Sniffers

Снифферы (sniffers) — это программы, способные перехватывать и анализировать сетевой трафик. Снифферы полезны в тех случаях, когда нужно извлечь из потока данных какие-либо сведения (например, пароли) или провести диагностику сети. Программу можно установить на одном устройстве, к которому есть доступ, и в течение короткого времени получить все передаваемые данные.

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.

Классификация снифферов (sniffers)

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

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.

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.

Для чего QA нужен sniffers

1. Достать токен авторизации с мобильного устройства
2. Получить тело ответа при оплате на мобильном устройстве
3. Выбрать запрос, поменять 1 символ в jwt токене и проверить, будет ли ошибка 401 (или вообще без него отправить запрос)
4. Выбрать запрос, поменять ему метод POST на PUT и проверить, будет ли ошибка 405.
5. REWRITE – автоматическая подмена запросов и ответовПолезно, когда нужно протестировать приложение на медленной скорости интернета (Например, 2G). Throttling позволяет также настроить стабильность интернета и даже Пинг! Ограничение можно включить для всего трафика, либо для конкретного хоста.
6. No-caching Инструмент No Caching предотвращает кэширование, манипулируя заголовками HTTP. Заголовки If-Modified-Since и If-None-Match удаляются из запросов, добавляются Pragma: no-cache и Cache-control: no-cache. Заголовки Expires, Last-Modified и ETag удаляются из ответов и добавляются Expires: 0 и Cache-Control: no-cache.Это полезно, если нужно изменить ответ сервера, а браузер берёт данные из кэша. Таким образом при каждом запросе будут использоваться данные от сервера.

7. Block cookies По аналогии с No caching эта функция удаляет заголовок Cookie из запросов. Также из ответа сервера она удаляет заголовок Set cookie. После включения этой опции сервер не сможет собирать Cookie с запросов. Также можно настраивать это для всех хостов или для какого-то конкретного.