УДК 004.7.056.53

Асяев Г. Д., Никольская К. Ю.

АТАКИ НА КАНАЛЬНЫЙ УРОВЕНЬ

С развитием постиндустриального общества. Развиваются и информационные технологии, следовательно, учащаются атаки на эти технологии. Сетевая отрасль занимает лидирующую позицию по количеству атак. В модели OSI будем брать канальный уровень. Так как на этом уровне основной опасность является, что взломав сеть , тот кто атакует может пройти через средства защиты более высоких уровней.

Ключевые слова: *Канальный уровень, Модель OSI, виды атак, безопасность.*

Asyaev G. D., Nikolskaya K. U.

ATTACKS ON THE DATA LINK LAYER

With the development of post-industrial society. Developing information technologies and, consequently, more frequent attacks on these technologies. Network industry is a leader in the number of attacks. The OSI model will take the data link layer. Since at this level, the main risk is that the hacking network, the one who attacks can pass through the higher levels of protection.

Keywords: *Link Layer Model OSI, types of attacks, security.*

Модель OSI представляет собой семиуровневую систему. Это физический, канальный, сетевой, транспортный, сеансовый, представительный, прикладной уровень. Каждый уровень поддерживает интерфейсы с выше и нижележащими уровнями и использует протоколы. Протоколы - это стандарты, определяющие формы представления и способы пересылки сообщений, процедуры их интерпретации, правила совместной работы различного оборудования в сетях.

Рассмотрим основной принцип функционирования и функции канального уровня. Для этого перенесёмся на физический уровень. Там передаются только биты. И, к сожалению, не учитывается, что физическая среда для передачи может быть занята, из-за чего возникают ошибки. Именно для этого на канальном уровне осуществляется проверка доступности среды передачи. А также обнаружение и устранение ошибок. В глобальных же сетях, канальный уровень обеспечивает обмен сообщениями между соседними компьютерами. Так канальный уровень можно понимать как локальную сеть. Именно поэтому стоит обеспечить максимальную безопасность. В соответствии с Федеральным законом «О безопасности» [1] основными принципами обеспечения безопасности являются:

1. Соблюдение и защита прав и свобод человека и гражданина;
2. Законность;
3. Системность и комплексность;
4. Приоритет предупредительных мер в целях обеспечения безопасности;
5. Взаимодействие федеральных органов государственной власти.

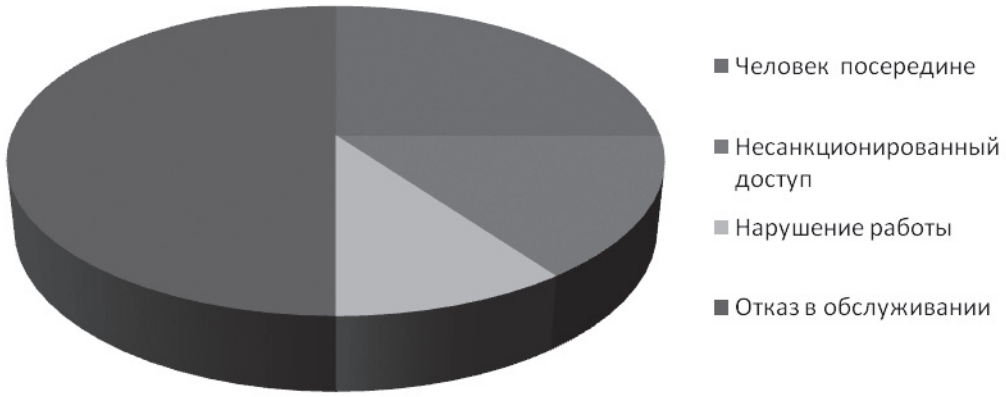

Рис. 1. Частота использования типов атак на канальном уровне.

Атаки на канальном уровне очень распространены. Как правило, предполагается, что тот кто атакует находит в локальной сети, либо есть какое-то связующее звено.

