МОНИТОРИНГ СЕТИ НА ФИЗИЧЕСКОМ УРОВНЕ

Романов Сергей Андреевич
КНИТУ-КАИ, Казань, студент
rsa5325@yandex.ru

Аннотация. В статье рассматриваются проблемы мониторинга сети: причины, способы мониторинга, способы борьбы с несанкционированным мониторингом сетей.

Применение на практике

Причины применения мониторинга за сетью.

Например, сеть состоит из трех компьютеров a, b и c. На компьютере a запущен сетевой анализатор, и вы можете наблюдать не только входящий/исходящий трафик на компьютере a, но и данные, проходящие между компьютерами b и c. Это типовая ситуация при работе с сетевыми анализаторами, системами учета трафика и мониторинга сетевого контента. В принципе, вы можете запустить эти программы на каждом компьютере, но это довольно неудобно, поскольку у вас перед глазами не будет всей полноты картины.

Способы мониторинга Ethernet

Мониторинг с помощью хабов

Из-за достаточно низкой стоимости в небольших сетях чаще используются хабы нежели коммутаторы, что позволяет использовать их особенность ретрансляции поступающих данных на все порты в promiscuous мониторинге. Помимо этого некоторые виды хабов могут не позволить вести полноценный мониторинг своего сегмента сети.

1) Компьютер, подключенный к хабу

Любой компьютер, подключенный к хабу, может использоваться для мониторинга, поскольку хаб передает принятые/переданные данные от маршрутизатора на все порты. Достаточно лишь отключить на компьютере фильтрацию данных, направляемых по другим IP-адресам. Также отметим, что возможен мониторинг обмена между локальными ПК.

2) Хаб между маршрутизатором и коммутатором

Есть возможность наблюдать данные, передаваемые и получаемые из Интернета, но данные, которыми обмениваются локальные компьютеры внутри ЛВС, вам недоступны.

3) Мониторинг локальной сети без коммутатора

Топология малых компьютерных сетей предусматривает совмещение маршрутизатора и коммутатора, к которому подключаются остальные компьютеры (терминалы). Для мониторинга всех данных, передаваемых или принимаемых из Интернета, можно установить хаб между внешней сетью и маршрутизатором, тогда можно будет узнать даже передаваемые скрытым путем данные. Важно отметить, что программа сетевого мониторинга не сможет различать трафик от разных рабочих станций до тех пор, пока у этих рабочих станций, находящихся за маршрутизатором, не будет трассируемых ip-адресов. Если у них нет трассируемых ip-адресов, то все пакеты будут иметь один ip-адрес – это публичный ip-адрес вашей сети. Компьютер для мониторинга должен быть абсолютно пассивным и не передавать данных в сеть, то есть интерфейс должен только принимать данные. Этого можно достичь путем назначения достичь путем назначения сетевой карте нетрассируемого IP-адреса.

Мониторинг с помощью коммутаторов

Для сетевого мониторинга подходил управляемый коммутатор с поддержкой зеркалирвания портов. Функция зеркалирования позволяет перенаправлять трафик с любых портов на один определенный порт коммутатора.

Есть два типичных способа зеркалирования портов:

1) Использование коммутатора с зеркалированием портов

Главный коммутатор обладает способностью зеркалировать порты на определенный порт. Подключаем компьютер к «зеркальному» порту, на который производится перенаправление трафика с ЛВС. Причем, можно зеркалировать трафик не с одного, а с нескольких портов коммутатора.

2) Использование неконтролируемых коммутаторов в сети

При использовании в сети неконтролируемых коммутаторов, не поддрживающих зеркалирование портов, невозможно подключить к ним контролируемый коммутатор. Максимально возможное в данном случае: подключиться к коммутатору, подключенному к Интернету (они, чаще всего, поддерживают зеркалирование портов) и перехватывать трафик между ЛВС и сетью Интернет. Но будет недоступна информация, передаваемая внутри ЛВС между рабочими станциями. Некоторые коммутаторы, не поддерживающие зерклирование пор-

тов, могут быть использованы для мониторинга в режиме "promiscuous", но в таком случае в результате реализации arp флуда" или arp спуффинга, коммутатор начинает рассылать пакеты по всем портам

Рекомендации по выбору конфигурации сети:

1) Использование отдельного терминала для мониторинга. Мониторинг сети является задачей, требующей больших ресурсов, при обработке данных и трафика, что создает большую нагрузку на процессор. В связи с этим рекомендуется выполнять эту задачу на отдельном компьютере.

2) Использование вместо хабов, ретранслирующих данные на все порты, управляемых коммутаторов, транслирующих трафик на отдельный порт, что снижает нагрузку в сети и риск несанкционированного мониторинга.

Удаленный мониторинг

Способы удаленного мониторинга:

1) Использование программ для удаленного доступа позволяет, которые получили широкое распространение в виду простоты их использования (microsoft remote desktop connection и terminal services, TeamViewer

2) Использование удаленных сетевых модулей. Подключившись к одному или к нескольким удаленным агентам из одного центра, администратор видит в своей программе мониторинга весь трафик с удаленных машин в режиме реального времени. Что дает одновременное подключение сразу ко многим удаленным модулям и возможность анализировать/сохранять данные на вашем компьютере.

Способ мониторинга на базе двух сетевых карт.

На внешней сетевой карте настраивается режим «promiscuous». Promiscuous mode или promisc mode — так называемый «неразборчивый» режим, в котором сетевая плата позволяет принимать все пакеты независимо от того, кому они адресованы. По умолчанию сетевое оборудование игнорирует трафик, адресованный не ему путем сравнения заголовков пакетов. В более широком смысле режим promiscuous также означает прозрачность сети с определенной точки наблюдения, но при этом не подразумевается обязательного перевода адаптеров в данный режим. В современном оборудовании и программном обеспечении часто реализованы и другие способы мониторинга для достижения полной видимости всех сетевых процессов.

Список источников

1. Техника и философия хакерских атак. М.: СОЛОН-Р, 1999, ISBN 5-93455-015-2

2. Лаем Куин, Ричард Рассел Fast Ethernet, bhv, Киев, 1998. ISBN 5-7315-0014-2 (англ: ISBN 0-471-16998-6)

3. Техника сетевых атак. М.: СОЛОН-Р, 2001, ISBN 5-93455-078-0