Sniffers

Снифферы (sniffers) — это программы, способные перехватывать и анализировать. Снифферы полезны в тех случаях, когда нужно извлечь из потока данных какие-либо сведения (например, пароли). Программу можно установить на одном устройстве, к которому есть доступ, и в течение короткого времени получить все передаваемые данные.
Снифферы позволяют **перехватывать и анализировать сетевой трафик** (посещенные сайты, сообщения, в т. ч. - голосовые, файлы и другую информацию и данные). Анализатор захватывает все потоки (перехватывает и протоколирует интернет трафик) и, при необходимости, производит декодирование данных, последовательно сохраняя передаваемую информацию пользователей. Снифферы дают возможность модернизировать все запросы, которые через них проходят. Они полезны, когда из потока нужно извлечь какие-либо сведения, создать нужный ответ сервера, провести диагностику сети или уменьшать пропускную нагрузку. Самые популярные снифферы — Fiddler и Charles.

Принцип работы снифферов

Перехватить трафик через сниффер можно следующими способами: путем прослушивания в обычном режиме сетевого интерфейса, подключением в разрыв канала, перенаправлением трафика, посредством анализа побочных электромагнитных излучений, при помощи атаки на уровень канала и сети, приводящей к изменению сетевых маршрутов. Поток данных, перехваченный сниффером, подвергается анализу, что позволяет: выявить паразитный трафик (его присутствие значительно увеличивает нагрузку на сетевое оборудование), обнаружить активность вредоносных и нежелательных программ (сканеры сети, троянцы, флудеры, пиринговые клиенты и т.п.), произвести перехват любого зашифрованного или незашифрованного трафика пользователя для извлечения паролей и других ценных данных.
Некоторые снифферы могут генерировать трафик и действовать в качестве исходного устройства. Например, применятся в качестве тестеров протоколов. Такие системы тест-снифферов позволяют генерировать правильный трафик необходимый для функционального тестирования. Помимо этого, снифферы могут целенаправленно вводить ошибки для проверки способностей тестируемого устройства.

Классификация снифферов

Снифферы различаются следующими функциональными особенностями: Поддержка протоколов канального уровня, а также физических интерфейсов. Качество декодирования протоколов. Пользовательский интерфейс. Доступ к статистике, просмотру трафика в реальном времени и т.д.

Анализаторы различаются по:

- *способности отображения данных* (создание временных диаграмм, реконструирование UDP, TCP протоколов данных и пр.);
- *типу применения* (для обнаружения ошибок, первопричин либо для слежения онлайн за пользователями).

Аппаратные снифферы. Анализаторы трафика могут быть и аппаратного типа, в виде зонда или дискового массива (более распространенный тип). Данные устройства осуществляют запись информационных пакетов или их частей на дисковый массив. Это позволяет воссоздать любую информацию полученную или переданную пользователем в просторы интернета либо своевременно выявить неисправность интернет-трафика.

Методы применения.

Анализаторы сетевых пакетов применяются для:

- анализа имеющихся проблем в сети;
- обнаружения сетевых попыток вторжения;
- определения злоупотребления трафика пользователями (внутри системы так и снаружи нее);
- документирования нормативных требований (возможного периметра входа в систему, конечных точек распространения трафика);
- получения информации о возможностях сетевого вторжения;
- изолирования эксплуатируемых систем;
- мониторинга загрузки каналов глобальной сети;
- использования для отслеживания состояния сети (в том числе деятельность пользователей как в системе, так и за ее пределами);
- мониторинга перемещаемых данных;
- отслеживания WAN и безопасности конечных точек состояния;
- сбора сетевой статистики;
- фильтрации подозрительного контента, идущего от сетевого трафика;
- создания первичного источника данных для отслеживания состояния и управления сети;
- слежения онлайн в качестве шпиона, собирающего конфиденциальную информацию пользователей;
- отладки серверной, клиентской связи;
- проверки эффективности внутреннего контроля (контроля доступа, брандмауэров, фильтров спама и пр.).