Атаки на канальный уровень подразделяются на такие типы как:

- Несанкционированный доступ к сети либо к её участкам;
- Отказ в обслуживании (DoS);
- «Человек посередине»(Man in the middle);
- Нарушение работы сети(Disruption of the network);
- Воздействия на тело кадра (внесение ошибок, подмена, потеря и имитация);
- Воздействия на оборудование звена передачи данных;
- Попытки несанкционированного доступа к средствам криптографической защиты информации канального уровня.

Рассмотрим поподробнее эти атаки.

Несанкционированный доступ к сети. Основной принцип заключается в том, чтобы найти и использовать недостатки протоколов. В том числе путём воздействия на тело кадра, а именно: внесение ошибок, подмена, потеря. Тем самым, всеми этими действиями получая доступ к участкам сети. [2]

Отказ в обслуживании. Один из самых распространённых типов атак. Основная суть состоит в том, что взять какой-либо ресурс системы и частыми запросами довести его до отказа. Кроме того на канальном уровне есть определённый тип атак, с помощью которых можно получить односторонний доступ. Одним из наиболее часто используемых способов нападения на канальный уровень является управление разнесенными антеннами. Допустим: есть точка доступа называемая AP с разнесенными антеннами A (для левой стороны) и B (соответственно для правой). Если пользователи I и II находятся на разных сторонах офиса, то каждый из них по умолчанию обращается к различным антеннам на точке доступа. Здесь возникает проблема: если пользователь I решит имитировать MAC адрес пользователя II. Увеличивая силу его сигнала, чтобы по крайней меру уровнять и при этом не превысить силу сигнала пользователя II на антенне B, точка доступа больше не будет принимать или посылать данные от пользователя II. Что свидетельствует об успешной атаке.

Другой проблемой на канальном уровне беспроводных сетей является spoofing точек доступа. Зададимся вопросом в контексте сетевой безопасности spoofing attack понимается как ситуация, в которой один человек или программа успешно маскируется под другую путем фальсификации данных и позволяет получить незаконные преимущества. Клиентская часть обычно конфигурируется таким образом, чтобы связываться с точкой доступа с наиболее сильным сигналом. Нападавший может просто подделывать название точки доступа и клиенты автоматически будут с ней связываться. Таким образом, злоумышленник может захватывать весь трафик.

Нарушение работы. Без сомнений, протокол содержит какие-либо ошибки или недостатки. Суть данной атаки это найти эти недостатки и нарушить их нормальную работу и ,как следствие, нарушить работу всей сети

Человек посередине. Суть: предполагает наличие человека, который прослушивает трафик или подменяет его. Перехват трафика, в свою очередь, может осуществляться:

1) обычным «прослушиванием» сетевого интерфейса.

2) подключением сниффера в разрыв канала. Под сниффером стоит понимать сетевой анализатор трафика, программа или программно-аппаратное устройство, предназначенное для перехвата и последующего анализа, либо только анализа сетевого трафика, предназначенного для других узлов.

3) ответвлением (программным или аппаратным) трафика и направлением его копии на сниффер.

Для того чтобы предотвратить атаку такого типа нужно провести шифрование данных на различных уровнях. В противном случае большие объемы передаваемой конфиденциальной информации будут попадать к злоумышленникам для дальнейшего использования (в том числе и в коммерческих целях).

Тем самым, канальный уровень выполняет функции логической организации передачи данных через физический уровень. Отсюда следует, что канальный уровень – достаточно уязвлённое место. А с ростом информатизации, количество атак становится всё больше и больше. Рассматривая уже существующие типы атак, следует особое внимание уделить такому типу как «Человек посередине», и Отказ в обслуживании.

Примечания

1. Федеральный закон о безопасности.
2. https://ru.wikipedia.org/wiki/%CA%E0%ED%E0%EB%FC%ED%FB%E9_%F3%F0%EE%E2%E5%ED%FC
3. http://www.on-lan.ru/ch9-5.html

Информация об авторах отсутствует на обоих языках