сетевой интерфейс - сетевой адаптер или адаптер удалённого доступа. CommView Remote Agent можно устанавливать как на подключенные к сети, так и изолированные компьютеры.

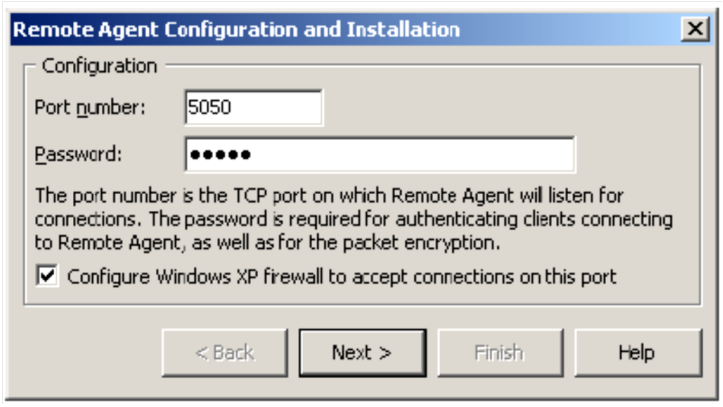
Для установки программы под Windows NT/2000/XP требуются права администратора, после установки и конфигурирования программы - такой уровень привилегий для работы с ней не требуется. Не устанавливайте ОДНОВРЕМЕННО и CommView и CommView Remote Agent на одном и том же компьютере, поскольку это бессмысленно.

Установите программу CommView Remote Agent на виртуальный ПК с Windows XP.

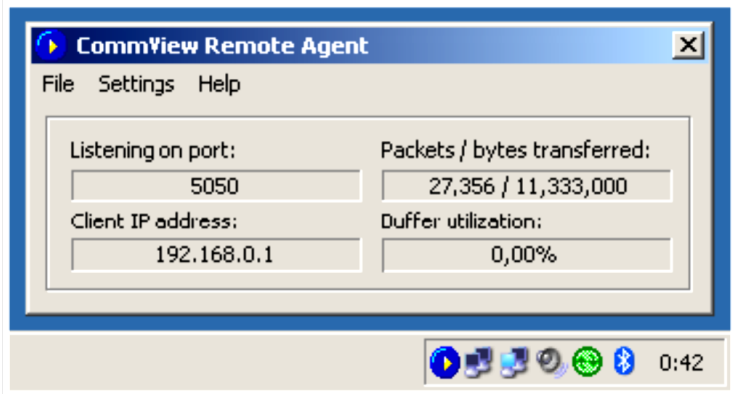
2. **Настройка программы**

Для установки программы - запустите SETUP.EXE и следуйте инструкциям. Когда копирование необходимых файлов завершится, вы увидите окно Установки и Конфигурации (Installation and Configuration), где необходимо указать номер порта TCP и пароль доступа. По умолчанию выбран порт 5050, к нему будет подключаться клиентская программа CommView. Пароль требуется для идентификации клиента и последующей шифрации трафика.

Выбирайте **хороший** пароль (достаточно длинный, содержащий буквенно-цифровые комбинации, который трудно угадать), иначе, если кто-либо посторонний угадает пароль, он получит ПОЛНЫЙ доступ к сетевому трафику данного компьютера.



Нажмите **Next**, чтобы продолжить, программа установит необходимые драйверы и произведёт первый запуск CommViewRemote Agent. Иконка программы появится в панели уведомлений, как показано на рисунке внизу. Для вызова окна приложения CommView Remote Agent, щёлкните по ней:



Поле **Status** показывает состояние программы: номер порта, на котором CommView Remote Agent ожидает подключения, IP адрес подключившегося клиента, статистику передачи пакетов, использование буфера. Поле **Service** содержит несколько настроечных кнопок. Изменить номер порта можно нажав **Change Port**. Изменить пароль можно нажав **Change Password**.

Приостановить и продолжить работу можно нажав соответственно кнопку **Pause** или **Resume**. Нажав на кнопку **About**, можно узнать общие сведения о программе. CommView Remote Agent способен устанавливать только одно клиентское подключение за раз.

