Снифферы или Анализаторы сетевых пакетов

Снифферы или Анализаторы сетевых пакетов

Снифферы — это программы, способные **перехватывать**, **интерпретировать** и **сохранять** для последующего анализа пакеты, передаваемые по сети.

Анализаторы сетевых пакетов, или **снифферы**, первоначально были разработаны как средство решения сетевых проблем, позволяющие системным администраторам и инженерам службы технической поддержки **наблюдать** за тем, как данные передаются по сети, диагностировать и устранять возникающие проблемы.

Снифферы или Анализаторы сетевых пакетов

С течением времени снифферы стали применяться абсолютно **для других целей**.

В руках **злоумышленника** сниффер представляет собой довольно опасное средство и может использоваться для завладения паролями и другой конфиденциальной информацией.

Принципы работы пакетных снифферов

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.

Снифферы обходят механизмы фильтрации (адреса, порты и т. д.), которые драйверы Ethernet и стек TCP/IP используют для интерпретации данных.

Пакетные снифферы захватывают из кабеля все данные, которые по нему передаются.

Принципы работы пакетных снифферов

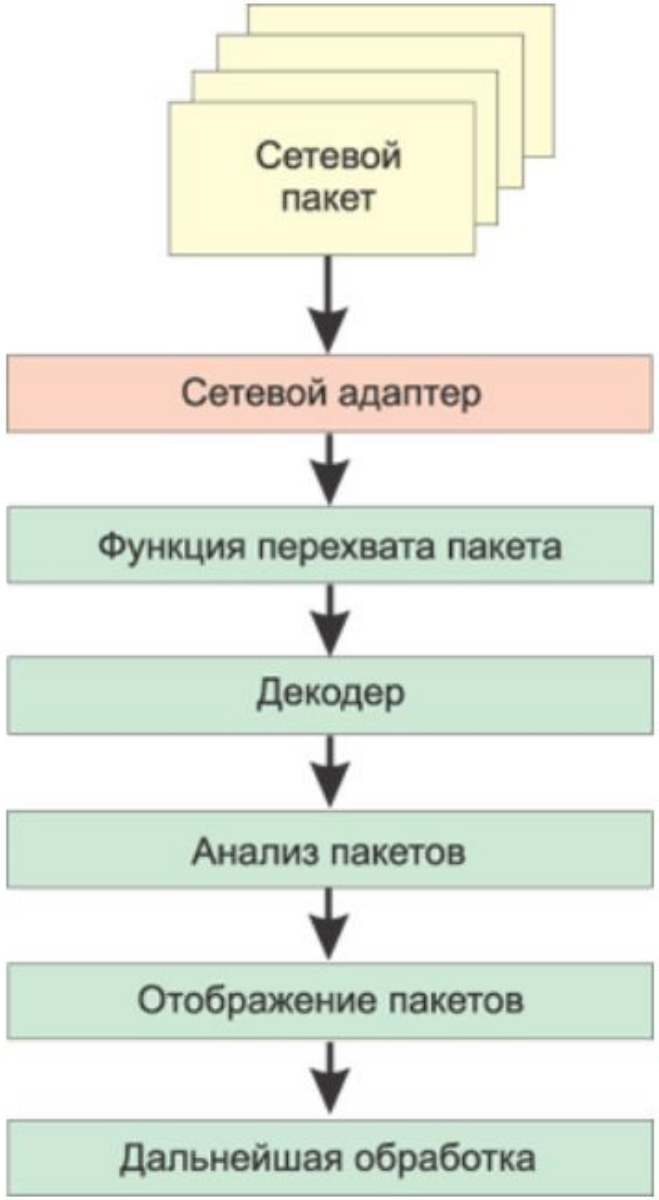
Для того чтобы сниффер мог перехватывать все пакеты, проходящие через сетевой адаптер, драйвер сетевого адаптера должен поддерживать режим функционирования promiscuous mode (**беспорядочный режим**), в котором сетевая плата позволяет принимать все пакеты независимо от того, кому они адресованы.