Есть четыре сферы, в которых люди используют сниффер в благих намерениях:

- Сетевые инженеры: чтобы оптимизировать сеть, они должны следить за трафиком.

- Системные администраторы: им необходимо наблюдать за трафиком, чтобы собирать данные о показателях, вроде пропускной способности сети.

- Специалисты по кибербезопасности: они могут заметить подозрительную активность в Сети, отслеживая ее. Аномальные всплески или различные типы трафика могут указывать на наличие вредоносного программного обеспечения или проникновения хакеров в систему.

- Корпорации. Работодатели могут использовать программное обеспечение для отслеживания своих сотрудников и выяснять, сколько времени в течение рабочего дня они тратят на работу и сколько — на развлечения.

В целях обслуживания сети сниффер обеспечивает:
- захват пакетов данных;
- запись и анализ трафика;
- расшифровку пакета;
- устранение неполадок сети;
- тестирование межсетевого экрана;
- обеспечение бесперебойного потока трафика.

Снифферы часто используются и для мониторинга компьютерных сетей. Выполняя постоянное, непрерывное наблюдение, анализаторы сетевых пакетов выявляют

медленные, неисправные системы и передают (на почту, телефон или сервер) полученную информацию о сбоях администратору.

На беспроводных сетях, даже когда адаптер находится в «неразборчивом» режиме, пакеты данных, перенаправляющиеся не с настроенной (основной) системы, будут автоматически проигнорированы. Чтобы отслеживать данные информационные пакеты, адаптер должен находится в ином режиме – мониторинга.

Нередко анализаторы трафика применяются в «мирных» целях — для диагностики сети, выявления и устранения неполадок, обнаружения вредоносного ПО или чтобы выяснить, чем заняты пользователи и какие сайты они посещают. Но именно при исследовании безопасности сетевого периметра или тестировании на проникновение сниффер — незаменимый инструмент для разведки и сбора данных. Существуют снифферы для различных операционных систем, кроме того, подобное ПО можно установить на роутере и исследовать весь проходящий через него трафик.

Традиционно идея сниффинга жила в двух ипостасях: легальное и нелегальное применение. Что характерно, слово "сниффер" чаще применяется в нелегальной сфере, а "сетевой анализатор" - в легальной. Начнем, с легального применения:

- troubleshooting (обнаружение проблем и узких мест сети). В расширенном режиме, когда сниффер работает в некоммутируемом сегменте или на шлюзе, мы можем получить практически полную картину событий, происходящих в нашей сети: интенсивность трафика по времени, по рабочим станциям, по протоколам, количество ошибок разных типов. Кроме того, в обоих режимах, мы можем "разгребать" более специфические проблемы, когда, скажем, у конкретной станции ни в какую не получается организовать некое взаимодействие по сети, и это при том, что внешне сеть выглядит вполне работоспособной. Особенно полезен сниффер в случаях, когда сетевое ПО плохо документировано или использует свои закрытые (недокументированные), зачастую подозрительные технологии (протоколы). Например: ICQ, Europe Online. Под подозрительными технологиями/ПО следует понимать ситуации, когда вы предполагаете наличие в программе закладки или иной недокументированной функциональности.

Не менее полезен сниффер для отладки вашего собственного ПО. Пример: прокси-сервер не желал устанавливать соединение, если GET-запрос оканчивался на \n\n вместо требуемого \r\n\r\n. Только исследование пакетов, отправляемых "законопослушным" браузером и сравнение их с пакетами, отправляемыми моим "выскочкой"-скриптом, указало мне на досадную ошибку. Очень и очень часто в повседневной админской практике мне приходится сталкиваться и с анализом на уровне TCP/UDP.

