СӘТБАЕВ УНИВЕРСИТЕТІ SATBAYEV UNIVERSITY

Дисциплина «Этичный хакинг и противодействие взлому»

Лекция 5

Анализаторы трафика (снифферы)

Преподаватель: **Батыргалиев Асхат Болатканович, PhD, ассоц.проф. кафедры «Кибербезопасность, обработка и хранение информации»**

askhat.b.b@gmail.com

Содержание

1. Определение анализатора трафика
2. Принцип работы анализатора трафика
3. Классификация снифферов
4. Источник угрозы, анализ рисков
5. Ограничения использования снифферов
6. Методы перехвата сетевого трафика
7. Обзор программных пакетных снифферов
8. Виды снифферов

По завершению урока Вы будете знать:

1. Понятие анализатора трафика
2. Принцип работы анализатора трафика
3. Классификацию снифферов
4. Ограничения при использовании снифферов
5. Методы перехвата сетевого трафика
6. Общие сведения о программных снифферах

Анализатор трафика

Анализатор трафика или сниффер (to sniff – нюхать) – программа или устройство для перехвата и анализа сетевого трафика (своего и/или чужого).

Снифферы применяются как в деструктивных, так и в благих целях. Анализ прошедшего через сниффер трафика позволяет:

- обнаружить паразитный, вирусный и закольцованный трафик, наличие которого увеличивает загрузку сетевого оборудования и каналов связи (снифферы здесь малоэффективны, как правило, для этих целей используют сбор разнообразной статистики серверами и активным сетевым оборудованием и её последующий анализ);
- выявить в сети вредоносное и несанкционированное ПО, например, сетевые сканеры, флудеры, троянские программы, клиенты пиринговых сетей и другие (это обычно делают при помощи специализированных снифферов – мониторов сетевой активности);
- перехватить любой незашифрованный (иногда зашифрованный) трафик с целью получения паролей и другой информации;
- локализовать неисправность сети или ошибку конфигурации сетевых агентов (для этой цели снифферы часто применяются системными администраторами).

Поскольку в «классическом» сниффере анализ трафика происходит вручную, с применением лишь простейших средств автоматизации (анализ протоколов, восстановление TCP-потока), то он подходит для анализа лишь небольших его объёмов.

Принцип работы анализатора трафика

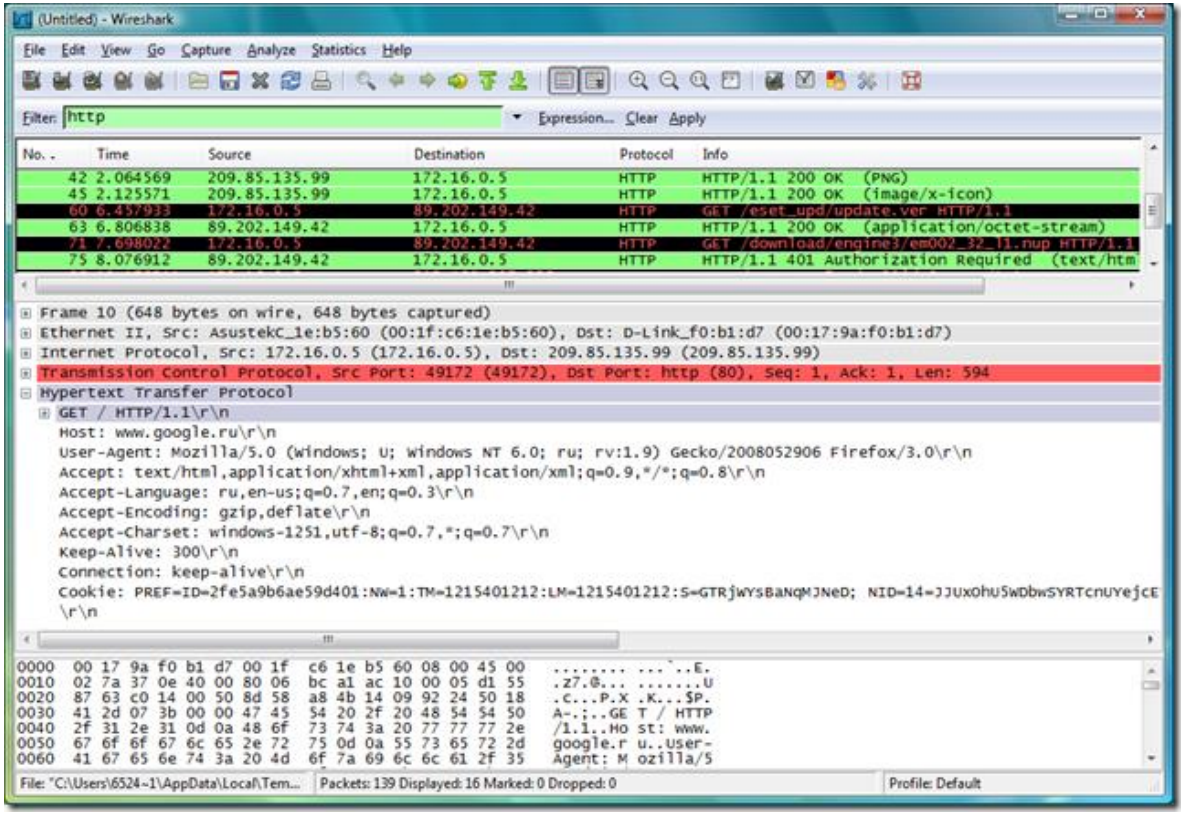
Сниффер может анализировать только то, что проходит через его сетевую карту. Внутри одного сегмента сети Ethernet все пакеты рассылаются всем машинам, из-за этого возможно перехватывать чужую информацию. Использование коммутаторов (switch, switch-hub) и их грамотная конфигурация уже является защитой от прослушивания. Между сегментами информация передаётся через коммутаторы. Коммутация пакетов – форма передачи, при которой данные, разбитые на отдельные пакеты, могут пересылаться из исходного пункта в пункт назначения разными маршрутами. Так что если кто-то в другом сегменте посылает внутри него какие-либо пакеты, то в ваш сегмент коммутатор эти данные не отправит.