Данный режим работы сетевого адаптера **автоматически** активизируется при запуске сниффера или устанавливается вручную соответствующими настройками сниффера.

Принципы работы пакетных снифферов

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.


Сетевой пакет
Сетевой адаптер
Функция перехвата пакета
Декодер
Анализ пакетов
Отображение пакетов
Дальнейшая обработка

Ограничения использования снифферов

Ограничения использования снифферов

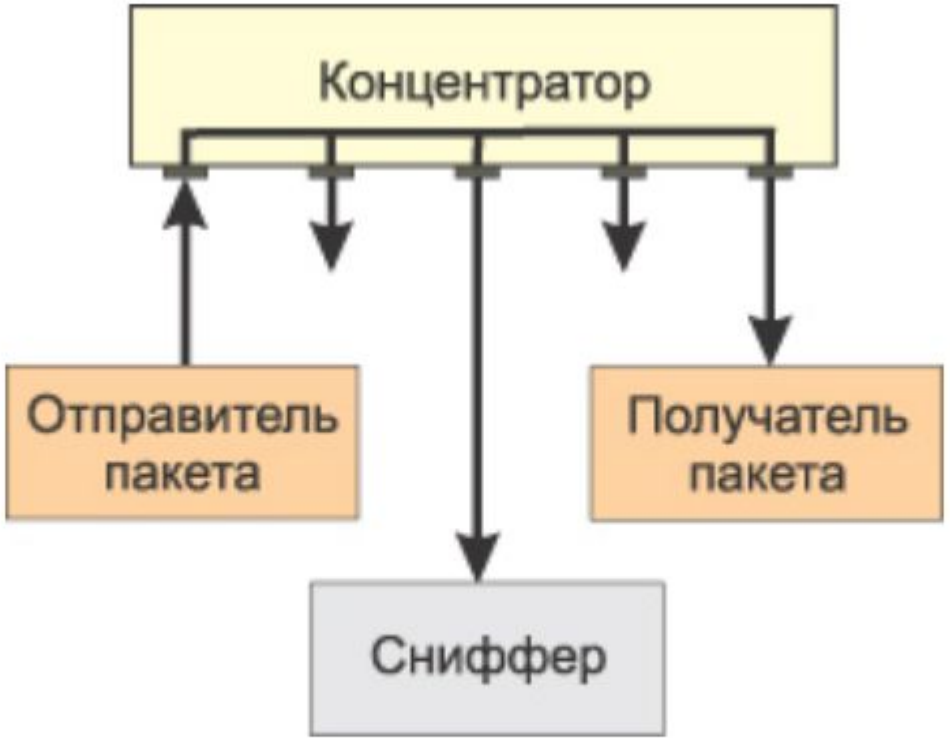


Рис. 2. При использовании концентраторов сниффер способен перехватывать все пакеты сетевого сегмента

