УДК 004.7

Поротиков А.А.,
студент магистратуры
2 курс, факультет «Магистратуры»
Поволжский Государственный Университет Телекоммуникаций и Информатики
Россия, г. Самара
Научный руководитель: Стефанова Ирина Алексеевна

МОНИТОРИНГ ТРАФИКА ПРИ УДАЛЕННОЙ РАБОТЕ

Аннотация: *в статье рассматриваются понятие сниффиринга трафика. Рассмотрены различные программные. Кратко описаны особенности ПО и их сценарии использования в наши дни.*

Ключевые слова: *Сниффер, сеть, VPN, Интернет, безопасность, построение, соединение.*

Annotation: *The article deals with the concept of traffic sniffing. Various software programs are considered. Briefly describes the features of the software and their usage scenarios today.*

Key words: *Sniffer, network, VPN, Internet, security, building, connection.*

События последних трех лет за период пандемии изменили традиционные подходы офисной работы сотрудников, это привело к резкому росту перехода на удаленный формат трудового дня. У работы из дома из-за определенных обстоятельств есть ряд преимуществ, например, не нужно тратить время на дорогу. Однако приходится самостоятельно мотивировать себя заниматься делами и использовать время так же продуктивно, как в офисе. Для выполнения своих обязанностей, работникам требуется подключение к корпоративным ресурсам компании. На помощь создавшейся

ситуации могут прийти VPN сети. Создание комфортных условий работы в виде удаленного формата хорошо для сотрудников, но может доставить ряд проблем для компании работодателя. Сотрудники могут работать менее продуктивно, чем в офисе, в силу отсутствия какого-либо контроля, в связи с чем могут начать просматривать контент, который не относится к работе. Но главную проблему может вызвать утечка важных данных, либо наоборот, закачка вредоносных файлов в систему компании. Чтобы избежать таких проблем, появляется понятие анализа трафика, а именно – сниффера.

Анализатор трафика, или же **сниффер** является сетевым анализатором трафика, программой или программно-аппаратным устройством. Его предназначеннием является перехват и последующий анализ, либо только анализ сетевого трафика, предназначенного для других узлов.

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 и их грамотная конфигурация уже является защитой от прослушивания. Между сегментами информация передаётся через коммутаторы. Так что если кто-то в другом сегменте посылает внутри его 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;
- 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 жертвы или всего трафика сегмента на сниффер с последующим возвращением трафика в надлежащий адрес.

Снифферы применяются как в благих, так и в деструктивных 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 (а порой и зашифрованный) пользовательский трафик с целью получения паролей и другой информации.
- Локализовать неисправность сети или ошибку конфигурации сетевых агентов (для этой цели снифферы часто применяются системными администраторами)

Выделяют ряд популярных анализаторов трафика, а именно:

SolarWinds - это очень большой набор инструментов управления IT. Большинство сетевых устройств, чтобы убедиться, что пакет идет туда, куда нужно, используют метаданные каждого пакета. Содержимое пакета неизвестно сетевому устройству. Другое дело - глубокая инспекция пакетов; это означает, что проверяется фактическое содержимое пакета. Таким образом можно обнаружить критическую сетевую информацию, которую нельзя почерпнуть из метаданных. Инструменты, подобные тем, которые предоставляются SolarWinds, могут выдавать более значимые данные, чем просто поток трафика.

tcpdump. Это приложение с открытым исходным кодом, которое устанавливается практически во всех Unix-подобных операционных системах. Tcpdump - отличная утилита для сбора данных, которая имеет очень сложный язык фильтрации. Важно знать, как фильтровать данные при их сборе, чтобы в итоге получить нормальный набор данных для анализа. Захват всех данных с сетевого устройства даже в умеренно загруженной сети может породить слишком много данных, которые будет очень трудно проанализировать. В некоторых редких случаях достаточно будет выводить захваченные tcpdump данные прямо на экран, чтобы найти то, что вам нужно.

Windump. Большинство полезных утилит с открытым исходным кодом в конечном итоге клонируют в другие операционные системы. Когда это происходит, говорят, что приложение было перенесено. Windump - это порт tcpdump и ведет себя очень похожим образом. Самое существенное различие между Windump и tcpdump заключается в том, что Windump нуждается в библиотеке Winpcap, установленной до запуска Windump. Несмотря на то, что Windump и Winpcap предоставляются одним и тем же майнтайнером, их нужно скачивать отдельно.

Winpcap - это библиотека, которая должна быть предварительно установлена. Но Windump - это exe-файл, который не нуждается в установке, поэтому его можно просто запускать. Это нужно иметь в виду, если вы используете сеть Windows. Вам не обязательно устанавливать Windump на каждой машине, поскольку вы можете просто копировать его по мере необходимости, но вам понадобится Winpcap для поддержки Windup. Как и в случае с tcpdump, Windump может выводить сетевые данные на экран для анализа, фильтровать таким же образом, а также записывать данные в файл pcap для последующего анализа.

Wireshark является следующим самым известным инструментом в наборе системного администратора. Он позволяет не только захватывать данные, но также предоставляет некоторые расширенные инструменты

анализа. Кроме того, Wireshark является программой с открытым исходным кодом и перенесен практически на все существующие серверные операционные системы. Под названием Etheral, Wireshark теперь работает везде, в том числе в качестве автономного переносимого приложения. Если вы анализируете трафик на сервере с графическим интерфейсом, Wireshark может сделать все за вас. Он может собрать данные, а затем анализировать их все здесь же. Однако на серверах графический интерфейс встречается редко, поэтому вы можете собирать сетевые данные удаленно, а затем изучать полученный файл pcap в Wireshark на своем компьютере. При первом запуске Wireshark позволяет либо загрузить существующий файл pcap, либо запустить захват трафика. В последнем случае вы можете дополнительно задать фильтры для уменьшения количества собираемых данных. Если вы не укажете фильтр, Wireshark будет просто собирать все сетевые данные с выбранного интерфейса.

Использованные источники:

1. Russel, J. Анализатор трафика [Текст]: справочник / J. Russel. – М.: Bookvika, 2012. – 108 с.