Перехват трафика может осуществляться:

- обычным «прослушиванием» сетевого интерфейса (метод эффективен при использовании в сегменте концентраторов (хабов) вместо коммутаторов (свитчей), в противном случае метод малоэффективен, поскольку на сниффер попадают лишь отдельные фреймы);
- подключением сниффера в разрыв канала;
- ответвлением (программным или аппаратным) трафика и направлением его копии на сниффер (Network tap);
- через анализ побочных электромагнитных излучений и восстановление таким образом прослушиваемого трафика;
- через атаку на канальном (2) (MAC-spoofing) или сетевом (3) уровне (IP-spoofing), приводящую к перенаправлению трафика хоста или всего трафика сегмента на сниффер с последующим возвращением трафика в надлежащий адрес.

Принцип работы анализатора трафика

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.



Принцип работы анализатора трафика

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.

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.

Классификация 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. 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.

Источник угрозы, анализ рисков

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. Снифферы позволяют переключаться в этот режим.

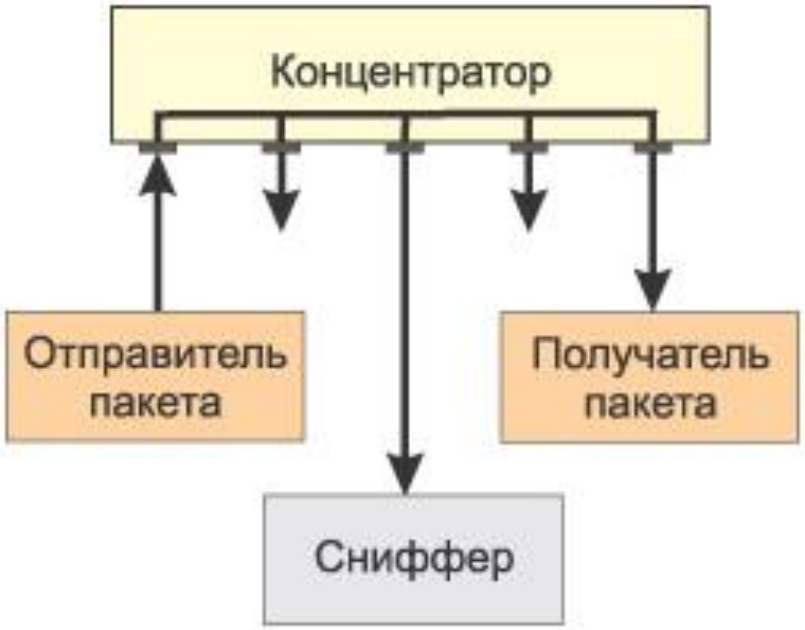
Анализ рисков

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.

