РАЗРАБОТКА ИНСТРУМЕНТАЛЬНОГО СРЕДСТВА ТЕСТИРОВАНИЯ СЕГМЕНТА КОРПОРАТИВНОЙ СЕТИ С ПАКЕТНОЙ КОММУТАЦИЕЙ

В. Н. Кулинченко
Кафедра автоматизированных систем обработки информации, Гомельский государственный университет имени Франциска Скорины
Гомель, Республика Беларусь
E-mail: kulinchenko@gsu.by

Анализаторы протоколов (трафика) применяются как для тестирования и диагностики сети, так и для деструктивных целей. Анализ прошедшего через анализатор трафика позволяет обнаружить паразитный, вирусный и закольцованный трафик, наличие которого увеличивает загрузку сетевого оборудования и каналов связи (анализаторы трафика 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, троянские программы, клиенты пиринговых сетей и другие (это обычно делают при помощи специализированных анализаторов трафика – 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 анализаторы трафика часто применяются системными администраторами).

Введение

В современном обществе наблюдается экспоненциальный рост «интеллектуальной» техники, в том числе на предприятиях и в организациях. Все большее количество фирм, заводов внедряют у себя всякого рода технологические новшества. Естественно все внедренные устройства объединяются в одну корпоративную сеть масштаба предприятия. Так как сеть постепенно «растет» в геометрических размерах и объемах, то при неправильном подходе в проектировании и увеличении сети появляются всякого рода неисправности и коллизии в сети.

Для обнаружения различного рода неисправностей недостаточно стандартных средств, поэтому используется специализированное программное обеспечение, которое позволяет выявлять неисправности в режиме реального времени. Так как большинство программ такого плана платные, то просто необходима разработка и внедрение собственного инструментария для диагностирования корпоративной сети.

I. Сетевой анализатор протоколов и его использование

Наиболее совершенным средством исследования и тестирования сети является анализатор протоколов. Процесс анализа протоколов включает захват циркулирующих в сети пакетов, реализующих тот или иной сетевой протокол, и изучение содержимого этих пакетов. Основываясь на результатах анализа, можно осуществлять обоснованное и взвешенное изменение каких-либо компонент сети, оптимизацию ее производительности, поиск и устранение неполадок.

Целью данной разработки является разработка инструментального средства тестирования корпоративной сети с пакетной коммутацией. Средства тестирования должны иметь простой функционал, а также должны быть снабжены визуальным интерфейсом для простоты использования. Полученное в результате программное обеспечение будет бесплатным и может распространяться по лицензии GNU GPLv3. Реализация данного проекта включает следующие пункты:

- сбор информации;
- обзор существующих инструментальных средств тестирования;
- разработка инструментального средства тестирования;
- написание программного обеспечения.

Полученное программное обеспечение должно выполнять следующие задачи

- предоставлять информацию пользователю;
- иметь возможность расширения функционала в зависимости от требований системного администратора.

II. Разработка сетевого анализатора протоколов

В руках сетевого администратора сетевой анализатор протоколов является весьма полезным инструментом, помогающим находить и устранять неисправности, избавляться от узких мест, снижающих пропускную способность сети, и обнаруживать проникновение в нее различный вредоносных программ[1].

Перехват трафика анализатором протоколов может осуществляться: – обычным «прослушиванием» сетевого интерфейса (метод эффективен при использовании в сегменте концентраторов (хабов) вместо коммутаторов (свитчей), в противном случае метод малоэффективен, по-

скольку на анализатор трафика попадают лишь отдельные фреймы); – подключением анализатора трафика в разрыв канала; – ответвлением (программным или аппаратным) трафика и направлением его копии на анализатор трафика; – через анализ побочных электромагнитных излучений и восстановление таким образом прослушиваемого трафика; – через атаку на канальном (MAC-spoofing) или сетевом уровне (IP-spoofing), приводящую к перенаправлению трафика жертвы или всего трафика сегмента на анализатор трафика с последующим возвращением трафика в надлежащий адрес.