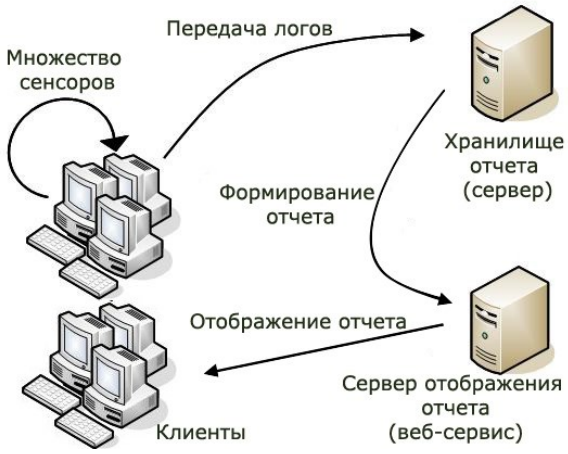
- обучение. Можно довестись до полуобморочного состояния, зазубривая форматы заголовков пакетов различных протоколов и методы взаимодействия (скажем, 3-way TCP handshake, DNS, прикладные методы плана traceroute), но эти знания будут мертвыми, пока вы не попытаетесь "потрогать это руками" - написав однажды программу либо... заглянув в сниффер! Попробуйте после прочтения документации на неизвестный или плохо понятный вам протокол, смоделировать взаимодействие, перехватить пакеты и проанализировать их - уверяю вас, все станет чрезвычайно понятно и более того, это знание более реально и надолго отложится в голове. В случае же с закрытыми технологиями, сниффер может оказаться чуть ли не единственным средством для их изучения.

- протоколирование сетевого трафика. Можно много дискутировать на тему правомерности и этичности протоколирования администратором трафика пользователей для дальнейшего просмотра, но факт остается фактом - многие организации включают в политику безопасности эту технологию. Мое личное мнение - хозяин барин, то бишь если компания обеспечивает своих сотрудников оборудованием, подключением к локальным и глобальным сетям, она вправе требовать надлежащего использования этих ресурсов. Вторая важная причина для протоколирования трафика - обнаружение попыток несанкционированного доступа и других

зловредностей - DoS-атак например. Имея такие логи администратор с 100-процентной точностью может знать, что происходит в его сетевых владениях.

Использование снифферов в тестировании

Анализ трафика — важнейший этап тестирования на проникновение (или даже взлома). В передаваемых по сети пакетах можно обнаружить много интересного, например пароли для доступа к разным ресурсам и другие ценные данные. Так можно проводить модульное тестирование продукта, в котором есть и бэк, и фронт, и разные команды со своей версионностью. С его помощью можно не только проверять различные коды ответов и реакцию приложения на них, но и проверять http-запросы, подменять HTTP пакеты и POST данные. Можно изменять Coockie и создавать имитацию нужных ответов сервера. Ответы возможно автоматизировать, используя функцию breakpoints.
Это работает следующим образом: браузер отправляет запрос, сниффер его «проксирует» и отправляет от своего лица пользователю. Далее приходит ответ от сервера – он тоже поступает сначала в сниффер, а затем – к нам.



Особенности применения снифферов

Перехватывать потоки данных можно легально и нелегально. Понятие «сниффер» применяется именно по **отношению к нелегальному сценарию,** а легальные продукты такого рода называют «анализатор трафика». Решения, применяемые в рамках правового поля, полезны для того, чтобы получать полную информацию о состоянии сети и понимать, чем заняты сотрудники на рабочих местах. Помощь таких программ оказывается ценной, когда необходимо «прослушать» порты приложений, через которые могут отсылаться конфиденциальные данные. Программистам они помогают проводить отладку, проверять сценарии сетевого взаимодействия. Используя анализаторы трафика, можно своевременно обнаружить несанкционированный доступ к данным или проведение DoS-атаки. Нелегальный перехват подразумевает шпионаж за пользователями сети: злоумышленник сможет получить информацию о том, какие сайты посещает пользователь, и о том, какие данные он пересылает, а также узнать о применяемых для общения программах. Впрочем, основная цель незаконного «прослушивания» трафика — получение логинов и паролей, передаваемых в незашифрованном виде.
Хакеры используют снифферы для кражи ценных данных с помощью отслеживания сетевой активности и сбора персональной информации о пользователях. Чаще всего злоумышленники заинтересованы в паролях и учетных данных пользователей. Имея эти данные, можно получить доступ к онлайн-банкингу и учетным записям онлайн-магазинов.

