5. Маркушин А.Г. Оперативно-розыскная деятельность. Москва: Изд-во Юрайт, 2013. С. 13-14.
6. Поляков, В.В. Особенности расследования неправомерного удаленного доступа к компьютерной информации: автореф. дис. … канд. юрид. наук: 12.00.09 / В.В. Поляков. – Омск, 2008. – 28 с.
7. Горянинов К.К., Овчинский В.С., Синилов Г.К. Теория оперативно-розыскной деятельности. Москва: Изд-во ИНФРА-М, 2014. С. 328.
8. Федеральный закон от 12.08.1995 N 144-ФЗ (ред. от 21.12.2013) Об оперативно-розыскной деятельности // Собрание законодательства РФ. 14.08.1995. N 33. ст. 3349.
9. Горянинов К.К., Овчинский В.С., Синилов Г.К. Теория оперативно-розыскной деятельности. Москва: Изд-во ИНФРА-М, 2014. С. 335.

ГЕНЕРАЦИЯ ПАКЕТОВ С ПРОИЗВОЛЬНЫМ СОДЕРЖИМЫМ

К.Ю. Манзюк, АлтГУ, физико-технический факультет, 3 к.
Научный руководитель – ***А.В. Мансуров,*** к.т.н., доцент.

Задача генерации кадров/пакетов сетевого обмена с произвольным содержимым является достаточно актуальной как для вопросов исследования механизмов безопасности сетевого обмена и безопасности сетевых сервисов, так и для практического изучения принципов безопасной работы сетевых сервисов в условиях учебной лаборатории ФТФ. Данное исследование предполагает изучение принципов формирования сетевых кадров/пакетов с произвольной нагрузкой и последующую разработку приложения, специализированного на учебном лабораторном применении при выполнении лабораторных работ в учебной лаборатории безопасности информационных сетей.

Существующие программные средства генерации пакетов с произвольным содержимым являются либо излишне сложными, либо, наоборот, слишком простыми и непригодными для простого решения возникающих задач. Немаловажный аспект — это простой интерфейс, возможность модификации заголовков протоко-

лов начиная с 2го уровня в рамках 7уровневой модели ОСИ, наличие шаблонов для заполнения пакетов под конкретные задачи, бесплатность ПО. Очевидно, что рациональнее подойти к этому вопросу в виде разработки собственного приложения, отвечающего поставленным требованиям.

Структура разработанного в рамках исследования генератора кадров/пакетов с произвольной полезной нагрузкой выглядит следующим образом — интерфейс программы с возможностью модифицировать и управлять параметрами полезной нагрузки на различных уровнях (от 2 до 7), модуль формирования полезной нагрузки в виде стека различных популярных сетевых протоколов + поддержка шаблонов для выполнения действий по быстрому формированию полезной нагрузки, модуль взаимодействия с драйвером сетевого устройства (посредством ядра ОС или специальной библиотеки) для отправки сформированного кадра/пакета.

Графический интерфейс реализован при помощи библиотек Qt. Модуль по формированию полезной нагрузки реализован на языке C. Набор шаблонов динамически расширяется путем добавления новых. В настоящее время реализованы шаблоны для генерации произвольной полезной нагрузки ARP-ответа и DNS-ответа, что является достаточным для осуществления популярных сетевых атак «man in the middle», связанной с преднамеренной модификацией злоумышленником ARP- и DNS-кешей компьютеров, работающих в локальной сети.

Рис. 1. Структура разработанного программного решения в нотации UML.

Модуль взаимодействия с драйвером сетевого устройства использует специальные RAW-сокеты для отправки сформированного набора данных непосредственно в сетевое устройство для дальнейшей передачи по сети. Также модуль поддерживает работу

со специализированным модулем ядра ОС Линукс — pktgen, который используется для генерации трафика. После запуска модуль pktgen, создает поток ядра и привязывает его к CPU, к потоку привязываются устройства через которые будет проходит сгенерированный, такие как /dev/eth[0], /dev/vlan[]. Соответственно 1 CPU — 1 поток, 2 CPU — 2 потока и так далее. К каждому CPU можно привязать несколько устройств, с разными настройками, что дает необходимую гибкость в управлении генератором.