Ограничения использования снифферов

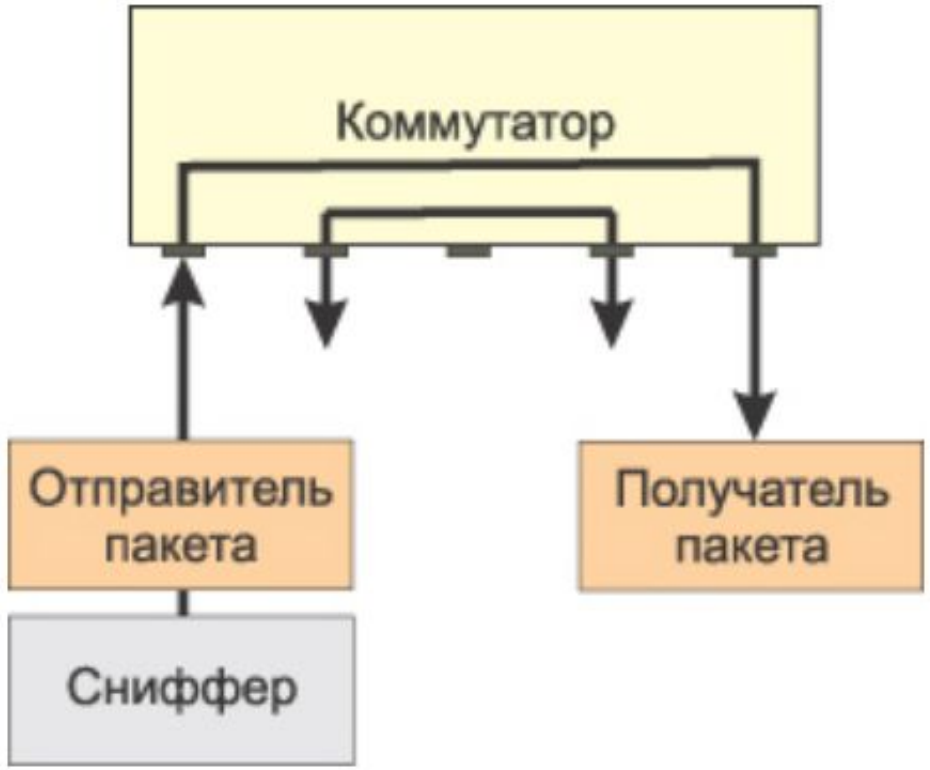


Рис. 3. При использовании коммутаторов сниффер способен перехватывать только входящие и исходящие пакеты одного узла сети

Ограничения использования снифферов

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).

Ограничения использования снифферов

Поэтому в настоящее время пакетные снифферы постепенно **утрачивают** свою **актуальность** в качестве инструментов хакеров.

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.

Ограничения использования снифферов

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

Обзор программных пакетных снифферов

Все программные снифферы можно условно разделить на две категории:

- снифферы, поддерживающие запуск из командной строки,
- снифферы, имеющие графический интерфейс.

При этом отметим, что существуют снифферы, которые **объединяют** в себе **обе эти возможности**.

Обзор программных пакетных снифферов

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.

Обзор программных пакетных снифферов

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

Обзор программных пакетных снифферов

Во второй области выводится статистическая информация об отдельном выбранном пакете.

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.

Обзор программных пакетных снифферов

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 (пятиста) различных протоколов** и умеют описывать и декодировать их по именам.

Обзор программных пакетных снифферов

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.

Обзор программных пакетных снифферов

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.

Обзор программных пакетных снифферов

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.

Далее мы рассмотрим возможности нескольких доступных для скачивания снифферов, которые ориентированы на использование с платформами Windows.

Защита от DDOS-атак

Что такое DDOS-атаки?

Атака типа «отказ в обслуживании» (DoS) – это попытка причинить вред, сделав недоступной целевую систему, для обычных конечных пользователей. Обычно злоумышленники генерируют большое количество пакетов или запросов, которые перегружают работу целевой системы. Для осуществления атаки типа «распределенный отказ в обслуживании» (DDoS) злоумышленник использует множество взломанных или контролируемых источников.

Классификация DDoS-атак

Рассматривая методы предотвращения DDoS-атак, полезно разделить их на две группы:

Атаки уровня **инфраструктуры** - сетевом уровне (уровень 3) и транспортном уровне (уровень 4);

Атаки уровня **приложения** - уровне представления (уровень 6) и уровне приложений (уровень 7);

DDoS-атака на уровне инфраструктуры

Это наиболее распространенный тип DDoS-атак, который включает в себя такие векторы, как SYN-флуд, и другие атаки отражения, такие как UDP-флуд.

