Н.Н. Васин, А.А. Ирбахтин

МОДЕЛИРОВАНИЕ И МОНИТОРИНГ ТРАФИКА В ЗАЩИЩЕННЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

(Поволжский государственный университет телекоммуникаций и информатики)

Целью данной работы является разработка программно-аппаратного комплекса для обучения студентов навыкам конфигурирования защищенных соединений, моделирование и мониторинг трафика в защищенных сетях.

В настоящее время вопросы информационной безопасности при постоянно изменяющихся условиях среды эксплуатации сетевых устройств имеют большое значение. Сеть является первым барьером защиты. При построении сетей и их эксплуатации всегда необходим контроль уязвимостей в конфигурации устройств, а также уязвимостей программного обеспечения [1, 2]. Тестирование сети и выявление «брешей» дает возможность дальнейшего усиления защиты. Важным вопросом информационной безопасности является настройка защищенных каналов связи путем шифрования информационных и служебных передаваемых данных, а также проверки целостности принятых данных. Передача трафика в незашифрованном виде, приводит к утечке данных.

В настоящее время широко распространены средства для перехвата трафика, которые активно пользуются злоумышленниками. Современные средства позволяют не только перехватывать трафик, но даже расшифровывать его. Средства для перехвата берутся на вооружение и самими администраторами сетей, с целью тестирования сети на предмет возможности утечек данных.

Идеальным средством для физического перехвата трафика небольших сетей, а также отдельных участков крупных сетей является многопортовый повторитель или концентратор (hub), поскольку он передает принимаемые пакеты из всех портов. В современных телекоммуникационных сетях наличие концентратора в сети является угрозой безопасности. Используя одну витую пару Ethernet-кабеля только на приеме (для чтения), персональный компьютер (ПК) злоумышленника, проводящего мониторинг в таких сетях, может оказаться необнаруженным.

Известное программное средство Wireshark - широко распространенный инструмент для захвата и анализа трафика [3]. Wireshark имеет возможность детального рассмотрения структуры пакета, что делает его мощным средством для перехвата трафика. Может перехватывать информацию из HTTP и FTP запросов, а также из протоколов голосовой связи. Он также широко используется злоумышленниками.

В работе демонстрируется возможность перехвата трафика с использованием концентраторов в отсутствие шифрования и применения Wireshark для перехвата трафика сети. В качестве примера в работе рассматривается сеть передачи данных по протоколу FTP с шифрованием и без шифрования, на участках с открытым каналом передачи и по каналу с VPN. Для этого построена модель, показанная на рис.1, в среде эмулятора сетей GNS3, используемого в комплексе со средством виртуализации VirtualBox . В качестве маршрутизаторов R1 и R2 используются программные маршрутизаторы с ОС Vyatta 6.6, основанные на ОС Linux. В качестве серверов используется ОС Ubuntu Server 14.04 [4, 5]. Для мониторинга трафика использована ОС Kali Linux со встроенным анализатором трафика Wireshark. Концентраторы берутся из стандартных средств, входящих в программу GNS3. Таким образом, комплекс построен на базе свободно распространяемого ПО.

При настройке сети для маршрутизации использован протокол OSPF, между маршрутизаторами R1 и R2 создан туннель IPSec [6, 7]. На ОС Ubuntu Server установлена и настроена утилита vsFTPd, реализующая FTP сервер. На FTP сервере с шифрованием утилита vsFTPd установлена и настроена в комплексе с криптографическим пакетом для шифрования OpenSSL. Таким образом, сконфигурирован сервер с шифрованием FTP данных по протоколу SSL. Также для шифрования данных может быть использован и протокол TLS.

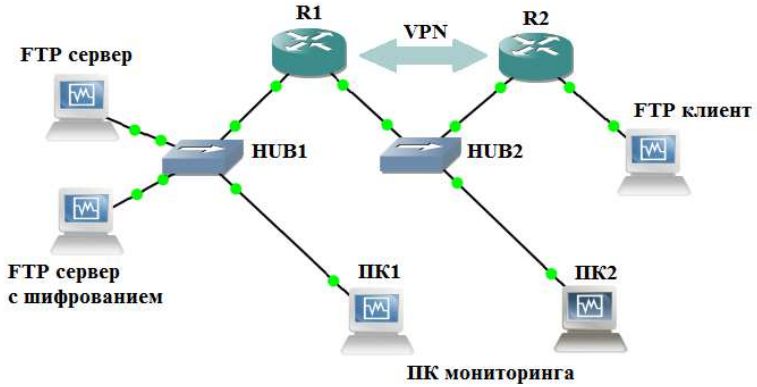

Рис.1. Структурная схема моделируемой сети.

