Лекция 1. Анализ пакетов и основы организации сетей

1) Анализ пакетов и их анализаторы
2) Оценка анализатора пакетов
3) Принцип действия анализаторов пакетов
4) Классификация сетевого трафика

1) Анализ пакетов и их анализаторы

Анализ пакетов, иногда еще называемый анализом протоколов, описывает процесс перехвата и интерпретации действующих данных по мере их продвижения по сети, чтобы лучше понять, что же в ней происходит. Как правило, анализ пакетов проводится анализатором пакетов – инструментальным средством, применяемым для перехвата первичных данных, передаваемых по проводам сети.

Анализ пакетов может оказать помощь в следующем:

• Уяснить характеристики сети;
• Выяснить, кто находится в сети;
• Определить, кто или что "съедает" доступную пропускную способность сети;
• Выявить моменты, когда использование сети достигает своего пика;
• Выявить зловредную деятельность в сети;
• Обнаружить небезопасные и громоздкие приложения.

Для анализа пакетов имеются различные программы: как бесплатные, так и коммерческие. Каждая такая программа предназначена для определенных целей. К числу самых распространенных программ анализа пакетов относятся **tcpdwnp, OmniPeek** и **Wireshark**. Программы **OmniPeek** и **Wireshark** снабжены графическим пользовательским интерфейсом, тогда как **tcpdump** является утилитой командной строки.

2) Оценка анализатора пакетов

Выбирая анализатор пакетов, необходимо принять во внимание целый ряд факторов, включая следующие.

• ***Поддержка сетевых протоколов***. Все анализаторы пакетов способны интерпретировать различные протоколы, а большинство из них – наиболее распространенные сетевые протоколы (например, IPv4 и ICMP), транспортные протоколы (например, TCP и UDP) и даже протоколы уровня приложений (например, DNS и HTTP). Хотя они могуг и не поддерживать нетрадиционные и более сложные протоколы (например, IPv6, SMBv2 и SIP). Поэтому, выбирая анализатор пакетов, убедитесь, что в нем поддерживаются применяемые вами протоколы.

• ***Удобство использования***. Обращайте особое внимание на интерфейс анализатора пакетов, простоту его установки и общую последовательность операций. Выбранная вами программа должна соответствовать уровню вашей квалификации. Так, если у вас имеется весьма скромный опыт анализа пакетов, вам вряд ли стоит выбирать такие сложные анализаторы пакетов, действующие в режиме командной строки, как утилита tcpdurnp. А если вы имеете немалый опыт анализа пакетов, то вам подойдет и более развитая, хотя и сложная программа. По мере приобретения необходимого опыта вы можете даже найти полезным сочетать в отдельных случаях несколько программ анализа пакетов.

• ***Стоимость***. Самое замечательное, что многие анализаторы пакетов бесплатны и практически ничем не уступают их коммерческим аналогам. А самое главное отличие бесплатных анализаторов пакетов от коммерческих заключается в их механизмах отчетности. В состав коммерческих продуктов, как правило, входит специальный модуль формирования

отчетов, тогда как в бесплатных приложениях такие средства отсутствуют, и поэтому они обеспечивают лишь ограниченную отчетность.

• ***Поддержка программ***. Даже если вы овладели основами работы с программой анализа пакетов, вам иногда потребуется дополнительная поддержка для решения новых задач по мере их появления. Оценивая имеющуюся поддержку программ, обращайте внимание на документацию для разработчиков, публичные форумы и списки рассылки пользователей. И несмотря на возможную нехватку формализованной коммерческой поддержки бесплатных программ анализа пакетов вроде Wireshark, сообщество пользователей и участников их разработки нередко ведет активные дискуссионные клубы, вики-страницы и блоги, чтобы помочь извлечь наибольшую пользу из выбранного вами анализатора пакетов.

• ***Доступ к исходному коду***. Некоторые анализаторы пакетов относятся к программному обеспечению с открытым исходным кодом. Это дает возможность просматривать исходный код программы, а иногда и вносить в него необходимые коррективы. Если у вас особый или сложный случай для применения анализатора пакетов, то такая возможность окажется для вас весьма привлекательной. Исходный код большинства коммерческих анализаторов пакетов недоступен.

• ***Поддержка операционной системы***. К сожалению, не во всех анализаторах пакетов поддерживается каждая операционная система. Следовательно, вам потребуется инструментальное средство, работающее в большинстве операционных систем. Следует также иметь в виду, что пакеты иногда придется перехватывать на одной машине, а просматривать на другой. Отличия в операционных системах могут вынудить вас пользоваться разными приложениями на отдельных машинах.