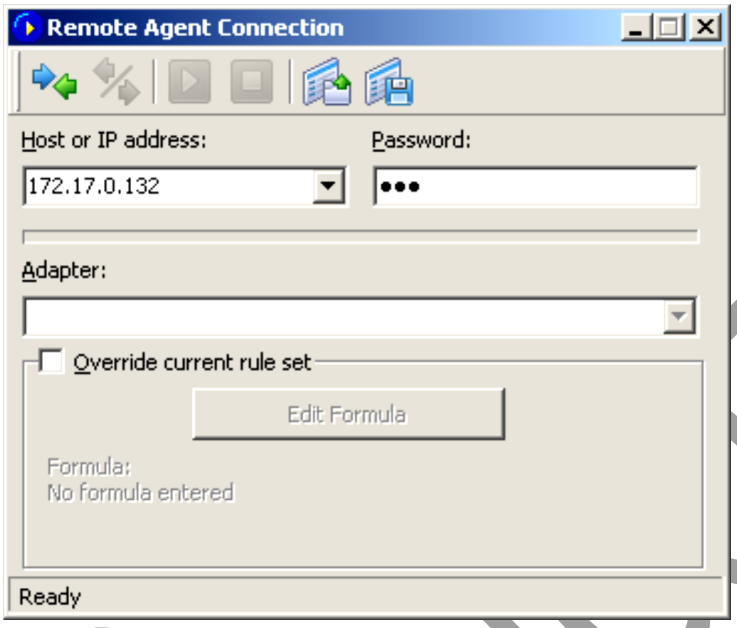
3. Наблюдение за трафиком

3.1. Включите виртуальную машину с сервером Windows Server 2008

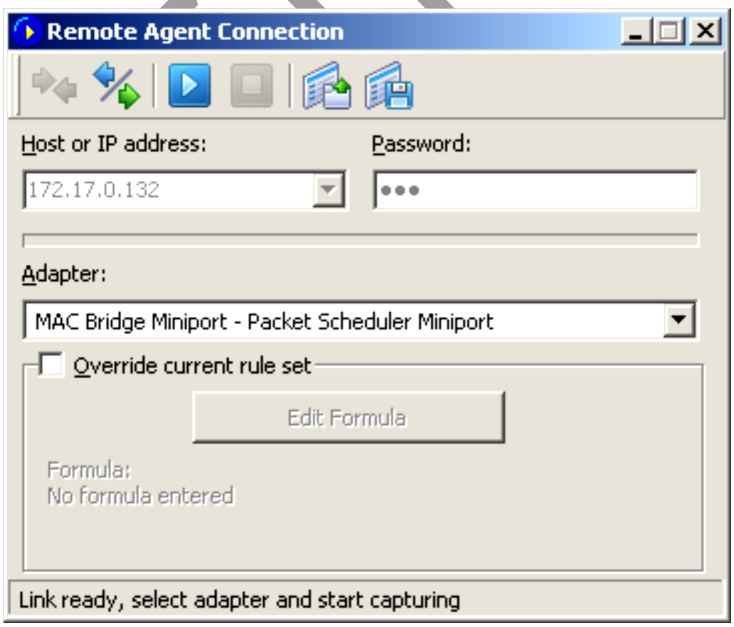
3.2. Установите программу CommView

3.3. Подключение CommView к CommView Remote Agent

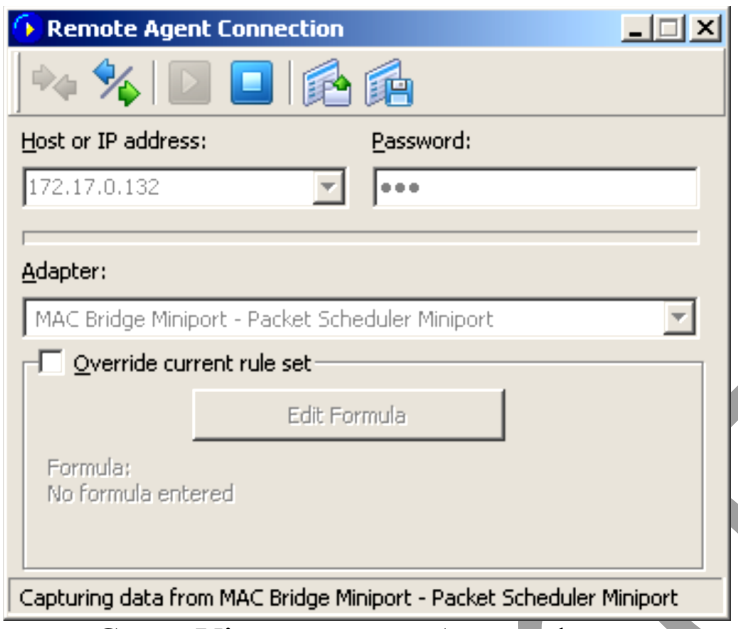
Чтобы включить режим удалённого наблюдения, выберите в меню **File (Файл)** => **Remote Monitoring Mode(Режим удалённого наблюдения)**. В дополнительной панели управления, появившейся под основной, укажите IP адрес компьютера, где запущен CommView Remote Agent, и нажмите кнопку **Connect** (Установить связь). Если вы работаете за брандмауэром (файрволом) или через прокси-сервер, или, если вы установили нестандартный номер порта на Remote Agent, вам придётся, нажав кнопку **Network Settings** (Сетевые установки), указать порт и/или ввести настройки прокси- сервера SOCKS5.



Во всплывающем окне укажите пароль доступа, заданный в установках Remote Agent. Если пароль указан верно, соединение будет сразу же установлено. Появится сообщение Link Ready(Связь подготовлена), а в списке доступных адаптеров появятся все имеющиеся на удалённом компьютере адаптеры.



Теперь необходимо установить правила в закладке **Rules(Правила)**. Важно настроить их так, чтобы не превысить пропускную способность канала связи между Remote Agent и CommView, иначе вы заметите существенное замедление реакции системы. Обязательно отфильтровывайте не интересующие вас пакеты (см. ниже). Когда всё готово, выберите в списке нужный адаптер и нажмите кнопку **Start Capture** (Начать сбор).



CommView начнёт сбор трафика удалённого компьютера, как если бы это был ваш локальный трафик, практически, нет разницы между этими двумя режимами работы CommView. Чтобы закончить удалённое наблюдение, нажмите кнопку **Stop Capture**. Можно или выбрать другой адаптер из списка или отключится от Remote Agent совсем, нажав кнопку **Disconnect**.