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, в настоящее время подавляющая часть трафика передается в шифрованном виде.

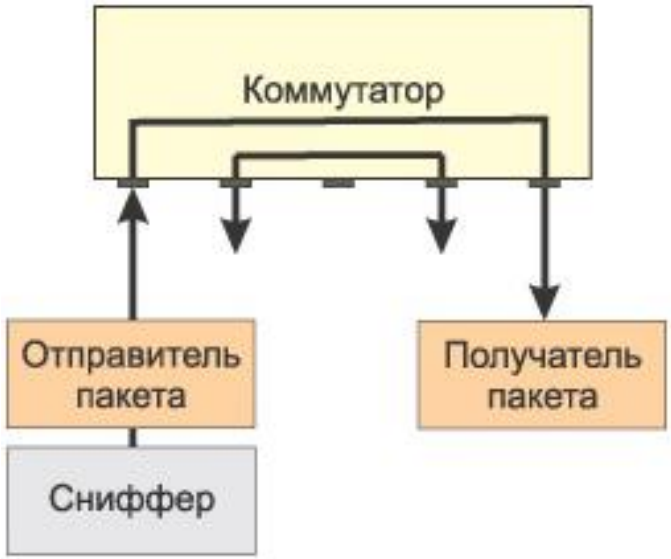
При построении локальных сетей на основе концентраторов существует некая общая среда передачи данных (сетевой кабель) и все узлы сети обмениваются пакетами, конкурируя за доступ к этой среде, причем пакет, посылаемый одним узлом сети, передается на все порты концентратора и этот пакет прослушивают все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



Ограничения использования снифферов

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.

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.



Ограничения использования снифферов

Необходимо отметить, 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 сниффером, 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).

Ограничения использования снифферов

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).

Методы перехвата сетевого трафика

Прослушивание сети с помощью программ сетевых анализаторов, является первым, самым простым способом перехвата данных.

Для защиты от прослушивания сети применяются специальные программы, например, AntiSniff, которые способны выявлять в сети компьютеры, занятые прослушиванием сетевого трафика. Программы-антисниферы для решения своих задач используют особый признак наличия в сети прослушивающих устройств - сетевая плата компьютера-снифера должна находиться в специальном режиме прослушивания. Находясь в режиме прослушивания, сетевые компьютеры особенным образом реагируют на IP-дейтаграммы, посылаемые в адрес тестируемого хоста. Например, прослушивающие хосты, как правило, обрабатывают весь поступающий трафик, не ограничиваясь только посланными на адрес хоста дейтаграммами. Имеются и другие признаки, указывающие на подозрительное поведение хоста, которые способна распознать программа AntiSniff.

Несомненно, прослушивание очень полезно с точки зрения злоумышленника, поскольку позволяет получить множество полезной информации - передаваемые по сети пароли, адреса компьютеров сети, конфиденциальные данные, письма и прочее. Однако простое прослушивание не позволяет хакеру вмешиваться в сетевое взаимодействие между двумя хостами с целью модификации и искажения данных. Для решения такой задачи требуется более сложная технология.

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.

Обзор программных пакетных снифферов

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).

Виды снифферов

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.

Известные снифферы:

- WinSniffer – обладает множеством разных настраиваемых режимов, способен перехватывать пароли различных сервисов;
- CommView – обрабатывает данные, передаваемые по локальной сети и в интернет, собирает сведения, связанные с модемом и сетевой картой, и подвергает их декодированию, что дает возможность видеть полный список соединений в сети и статистические сведения по IP. Перехваченная информация сохраняется в отдельный файл для последующего анализа, а удобная система фильтрации позволяет игнорировать ненужные пакеты и оставляет только те, которые нужны злоумышленнику;
- ZxSniffer – компактный сниффер;
- SpyNet – весьма популярный анализатор, в основную функциональность которого входят перехват трафика и декодирование пакетов данных;
- IRIS – имеет широкие возможности фильтрации, может перехватывать пакеты с заданными ограничениями.