УДК 004.681

Мороз Е.С.

МОНИТОРИНГ СЕТЕЙ

Для мониторинга сетевого трафика используют так называемые анализаторы сетевых пакетов, или снифферы, которые первоначально были разработаны как средство решения сетевых проблем. Они умеют перехватывать, интерпретировать и сохранять для последующего анализа пакеты, передаваемые по сети. С одной стороны, это позволяет системным администраторам и инженерам службы технической поддержки наблюдать за тем, как данные передаются по сети, диагностировать и устранять возникающие проблемы. В этом смысле пакетные снифферы представляют собой мощный инструмент диагностики сетевых проблем. С другой стороны, подобно многим другим мощным средствам, изначально предназначавшимся для администрирования, с течением времени снифферы стали применяться абсолютно для других целей. Действительно, сниффер в руках злоумышленника представляет собой довольно опасное средство и может использоваться для завладения паролями и другой конфиденциальной информацией. Однако не стоит думать, что снифферы — это некий магический инструмент, посредством которого любой хакер сможет легко просматривать конфиденциальную информацию, передаваемую по сети. И прежде чем доказать, что опасность, исходящая от снифферов, не столь велика, как нередко преподносят, рассмотрим более детально принципы их функционирования.

Принципы работы пакетных снифферов

В дальнейшем в рамках данной статьи мы будем рассматривать только программные снифферы, предназначенные для сетей Ethernet. Сниффер — это программа, которая работает на уровне сетевого адаптера NIC (Network Interface Card) (канальный уровень) и скрытым образом перехватывает весь трафик. Поскольку снифферы работают на канальном уровне модели OSI, они не должны играть по правилам протоколов более высокого уровня. Снифферы обходят механизмы фильтрации (адреса, порты и т.д.), которые драйверы Ethernet и стек TCP/IP используют для интерпретации данных. Пакетные снифферы захватывают из провода все, что по нему приходит. Снифферы могут сохранять кадры в двоичном формате и позже расшифровывать их, чтобы раскрыть информацию более высокого уровня, спрятанную внутри (рис. 1).

Для того чтобы сниффер мог перехватывать все пакеты, проходящие через сетевой адаптер, драйвер сетевого адаптера должен поддерживать режим функционирования promiscuous mode (беспорядочный режим). Именно в этом режиме работы сетевого адаптера сниффер способен перехватывать все пакеты. Данный режим работы сетевого адаптера автоматически активизируется при запуске сниффера или устанавливается вручную соответствующими настройками сниффера.

Весь перехваченный трафик передается декодеру пакетов, который идентифицирует и расщепляет пакеты по соответствующим уровням иерархии. В зависимости от возможностей конкретного сниффера представленная информация о пакетах может впоследствии дополнительно анализироваться и отфильтровываться.

Ограничения использования снифферов

Наибольшую опасность снифферы представляли в те времена, когда информация передавалась по сети в открытом виде (без шифрования), а локальные сети строились на основе концентраторов (хабов). Однако эти времена безвозвратно ушли, и в настоящее время использование снифферов для получения доступа к конфиденциальной информации — задача отнюдь не из простых.

Дело в том, что при построении локальных сетей на основе концентраторов существует некая общая среда передачи данных (сетевой кабель) и все узлы сети обмениваются пакетами, конкурируя за доступ к этой среде (рис. 2), причем пакет, посылаемый одним узлом сети, передается на все порты концентратора и этот пакет прослушивают все

остальные узлы сети, но принимает его только тот узел, которому он адресован. При этом если на одном из узлов сети установлен пакетный сниффер, то он может перехватывать все сетевые пакеты, относящиеся к данному сегменту сети (сети, образованной концентратором).

Рис. 1. Схема работы сниффера

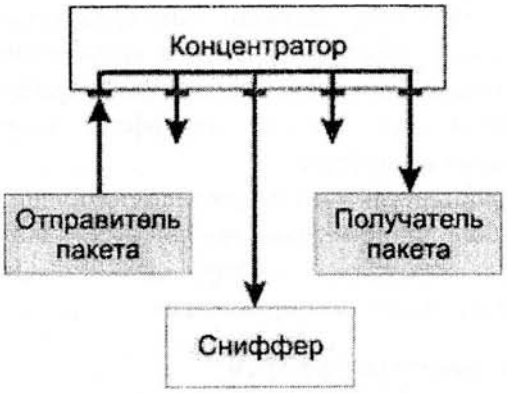

Рис. 2.

При использовании концентраторов сниффер способен перехватывать все пакеты сетевого сегмента.

Коммутаторы являются более интеллектуальными устройствами, чем широковещательные концентраторы, и изолируют сетевой трафик. Коммутатор знает адреса устройств, подключенных к каждому порту, и передает пакеты только между нужными портами. Это позволяет разгрузить другие порты, не передавая на них каждый пакет, как это делает концентратор. Таким образом, посланный неким узлом сети пакет передается только

на тот порт коммутатора, к которому подключен получатель пакета, а все остальные узлы сети не имеют возможности обнаружить данный пакет (рис. 3).

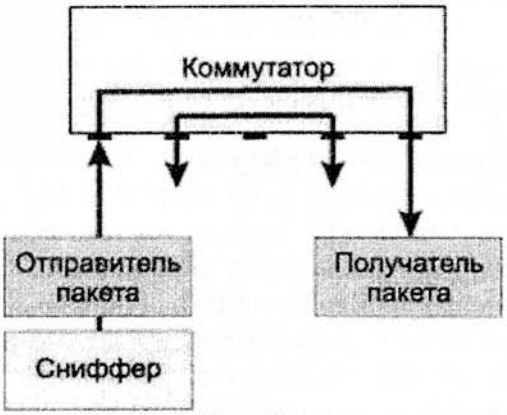

Рис. 3.

