Модель оценки защищенности алгоритмов маршрутизации трафика автоматизированных систем

Т. В. Лебедкина, email: alina010570@mail.ru
Н. Д. Степаненко

Краснодарское высшее военное училище
имени генерала армии С.М. Штеменко

Аннотация. *В статье рассматривается имитационная модель для оценки защищенности алгоритмов маршрутизации трафика в автоматизированных системах. Проанализированы алгоритмы маршрутизации трафика, использующиеся в автоматизированных системах, исследованы методы оценки защищенности алгоритмов маршрутизации трафика автоматизированных систем.*

Ключевые слова: *автоматизированная система, компьютерная атака, уязвимость, имитационное моделирование, защищаемая информация.*

Введение

При анализе защищенности автоматизированных систем (АС) одним из основных оцениваемых параметров является степень (уровень) уязвимости элементов сети к информационным атакам. В настоящее время для оценки данного параметра используется вероятностный подход, основанный на расчете вероятности уязвимости сетевого оборудования. Недостатком такого подхода является сложность или отсутствие адекватных математических методов расчета данной вероятности для различных сетевых устройств телекоммуникационных технологий и современных информационных атак, наличие неопределенности относительно задаваемых исходных данных. Это приводит к ошибкам при анализе защищенности АС, понижению управляемости сети в аспекте обеспечения информационной безопасности (ИБ).

1. Алгоритмы и протоколы маршрутизации трафика автоматизированных систем

В настоящий момент маршрутизация трафика в АС осуществляется с использованием общепринятых алгоритмов маршрутизации, таких как дистанционно-векторный алгоритм, алгоритм маршрутизации состояния канала и алгоритм маршрутизации по вектору состояния.

Основная функция сетевого уровня заключается в выборе маршрута для пакетов от начальной до конечной точки. В большинстве сетей пакетам приходится проходить через несколько маршрутизаторов. Алгоритмы выбора маршрутов и используемые ими структуры данных являются значительной областью при проектировании сетевого уровня. Алгоритм маршрутизации реализуется той частью программного обеспечения сетевого уровня, которая отвечает за выбор выходной линии для отправки пришедшего пакета [1].

Определение маршрута передачи данных происходит программно. Соответствующие программные средства носят названия протоколов маршрутизации. Логика их работы основана на алгоритмах маршрутизации.

Алгоритмы выбора маршрута можно разбить на два основных класса: неадаптивные и адаптивные.

Адаптивные алгоритмы в зависимости от способа вычисления оптимального маршрута можно разделить на следующие:

– дистанционно-векторный алгоритм – в данных алгоритмах маршрутизатор периодически всем своим соседям передает вектор сообщения, где указывает адреса всех известных ему подсетей и расстояние до них, в качестве расстояния используется промежуточные узлы – хопы. Примером протокола, основанного на дистанционно-векторном алгоритме является RIP.

– алгоритмы состояния связи – алгоритм снабжает все маршрутизаторы информацией, необходимой для построения подробного графа связей составной АС [3].

Протоколы маршрутизации:

RIP является протоколом маршрутизации, использующимся в сетях протокола IP. Протокол RIP принадлежит к классу так называемых IGP протоколов — Interior Gateway Protocol. Протоколы класса IGP, такие, как RIP или OSPF, используются, как правило, внутри автономных систем.

Протокол маршрутизации OSPF – протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала и использующий для нахождения кратчайшего пути алгоритм Дейкстры.

Протокол междоменной маршрутизации BGP сейчас повсеместно используется для маршрутизации в глобальной сети Интернет. Относится к классу протоколов маршрутизации внешнего шлюза. Протокол BGP предназначен для обмена информацией о достижимости подсетей между автономными системами, то есть группами маршрутизаторов под единым техническим и административным

управлением, использующими протокол внутридоменной маршрутизации для определения маршрутов внутри себя и протокол междоменной маршрутизации для определения маршрутов доставки пакетов в другие автономные системы [4].

Основной уязвимостью статической маршрутизации является преднамеренное или непреднамеренное изменение статических маршрутов на маршрутизаторах. С целью предотвращения данной уязвимости необходимо предпринять следующие меры. Прежде всего нужно реализовать физическую защиту, чтобы пользователи не имели доступа к маршрутизаторам.

Протокол RIP серьезно подвержен атакам прослушивания и модификации трафика. Основными угрозами, типичными для протокола маршрутизации RIP, являются [4]:

– ложные маршруты;
– понижение версии протокола RIP;
– взлом хэша MD 5.

Маршрутизаторы, работающие на протоколе RIP «слушают» трафик на порте 520. Таким образом, любой пакет соответствующего формата будет принят и обработан маршрутизаторам. В случае если аутентификация RIP не используется (применение RIP версии 1) или пароль пуст, злоумышленник сможет передать данному маршрутизатору неверные данные о маршрутах, перенаправив таким образом сетевой трафик через подконтрольные злоумышленнику узлы.

