УДК 681.3.053:681.32:007.5

ИНТЕЛЛЕКТУАЛЬНАЯ СИСТЕМА АНАЛИЗА ЗАЩИЩЕННОСТИ КОМПЬЮТЕРНЫХ СЕТЕЙ*

М.В. Степашкин[1], И.В. Котенко[2], В.С. Богданов[3]

В работе рассмотрена интеллектуальная система анализа защищенности компьютерных сетей, основанная на автоматической генерации общего графа атак и использовании качественных метрик защищенности. Общий граф атак отражает возможные распределенные сценарии атак с учетом конфигурации сети, реализуемой политики безопасности, а также местоположения, целей, уровня знаний и стратегий нарушителя. Метрики защищенности позволяют оценивать защищенность компьютерной сети с различной степенью детализации и с учетом разнообразных аспектов. Представлены структура системы, используемые в ней модели, в частности модели формирования графа атак и оценки уровня защищенности. Работа системы рассмотрена на тестовом примере.

Введение

В настоящее время наблюдается увеличение сложности используемых компьютерных сетей (КС), механизмов защиты и программного обеспечения, что приводит к увеличению количества уязвимостей в них. Используя комбинации имеющихся в сети уязвимостей и недостатков в ее конфигурации и применяемой политике безопасности, нарушители (как внешние, так и внутренние), в зависимости от своих целей, могут реализовать различные стратегии нападения. Эти стратегии могут быть направлены на реализацию различных угроз безопасности и включать цепочки компрометаций различных хостов.

Поэтому важной задачей для администратора компьютерной сети или ее проектировщика становится проверка того, обеспечивают ли

* Работа выполнена при финансовой поддержке РФФИ (проект №04-01-00167), программы фундаментальных исследований ОИТВС РАН (контракт №3.2/03) и при частичной финансовой поддержке, осуществляемой в рамках проекта Евросоюза POSITIF (контракт IST-2002-002314)

[1] *199178, С.-Петербург, 14 линия, 39, СПИИРАН, stepashkin@comsec.spb.ru*
[2] *199178, С.-Петербург, 14 линия, 39, СПИИРАН, ivkote@comsec.spb.ru*
[3] *199178, С.-Петербург, 14 линия, 39, СПИИРАН, bogdanov@comsec.spb.ru*

планируемые для применения или уже используемые параметры конфигурации сети и механизмы защиты требуемый уровень защищенности. Для решения данной задачи служат автоматизированные интеллектуальные средства (системы) анализа защищенности (САЗ) [McNab, 2004]. Эти системы должны базироваться на формализованных знаниях специалистов в области защиты информации, учитывать различные модели нарушителя (его местоположение, уровень знаний и умений, стратегии поведения), многошаговый и распределенный характер компьютерных атак, производить расчет комплекса метрик защищенности, характеризующих защищенность компьютерной сети в целом и ее компонентов в отдельности, учитывать конфигурацию компьютерной сети и реализуемые в ней политики безопасности. Полученные результаты анализа защищенности могут обеспечить выработку обоснованных рекомендаций по устранению “слабых мест” и усилению защищенности компьютерной сети.

В работе представлена разработанная авторами *интеллектуальная система анализа защищенности*, реализующая подход на базе автоматической генерации общего графа атак и использовании качественных метрик защищенности. Граф атак отражает возможные распределенные сценарии атак с учетом конфигурации сети, реализуемой политики безопасности, а также местоположения, целей, уровня знаний и стратегий нарушителя. Метрики защищенности позволяют оценивать защищенность компьютерной сети с различной степенью детализации и с учетом разнообразных аспектов.

Работа организована следующим образом. В *первом разделе* кратко описываются используемые в интеллектуальной САЗ модели. Во *втором разделе* приведена архитектура разработанной системы анализа защищенности. В *третьем разделе* дается описание работы системы на тестовом примере. В *заключении* формулируются результаты работы.

1. Модели, используемые в системе анализа защищенности

В предлагаемой системе анализа защищенности используются две базовые модели: (1) модель формирования общего графа атак; (2) модель оценки уровня защищенности.

Модель формирования общего графа атак служит для построения графа атак с использованием информации о различных типах атакующих действий (разведывательных; подготовительных, служащих для создания условий реализации атакующих действий последующих классов; направленных на нарушение конфиденциальности, целостности, доступности; приводящих к получению нарушителем прав локального пользователя или администратора), с учетом первоначального положения

нарушителя, его уровня знаний и умений, конфигурации компьютерной сети и реализуемой в ней политики безопасности.

Общий граф атак состоит из объектов, которые можно подразделить на базовые и составные. Вершины графа задаются с использованием базовых объектов. Для формирования различных последовательностей действий нарушителя базовые объекты связываются на графе атак с помощью дуг. Составные объекты графа строятся на основе объединения базовых объектов с помощью дуг. К *базовым объектам* общего графа атак относятся объекты, принадлежащие к типам “хост” и “атакующее действие”. *К составным объектам* отнесем объекты типов “трасса”, “угроза” и “граф”. *Трасса атаки* — это совокупность связанных вершин общего графа атак, первая из которых представляет хост, соответствующий первоначальному положению нарушителя, а последняя не имеет исходящих дуг. Под *угрозой* будем понимать множество различных трасс атак, имеющих одинаковые начальную и конечную вершины.