Чтобы вернуться в стандартный режим, выберите в меню **File(Файл)** => **Remote Monitoring Mode(Режим удалённого наблюдения)**, и дополнительная панель управления исчезнет.

Проверьте соединение между сервером и клиентской машиной с помощью команды ping.

Просмотрите содержимое анализа соединения в программе CommView на сервере:

1. Закройте окно Соединение с удаленным агентом
2. В окне программы CommView щелкните по вкладке Текущие IP-соединения (должна быть активна по умолчанию)
3. Двойным кликом мышки откройте локальный IP-адрес
4. В открывшемся окне справа выберите протокол и просмотрите информацию о соединении.
5. Запишите в тетрадь для лабораторных работ сл. Информацию:
    a. Какой версии протокол используется для соединения?
    b. Какой размер фрейма?
    c. Запишите номер IP-адреса ПК, чей трафик просматривается программой

Контрольные вопросы

1. Может ли CommView быть использован для перехвата dial-up (RAS) трафика?
2. Что может "видеть" CommView, которая инсталлирована на компьютер с локальной сетью?
3.
4. Я подключен к LAN через switch и, когда я запускаю CommView, он ловит только пакеты, идущие к/от меня, я не вижу трафика других машин. Почему?
5. Я подключен к сети через hub, но не вижу чужого трафика, как если бы это был switch. Почему?
6. Может ли CommView собирать данные на адаптере, который не имеет своего IP-адреса?
7. Я работаю в локальной сети с большим объемом трафика, и поэтому мне сложно изучать отдельные пакеты, когда программа принимает сотни и тысячи пакетов в секунду, и старые пакеты быстро исчезают из циркулярного буфера. Можно с этим что-нибудь сделать?
8. Я подключен к сети через cable/xDSL-модем. Будет ли CommView осуществлять мониторинг трафика в этом случае?
9. Как установить захват пакетов по расписанию?
10. Возможен невидимый режим данной программы? Если да, то как его настроить?