Для проведения компьютерной атаки злоумышленник, может использовать специализированные пакетные анализаторы, позволяющие перехватывать и анализировать именно обновления таблиц маршрутов. Типичная схема осуществления атаки представлена на рисунке 1.

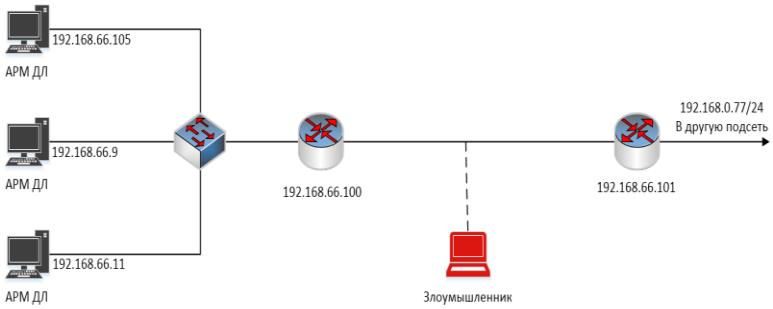

Рис. 1. Атака на протокол RIP

2. Методы оценки защищенности алгоритмов маршрутизации

Методы оценки защищенности алгоритмов маршрутизации в зависимости от характера показателей классифицируются следующим образом [1]:

- методы качественной оценки;
- методы количественной оценки;
- комплексные показатели.

К методам качественной оценки относятся методы, определенные в Руководящем документе Безопасность информационных технологий. Критерии оценки безопасности информационных технологий введенный в действие Приказом Гостехкомиссии России от 19.06.02 г. № 187. Недостатком данного метода является субъективное восприятие экспертом, проводящего оценку защищенности АС.

К методам количественной оценки относятся следующие методы: метод экспертных оценок; метод информационных потоков; метод весовых коэффициентов.

К комплексным показателям относят метод оценки CVSS (Common Vulnerability Scoring System). Данный стандарт входит в состав международного стандарта SCAP (Security Content Automation Protocol). Это протокол автоматизации управления данными безопасности – набор открытых стандартов, определяющих технические спецификации для представления данных по состоянию безопасности.

Необходимо ввести понятие рейтинга информационной безопасности сетевого оборудования. Рейтинг ИБ – это величина, которая показывает, насколько безопасна передача трафика через определенное сетевое оборудование (маршрутизатор, коммутатор) с учетом заданной конфигурации сети и настроек самого устройства. Под информационной безопасностью в данном случае подразумевается обеспечение конфиденциальности, доступности и целостности информации, передаваемой по сети [2].

Как видно из определения Рейтинга ИБ при его расчете должны учитываться следующие исходные данные:

- текущая или планируемая конфигурация сети.
- текущие или планируемые настройки сетевых устройств.

Анализ конфигурации сети позволяет учесть особенности структуры телекоммуникационной сети:

- расположение сетевых устройств;
- типы сетевых устройств;
- технологии передачи данных;
- логическое расположение интерфейсов (какие из интерфейсов соединяются с внешней сетью, а какие с внутренней) [4, 5].

Определение настроек сетевых устройств осуществляется путем автоматизированного анализа конфигурационных файлов устройства на соответствие определенным критериям: включены ли определенные политики безопасности, верно ли задана адресация, корректность настройки сетевых протоколов и т.п.

3. Структура, основное содержание и принципы функционирования имитационной модели оценки защищенности алгоритмов маршрутизации трафика в АС

Для оценки защищенности алгоритмов маршрутизации трафика в АС была разработана имитационная модель, представленная на рисунке 2.

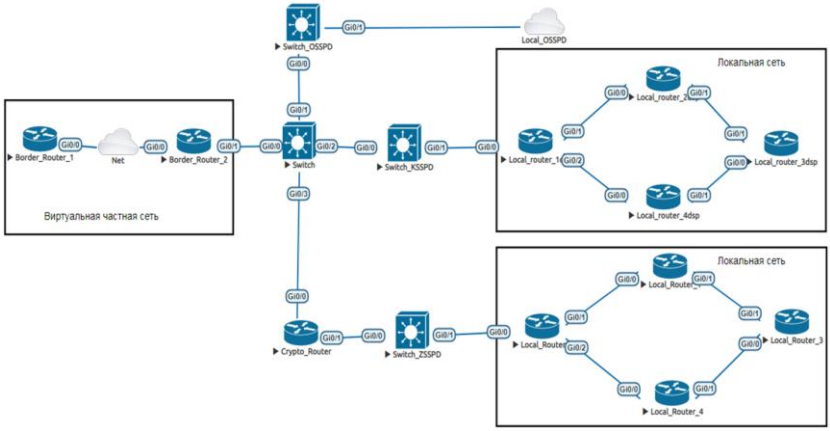

Рис. 2. Схема имитационной модели

Тестируемая часть имитационной модели состоит из виртуальных образов маршрутизаторов Cisco. Выбор данного виртуального образа обоснован аналогичностью логики функционирования маршрутизаторов Juniper MX 5000, Naters RT-3806 и других моделей, а также возможностью настройки протоколов маршрутизации BGP, RIP, OSPF.