Для анализа передаваемого по сети трафика выполнены следующие действия:

- Запущен Wireshark на ПК мониторинга.
- Сделан FTP запрос получения файла с ПК клиента на FTP сервер. На FTP сервер заранее помещены тестируемые файл, например изображения.
- Анализ трафика, перехваченного ПК2 между маршрутизаторами R1 и R2, свидетельствует о том, что данные FTP сессии недоступны для извлечения.
- ПК1 перехватывает FTP сессию и данные, передаваемые между клиентом и сервером. С помощью опций Analyze -> Follow TCP Stream Wireshark легко обнаруживает открытую FTP сессию. На рис. 2 изображен пример перехваченной FTP сессии. Перехвачены управляющие команды протокола FTP, имя пользователя (USER alex), пароль пользователя (PASS

1234), передаваемый файл (PETR image_for_test.png). Эти данные позволяют рассмотреть процесс инициализации сессии и передачу файла.

Рис.2. Перехваченная FTP сессия.

- Ниже пакета с запросом на передачу PETR, найден пакет FTP-DATA и с помощью опций Analyze -> Follow TCP Stream -> Save сохранен передаваемый файл (image_for_test.png).
- Передаваемый файл полностью соответствует файлу, заранее помещенному на FTP сервер.
- Проделаны аналогичные действия при запросе на FTP сервер с шифрованием.
- Перехваченные данные будут зашифрованы с помощью протокола SSL, что не исключит, но значительно затруднит их извлечение.

Выводы:

- Соединение между FTP клиентом и FTP сервером (без шифрования) не защищено полностью от перехвата во внутренних локальных сетях сервера и клиента соответственно;
- Соединение между FTP клиентом и FTP сервером с шифрованием защищено во внутренних локальных сетях с помощью шифрования SSL.

Таким образом, можно считать, что соединение защищено на всем участке передачи информации от сервера до клиента;

- На участке между роутерами R1 и R2 оба соединения надежно защищены с помощью VPN (IPSec). Сети клиента и серверов недоступны с ПК2;
- Таким образом, могут быть сконфигурированы и подвергнуты анализу другие типы защищенных соединений.

Представленная модель сети и методика анализа передаваемого по сети трафика может быть использована для приобретения студентами навыков конфигурирования защищенных соединений, а также для исследования процессов, происходящих в каналах передачи информации, как использующих защиту, так и без неё. Достоинство модели состоит в том, что она построена на базе свободно распространяемого программного обеспечения и может быть построена с использованием одного персонального компьютера. Аналогичным образом может быть смоделирована передача данных и других протоколов, например, путем замены сервера FTP на HTTP-сервер.

Литература

1. Васин, Н.Н. Технологии пакетной коммутации. Часть 1. Основы построения сетей пакетной коммутации: учеб. пособие.- Самара: ПГУТИ, 2014. – 239 с.

2. Васин, Н.Н. Технологии пакетной коммутации. Часть 2. Маршрутизация и коммутация в сетях пакетной коммутации: учеб. пособие.- Самара: ПГУТИ, 2015. – 261 с.

3. Laura Chappell, Wireshark Network Analysis. Second Edition. - Protocol Analysis Institute, dba “Chappell University”, 2012. – 461 с.

4. Ubuntu 14.04. Руководство по Ubuntu Server. Файл-серверы. FTP-сервер [Электронный ресурс].- Режим доступа: https://help.ubuntu.com/lts/serverguide/ftp-server.html. – Загл. с экрана.

5. Ubuntu 14.04. Руководство по Ubuntu Server. Защита. Сертификаты [Электронный ресурс].- Режим доступа: https://help.ubuntu.com/lts/serverguide/certificates-and-security.html. – Загл. с экрана.

6. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. СПб: Питер, 2011. – 944 с.

7. Vyatta System. VPN –виртуальная частная сеть. Справочное руководство. [Электронный ресурс].- Режим доступа: http://www.elco-tech.ru/files/Vyatta/Vyatta_VPNRef%20%28rus%29.pdf. – Загл. с экрана.