3) Принцип действия анализаторов пакетов

В процессе анализа пакетов задействованы как программные, так и аппаратные средства. Этот процесс делится на следующие стадии:

1. Сбор данных. Прежде всего анализатор пакетов собирает первичные двоичные данные из сети. Как правило, это делается переключением избранного сетевого интерфейса в смешанный режим *(promiscuous mode).* В этом режиме сетевая плата может принимать весь трафик в сегменте сети, а не только адресуемый ей трафик.

2. Преобразование. Далее перехваченные двоичные данные преобразуются в удобочитаемую форму. На это способно большинство развитых анализаторов пакетов, работающих в режиме командной строки. На этой стадии сетевые данные могут автоматически интерпретироваться только на самом элементарном уровне, оставляя бальшую часть анализа конечному пользователю вручную.

3. Анализ. Анализатор пакетов проводит анализ перехваченных и преобразованных данных. В частности, он проверяет протокол перехваченных в сети данных, исходя из извлекаемой информации, и далее начинает анализ характерных особенностей этого протокола.

4) Классификация сетевого трафика

Сетевой трафик можно классифицировать по трем типам: **широковещательный, много-** и **одноадресатный**. Каждая из этих классификаций сетевого трафика имеет свои особенности, определяющие порядок обработки пакетов в сетевом оборудовании.

Широковещательным (broadcast) называется такой пакет, который посылается во все порты в сетевом сегменте независимо от того, где установлен данный порт: на концентраторе или коммутаторе. Имеются формы широковещательного трафика второго и третьего уровня. На втором уровне *MAC-адрес* **ff:ff:ff:ff:ff:ff** является зарезервированным широковещательным адресом, и любой трафик, направляемый по этому адресу, распространяется по всему сетевому

сегменту. Широковещательный адрес имеется и на третьем уровне, но он меняется в зависимости от используемого диапазона сетевых адресов.

Самый большой из всех IP-адресов, допустимых в диапазоне адресов IPсети, зарезервирован для применения в качестве широковещательного адреса. Так, если у компьютера имеется *адрес* **192.168.0.20** и *маска подсети* **255.255.255.0**, адрес ***192.168.0.255*** оказывается широковещательным.

Многоадресатной (multicast) называется одновременная передача пакета из одного источника во многие места назначения. Цель многоадресатной передачи - использовать как можно меньше пропускной способности сети. Оптимизация многоадресатного трафика состоит в том, чтобы поменьше тиражировать поток данных по пути его следования к месту назначения. Конкретная обработка многоадресатного трафика зависит от его реализации в отдельных сетевых протоколах.

Многоадресатный трафик реализуется в основном через схему адресации, добавляющую получателей пакетов к многоадресатной группе. Именно так и действует многоадресатная передача по межсетевому протоколу IP. Такая схема адресации гарантирует от передачи пакетов тем компьютерам, для которых они не предназначены. Если вы обнаружите IP-адрес в пределах от ***224.0.0.0*** до ***239.255.255.255***, то по нему, вероятнее всего, обрабатывается многоадресатный трафик, поскольку именно в этих пределах зарезервированы адреса для подобных целей.

Одноадресатный (unicast) пакет передается непосредственно от одного компьютера к другому. Конкретное функционирование одноадресатной передачи зависит от применяемого сетевого протокола. В качестве примера можно привести устройство, которому требуется связаться с веб-сервером. Это одноточечное соединение, а следовательно, процесс передачи данных, должен быть начат клиентским устройством, передающим пакет только веб-серверу.

Вопросы для самопроверки 1:

1) Сетевые протоколы;
2) Семиуровневая модель OSI;
3) Прохождение данных по модели OSI;
4) Инкапсуляция данных;
5) Сетевое оборудование;

Литература:

1. Сандерс, Крис. Анализ пакетов: практическое руководство по использованию Wireshark и tcpdump для решения реальных проблем в локальных сетях, 3-е изд.: Пер. с англ. - СПб.: ООО "Диалектика", 2019 - 448 с.: ил. - Парал. тит. англ.

2. Анализатор протоколов Wireshark/ П.Н. Толмачев, Н.А. Ермакова, П.В. Подворный, С.А. Сапсай: Учебно-методическое пособие для выполнения лабораторных работ. – М.: РУТ (МИИТ), 2016. – 38 с.

3. https://www.wireshark.org.