Программное обеспечение анализатора состоит из ядра, поддерживающего работу сетевого адаптера и декодирующего получаемые данные, и дополнительного программного кода, зависящего от типа топологии исследуемой сети. Кроме того, поставляется ряд процедур декодирования, ориентированных на определенный протокол, например, IPX. В состав некоторых анализаторов может входить также экспертная система, которая может выдавать пользователю рекомендации о том, какие эксперименты следует проводить в данной ситуации, что могут означать те или иные результаты измерений, как устранить некоторые виды неисправности сети[2].

При разработке программы использовалась технология Winsocks версии 2 и среда разработки Embarcadero Rad Studio 2010. Программа разрабатывалась для операционных систем семейства Windows (начиная с Windows 2000/XP). Интерфейс в программе не перегружен лишними элементами, но как и в любом специализированном ПО есть все необходимое для работы. При желании ПО можно свободно изменять под свои нужды. На данном этапе программа позволяет проводить зондирование сети по трем основным протоколам TCP, IP, UDP и фиксировать полученные результаты в файл, а также выводить на экран. В полной версии программа будет включать в себя обработку большего количества протоколов. Во время работы анализатора трафика сетевой интерфейс переключается в так называемый «режим прослушивания» (promiscuous mode), что и позволяет ему получать пакеты, адресованные другим интерфейсам в сети[3].

III. Применение анализатора трафика для тестирования сегмента ЛВС

Поскольку в «классическом» анализаторе трафика анализ трафика происходит вручную, с применением лишь простейших средств автоматизации (анализ протоколов, восстановление TCP-потока), то он подходит для анализа лишь небольших его объёмов[4].

Тестирование сети с помощью созданного сетевого анализатора протоколов проводилось в сегменте кафедры автоматизированных систем обработки информации при проведении лабораторных работ по курсу «Диагностика и обслуживание сетей». Используемый кабель в сети типа UTP CAT5e, топология типа звезда-шина. На сервере установлена ОС Windows 2003 Server. Основной рабочий сетевой интерфейс – SiS 900 Based PCI Fast Ethernet Adapter. Данная корпоративная сеть является гетерогенной, на компьютерах пользователей используются операционные системы Windows XP и Windows 7.

Неисправность заключалась в том, что какой-то компьютер или роутер генерировал в локальную сеть паразитный трафик, тем самым снижая скорость обмена данными по сети. Сетевой анализатор был запущен на сервере и мог просматривать весь трафик на данном участке. Анализатор работал в течении 5 минут. Опытным путем был найден участок сети, в котором находился источник «шума». В течении этого времени особую активность проявлял компьютер с IP адресом 192.168.2.2.

После осмотра компьютера 192.168.2.2, было выявлено неразрешенное программное обеспечение, запущенное на данном компьютере, которое и генерировало этот цифровой мусор. Таким образом, сетевой анализатор успешно справился с поставленной задачей диагностирования сегмента корпоративной сети. Созданный анализатор протоколов хорошо подходит для диагностирования и контроля корпоративной и домашней сети. Он успешно справляется с поставленными задачами и не особо сложен в использовании.

1. Lai, K. Measuring Link Bandwidths Using a Deterministic Model of Packet Delay, Stanford University, – 2000.
2. Postel, J. (ed.), "Internet Control Message Protocol - DARPA Internet Program Protocol Specification,"RFC 792, USC/Information Sciences Institute, September 1981.
3. Dovrolis Constantinos, Ramanathan Paramenswaran, Moore David. What do packet dispersion techniques measure? In Proceedings of the 2001 Infocom, Anchorage AK, April 2001.
4. Фейт С. TCP/IP: Архитектура, протоколы, реализация (включая IP версии 6 и IP Security) - 2-е изд. McGraw-Hill Издательство "Лори 2000 , 450 стр.