Разрабатываемый генератор пакетов с шаблоном формирования ARP-ответа является удобным средством для изучения популярной модельной атаки «man in the middle», когда происходит подделка ARP-ответов и внесение искаженной информации в ARP-таблицы устройств, обмен между которыми необходимо перехватить. Каждый компьютер составляет свою ARP-таблицу, которую затем использует для преобразования IP адресов в Ethernet адреса. Для этого посылается широковещательный ARP-запрос в сеть (тут будет кадр презентации с примерным видом запроса). Его можно интерпретировать следующим образом: "Если ваш IP-адрес совпадает с указанным, то сообщите мне ваш Ethernet-адрес". Все сетевые устройства получают этот запрос и, если указанный IP-адрес совпадает со своим, то создается ARP-ответ (кадр с ответом). Суть атаки «man in the middle» заключается в том, что при получении ARP-запроса он А к В дать корректный ARP-ответ, «представившись» В, аналогично проделать при ARP-запросе от В к А. Таким образом все общение между А и В будет осуществляться через «человека по середине».

Генератор нам нужен для того, чтобы сформировать ARP-ответ и отправить его в сеть.

Возможность подключения дополнительных шаблонов позволит выполнять более сложные сетевые атаки, связанные с подменой и отправкой искаженной информации в сетевой обмен атакуемых целей. Кроме этого, данный генератор является потенциально ценным инструментом для исследования эффективности работы средств защиты и безопасности локальных корпоративных сетей, протоколов безопасного обмена между сетевыми службами.

Список литературы

1. Столлингс В. Современные компьютерные сети: пер. с англ. СПб. Питер, 2003. 783 с. (Сер. "Классика computer science").

2. Таненбаум Э. Компьютерные сети: пер. с англ. СПб. Питер, 2003. 992 с. (Сер. "Классика computerscience").
3. Иванов И.П., Бойченко М.К. Мониторинг ресурсов узлов корпоративной сети // Вестник МГТУ им. Н.Э. Баумана. Сер. Приборостроение. 2010. № 2. С. 114–120.

РАЗРАБОТКА ГЕНЕРАТОРА РЕЧЕПОДОБНОЙ ПОМЕХИ В ПРОГРАММНОЙ СРЕДЕ LABVIEW

Я.И. Грачева, АлтГУ, физико-технический факультет, 5 к.
Научный руководитель – ***А.В. Егоров,*** к.ф.-м.н., доцент.

Человеческий разговор, и в частности переговоры, остается важнейшим каналом информационного взаимодействия. Очень часто развитие и введение в эксплуатацию новых систем связи сосредоточено на совершенствование именно этого метода общения. Одновременно усиливается потребность в обеспечении конфиденциальности речевого обмена и защите информации, имеющей речевую природу [1]. В настоящий момент разработан достаточно широкий арсенал различных средств защиты (формальных и неформальных), которые могут обеспечить требуемый уровень защищенности разного рода информации, в том числе и речевой. Из существующих методов защиты речевого сигнала широкое применение нашли методы активной акустической маскировки. В частности в целях данной маскировки используют такие виды помех как белый шум и «речеподобная» помеха.

В настоящей работе был разработан виртуальный прибор, позволяющий генерировать практически любую помеху в зависимости от выбранных параметров и базы файлов. Существует возможность его применения в учебных целях. Прибор создан в среде графического программирования, которая широко используется в промышленности, образовании и научно-исследовательских лабораториях в качестве стандартного инструмента для сбора данных и управления приборами. LabVIEW - мощная и гибкая программная среда, применяемая для проведения измерений и анализа полученных данных [2].

В системах акустической и виброакустической маскировки, как правило, используются шумовые помехи следующих видов: "белый" шум (с постоянной спектральной плотностью в рече-