При использовании коммутаторов сниффер способен перехватывать только входящие и исходящие пакеты одного узла сети. Поэтому если сеть построена на основе коммутатора, то сниффер, установленный на одном из компьютеров сети, способен перехватывать только те пакеты, которыми обменивается данный компьютер с другими узлами сети. В результате, чтобы иметь возможность перехватывать пакеты, которыми интересующий злоумышленника компьютер или сервер обменивается с остальными узлами сети, необходимо установить сниффер именно на этом компьютере (сервере), что на самом деле не так-то просто. Правда, следует иметь в виду, что некоторые пакетные снифферы запускаются из командной строки и могут не иметь графического интерфейса. Такие снифферы, в принципе, можно устанавливать и запускать удаленно и незаметно для пользователя.

Кроме того, необходимо также иметь в виду, что, хотя коммутаторы изолируют сетевой трафик, все управляемые коммутаторы имеют функцию перенаправления или зеркалирования портов. То есть порт коммутатора можно настроить таким образом, чтобы на него дублировались все пакеты, приходящие на другие порты коммутатора. Если в этом случае к такому порту подключен компьютер с пакетным снифером, то он может перехватывать все пакеты, которыми обмениваются компьютеры в данном сетевом сегменте. Однако, как правило, возможность конфигурирования коммутатора доступна только сетевому администратору. Это, конечно, не означает, что он не может быть злоумышленником, но у сетевого администратора существует множество других способов контролировать всех пользователей локальной сети, и вряд ли он будет следить за вами столь изощренным способом.

Другая причина, по которой снифферы перестали быть настолько опасными, как раньше, заключается в том, что в настоящее время наиболее важные данные передаются в зашифрованном виде. Открытые, незашифрованные службы быстро исчезают из Интернета. К примеру, при посещении web-сайтов все чаще используется протокол SSL (Secure Sockets Layer); вместо открытого FTP используется SFTP (Secure FTP), а для других служб, которые не применяют шифрование по умолчанию, все чаще используются виртуальные частные сети (VPN).

Итак, те, кто беспокоится о возможности злонамеренного применения пакетных снифферов, должны иметь в виду следующее. Во-первых, чтобы представлять серьезную угрозу для вашей сети, снифферы должны находиться внутри самой сети. Во-вторых, сегодняшние стандарты шифрования чрезвычайно затрудняют процесс перехвата конфиденциальной информации. Поэтому в настоящее время пакетные снифферы постепенно утрачивают свою актуальность в качестве инструментов хакеров, но в то же время остаются действенным и мощным средством для диагностирования сетей. Более того, снифферы могут с успехом использоваться не только для диагностики и локализации

сетевых проблем, но и для аудита сетевой безопасности. В частности, применение пакетных анализаторов позволяет обнаружить несанкционированный трафик, обнаружить и идентифицировать несанкционированное программное обеспечение, идентифицировать неиспользуемые протоколы для удаления их из сети, осуществлять генерацию трафика для испытания на вторжение (penetration test) с целью проверки системы защиты, работать с системами обнаружения вторжений (Intrusion Detection System, IDS).

Обзор программных пакетных снифферов

Все программные снифферы можно условно разделить на две категории: снифферы, поддерживающие запуск из командной строки, и снифферы, имеющие графический интерфейс. При этом отметим, что существуют снифферы, которые объединяют в себе обе эти возможности. Кроме того, снифферы отличаются друг от друга протоколами, которые они поддерживают, глубиной анализа перехваченных пакетов, возможностями по настройке фильтров, а также возможностью совместимости с другими программами.

Обычно окно любого сниффера с графическим интерфейсом состоит их трех областей. В первой из них отображаются итоговые данные перехваченных пакетов. Обычно в этой области отображается минимум полей, а именно: время перехвата пакета; IP-адреса отправителя и получателя пакета; MAC-адреса отправителя и получателя пакета, исходные и целевые адреса портов; тип протокола (сетевой, транспортный или прикладного уровня); некоторая суммарная информация о перехваченных данных. Во второй области выводится статистическая информация об отдельном выбранном пакете, и, наконец, в третьей области пакет представлен в шестнадцатеричном виде или в символьной форме — ASCII.

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. Этот тип информации обычно отображается во второй области окна сниффера. К примеру, любой сниффер способен распознавать протокол TCP, а продвинутые снифферы умеют определять, каким приложением порожден данный трафик. Большинство анализаторов протоколов распознают свыше 500 различных протоколов и умеют описывать и декодировать их по именам. Чем больше информации в состоянии декодировать и представить на экране сниффер, тем меньше придется декодировать вручную.

Одна из проблем, с которой могут сталкиваться анализаторы пакетов, — невозможность корректной идентификации протокола, использующего порт, отличный от порта по умолчанию. К примеру, с целью повышения безопасности некоторые известные приложения могут настраиваться на применение портов, отличных от портов по умолчанию. Так, вместо традиционного порта 80, зарезервированного для web-сервера, данный сервер можно принудительно перенастроить на порт 8088 или на любой другой. Некоторые анализаторы пакетов в подобной ситуации не способны корректно определить протокол и отображают лишь информацию о протоколе нижнего уровня (TCP или UDP).

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.

Поступила 29.03.2007 г.