Управляющая часть модели представляет собой виртуальную машину под управлением ОС Kali Linux 2017.1 с установленным и настроенным программным обеспечением, включающим; Nmap 7.25 [3]; Scapy 2.4.2.

Проводимые эксперименты заключаются в сравнении оценки защищенности алгоритмов маршрутизации трафика путем практического проведения КА на алгоритмы маршрутизации при осуществлении базовой настройки маршрутизаторов и теоретической

оценки опасности данных КА, а затем практического проведения тех же КА на алгоритмы маршрутизации при осуществлении настройки маршрутизаторов со встроенными механизмами защиты и оценки опасности КА.

Разработанная имитационная модель подразделяется на три:

– применение в локальной сети имитационной модели АС протокола RIP;

– применение в локальной сети имитационной модели АС протокола OSPF;

– применение в локальной сети имитационной модели АС протокола IS-IS.

В трех имитационных моделях пограничные маршрутизаторы (border_router_1 и border_router_2), применяют протокол BGP.

Сетевое оборудование, используемое в имитационной модели, настроено в зависимости от применяемых протоколов.

Практический анализ защищенности алгоритмов маршрутизации трафика заключается в проведении КА на протоколы маршрутизации, реализуемые в АС. Он будет осуществляться с использованием ОС Kali-Linux и установленной на нее утилиты Scapy. Scapy — сетевая утилита, написанная на языке Python, которая позволяет посылать, просматривать и анализировать сетевые пакеты. С помощью Scapy легко осуществлять такие процедуры, как: сканирование, трассировку маршрута, проверку хоста (probing), юнит-тестирование каких-либо сетевых функций, исследование сети и различные виды атак.

В данном случае рассмотрена атака перенаправления трафика. Данная атака заключается в следующем:

– формирование пакета с ложной информацией LSA.

– отправка данного пакета в атакуемую сеть.

После того, как проведена КА, необходимо осуществить расчет оценки опасности КА с учетом особенностей ее проведения, а также степени причиняемого ущерба, и необходимо осуществить настройку встроенных механизмов защиты протоколов маршрутизации.

Соответственно применены следующие механизмы:

– протокол RIP: применение криптографической аутентификации по алгоритму криптографического хеширования SHA; применение фильтров маршрутов; использование вместо RIP v1 RIP v2.

– протокол OSPF: применение криптографической аутентификации по алгоритму криптографического хеширования SHA; применение фильтров пакетов LSA, а также фильтров маршрутов.

– протокол BGP: применение криптографической аутентификации по алгоритму криптографического хеширования SHA.

Настроив механизмы защиты, необходимо повторно осуществить КА. Алгоритм проведения КА и используемое ПО осталось неизменным. При проведении КА на протокол OSPF было получено, что механизм аутентификации не позволил злоумышленнику поменять таблицу маршрутизации.

После проведения КА осуществлена теоретическая оценка ее опасности до настройки механизмов защиты и после их настройки [2].

Заключение

Для оценки защищенности алгоритмов маршрутизации трафика АС была разработана имитационная модель, в которой были проведены КА на протоколы маршрутизации в локальной сети, а также осуществлена оценка защищенности алгоритмов маршрутизации, до и после применения встроенных механизмов защиты протоколов маршрутизации. Разработанная имитационная модель, за счет виртуального моделирования АС, в частности настройки протоколов маршрутизации на сетевом оборудовании, позволяет осуществить анализ защищенности АС, без наличия сетевого оборудования в максимально короткое время.

Список литературы

1. Бирюков, А. А. Информационная безопасность: защита и нападение. / А. А. Бирюков ; М. : ДМК Пресс, 2007. – 434 с.

2. Полянский, Д. А. Оценка защищенности : учебное пособие / Д. А. Полянский ; Владимирский. государственный университет. – Владимир : Издательство Владимирского государственного университета, 2005. – 80 с.

3. Карамышев, В. И. Анализ уязвимостей протоколов маршрутизации / В. И. Карамышев // Сборник научных статей XX военно-научной конференции курсантов и операторов научной роты КВВУ. – Краснодар, 2017. – С 223-227.

4. Шерстобитов, Р. С. Маскирование интегрированных сетей связи ведомственного назначения / Р. С. Шерстобитов, С. Р. Шарифуллин, Р. В. Максимов // Системы управления, связи и безопасности. – 2018. – № 4. – С. 136–175.

5. Соколовский, С. П. Концептуализация проблемы проактивной защиты интегрированных информационных систем / С. П. Соколовский, Д. Н. Орехов // Научные чтения имени профессора Н. Е. Жуковского: сб. научн. стат. VIII Междунар. науч. метод. конф. (Краснодар, 20–21 декабря 2017 г.). – Краснодар, 2018. – С. 47–52.