Чаще всего хакеры устанавливают снифферы в местах распространения незащищенного подключения Wi-Fi, например, в кафе, отелях и аэропортах. Снифферы могут

маскироваться под подключенное к Сети устройство.

Источник угрозы Снифферы могут работать на маршрутизаторе (router), когда анализируется весь трафик, проходящий через устройство, или на оконечном узле. Во втором случае злоумышленник эксплуатирует следующее обстоятельство: все данные, передаваемые по сети, доступны для всех подключенных к ней устройств, но в стандартном режиме работы сетевые карты не замечают «чужую» информацию. Если перевести сетевую карту в режим promiscuous mode, то появится возможность получать все данные из сети. И, конечно, снифферы позволяют переключаться в этот режим.

Незаконное использование снифферов

Сниффер может быть использован злоумышленниками для кражи данных. Снифферы анализируют все, что через них проходит, включая незашифрованные пароли и учетные данные. Поэтому хакеры, имеющие к ним доступ, могут завладеть личной информацией пользователей, такой как: имена пользователей, пароли, номера кредитных карт и т.д; запись сообщений, вроде электронных писем; подделки личных данных; кражи денег.

Перехватить трафик через сниффер можно следующими способами:

путем прослушивания в обычном режиме сетевого интерфейса;
подключением в разрыв канала и перенаправлением трафика;
с помощью анализа побочных электромагнитных излучений;
при помощи атаки на уровень канала и сети, приводящей к изменению сетевых маршрутов.

Последовательность перехвата информационных пакетов.

Перехват заголовков или всего содержимого. Снифферы могут перехватывать или все содержимое пакетов данных, или всего лишь их заголовки. Второй вариант позволяет уменьшить общие требования к хранению информации, а также избежать юридических проблем, связанных с несанкционированным изъятием личной информации пользователей. При этом, история передаваемых заголовков пакетов может иметь достаточный объем информации, для выявления необходимой информации или диагностики неисправностей.

Декодирование пакетов. Перехваченная информация декодируется из цифрового (нечитабельного вида) в удобный для восприятия, чтения тип. Система снифферов позволяет администраторам анализатора протоколов легко просматривать информацию, которая пересылалась или получалась пользователем.

Анализ рисков

Любая организация и любой пользователь могут оказаться под угрозой сниффинга — при условии, что у них есть данные, которые интересны злоумышленнику. При этом существует несколько вариантов того, как обезопасить себя от утечек информации. Во-первых, нужно использовать шифрование. Во-вторых, можно применить антиснифферы — программные или аппаратные средства, позволяющие выявлять перехват трафика. Следует помнить, что шифрование само по себе не может скрыть факт передачи данных, поэтому можно использовать криптозащиту совместно с антисниффером.

Как предотвратить утечку данных с помощью сниффера?

Если сниффер установлен на устройстве, то он уже имеет доступ к его данным. Чтобы предотвратить их утечку, Дмитрий Галов из «Лаборатории Касперского» рекомендует:

- Установить защитные решения, которые будут различными способами находить подозрительную активность.
- Использовать VPN от проверенного провайдера. С ним трафик будет передаваться в зашифрованном виде.
- Пользоваться только сайтами с протоколами https. Только на них можно вводить свои данные, в этом случае они шифруются.

Что делать, если сниффер уже установлен на компьютер

Чтобы обнаружить сниффер на компьютере, можно установить свой собственный сниффер и изучить весь трафик на уровне DNS в вашей сети, чтобы обнаружить любую подозрительную активность.

Удалить сниффер лучше всего с помощью антивируса. Если у вас нет платной подписки, можно установить пробную версию. Она проанализируют файлы на вашем компьютере, удалив из них подозрительные.