SYN-флуд заключается в отправке большого количества SYN-запросов (запросов на подключение по протоколу TCP) в короткий срок

UDP-флуд сетевая атака, использующая бессеансовый режим протокола UDP. Заключается в отправке множества UDP-пакетов на определённые или случайные номера портов удалённого хоста.

Подобные атаки обычно массовые и направлены на то, чтобы перегрузить пропускную способность сети либо серверы приложений.

Атаки уровня приложения

Эти атаки менее распространены, но в то же время являются более сложными. Как правило, они не столь массовые, как атаки уровня инфраструктуры, но нацелены на определенные дорогостоящие части приложения и приводят к тому, что оно становится недоступным для реальных пользователей. В качестве примера можно привести поток HTTP-запросов на страницу входа в систему, дорогой API поиска или даже потоки XML-RPC Wordpress (также известные как атаки Wordpress Pingback).

Методы защиты от DDoS-атак

Уменьшение зон, доступных для атаки

Одним из первых методов нейтрализации DDoS-атак является сведение к минимуму размера зоны, которую можно атаковать. Подобный прием ограничивает возможности для атаки и обеспечивает возможность создания централизованной защиты. Необходимо убедиться, что доступ к приложению или ресурсам не был открыт для портов, протоколов или приложений, взаимодействие с которыми не предусмотрено. Таким образом, сведение к минимуму количества возможных точек для атаки позволяет сосредоточить усилия на их нейтрализации.

Методы защиты от DDoS-атак

План масштабирования

Двумя основными элементами нейтрализации крупномасштабных DDoS-атак являются пропускная способность (или транзитный потенциал) и производительность сервера, достаточная для поглощения и нейтрализации атак.

Методы защиты от DDoS-атак

План масштабирования

Транзитный потенциал. При проектировании приложений необходимо убедиться, что поставщик услуг хостинга предоставляет избыточную пропускную способность подключения к Интернету, которая позволяет обрабатывать большие объемы трафика. Необходимо размещать их рядом не только с конечными пользователями, но и с крупными узлами межсетевого обмена трафиком, которые легко обеспечат вашим пользователям доступ к приложению даже при большом объеме трафика. Можно воспользоваться сетями распространения контента (CDN) и сервисами интеллектуального преобразования адресов DNS.

Методы защиты от DDoS-атак

План масштабирования

Производительность сервера. Большинство DDoS-атак являются объемными и потребляют много ресурсов, поэтому важно иметь возможность быстро увеличивать или уменьшать объем своих вычислительных ресурсов. Это можно обеспечить, используя избыточный объем вычислительных ресурсов или ресурсы со специальными возможностями, такими как более производительные сетевые интерфейсы или улучшенная сетевая конфигурация, что позволяет поддерживать обработку больших объемов трафика.

Методы защиты от DDoS-атак

Сведения о типичном и нетипичном трафике

Каждый раз, когда обнаруживается повышение объема трафика, попадающего на хост, в качестве ориентира можно брать максимально возможный объем трафика, который хост может обработать без ухудшения его доступности. Такая концепция называется ограничением скорости. Более продвинутые методы защиты соответственно обладают дополнительными возможностями и могут интеллектуально принимать только трафик, который разрешен, анализируя отдельные пакеты. Для использования подобных средств необходимо определить характеристики хорошего трафика, который обычно получает целевой объект, и иметь возможность сравнивать каждый пакет с этим эталоном.

Методы защиты от DDoS-атак

Развертывание брандмауэров для отражения сложных атак уровня приложений

Против атак, которые пытаются использовать уязвимость в приложении, например против попыток внедрения SQL-кода или подделки межсайтовых запросов, рекомендуется использовать Web Application Firewall (WAF). Кроме того, из-за уникальности этих атак вы должны быть способны самостоятельно нейтрализовать запрещенные запросы, которые могут иметь определенные характеристики, например могут определяться как отличные от хорошего трафика или исходить из подозрительных IP-адресов, из неожиданных географических регионов и т. д.