Алгоритм формирования общего графа атак основан на реализации следующей последовательности действий: (1) реализация действий по перемещению нарушителя с одного хоста на другой, (2) реализация разведывательных действий по определению живых хостов, (3) реализация сценариев (множества действий) разведки для каждого обнаруженного хоста и (4) реализация атакующих действий, использующих уязвимости программного и аппаратного обеспечения и общих действий пользователя.

Модель оценки уровня защищенности охватывает систему различных метрик защищенности (МЗ) и правил (формул), используемых для их расчета [Kotenko et al., 2005; Котенко и др., 2006]. Множество всех МЗ строится на основе сформированного общего графа атак. МЗ могут характеризовать защищенность как базовых, так и составных объектов графа атак. Основной метрикой (результатом работы) интеллектуальной САЗ является *общий уровень защищенности*, который может принимать одно из следующих четырех значений: красный, оранжевый, желтый и зеленый.

2. Архитектура интеллектуальной системы анализа защищенности

Архитектура разработанной интеллектуальной системы анализа защищенности компьютерных сетей приведена на рис. 1. На этапе проектирования, САЗ оперирует с моделью анализируемой компьютерной сети (системы), которая базируется на заданных спецификациях анализируемой сети и политики безопасности. На этапе эксплуатации для

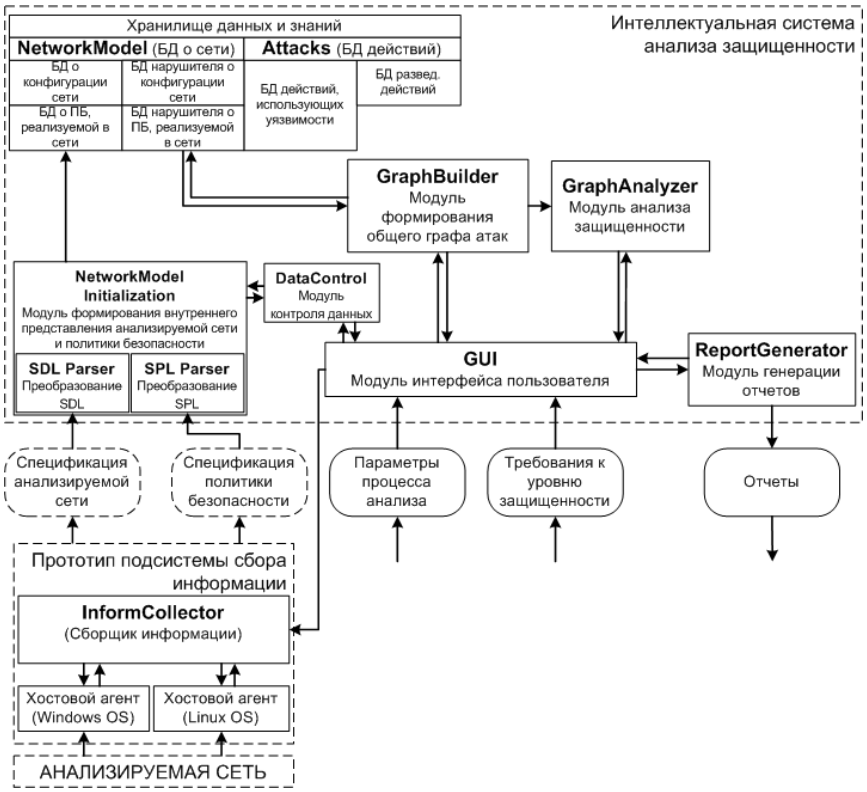

Рис. 1. Структура интеллектуальной системы анализа защищенности

построения модели анализируемой сети используется подсистема сбора информации об анализируемой компьютерной сети.

Модуль интерфейса пользователя позволяет пользователю управлять работой всех компонентов системы, задавать входные данные, просматривать отчеты по анализу защищенности и т.п.

Хранилище данных и знаний состоит из следующих групп баз данных (БД): (1) группа БД о конфигурации анализируемой компьютерной сети и используемой политике безопасности (*NetworkModel*); (2) группа БД атакующих действий (*Attacks*).

Группа БД об анализируемой компьютерной сети состоит из следующих баз: (1) БД о конфигурации сети; (2) БД о политике безопасности, реализуемой в сети; (3) БД нарушителя о конфигурации сети; (4) БД нарушителя о политике безопасности, реализуемой в сети. Структурно данные базы данных попарно совпадают (базы о конфигурации сети и реализуемой в ней политике безопасности

соответственно) и содержат информацию об архитектуре сети (например, типы и версии используемых операционных систем, приложений, список открытых портов и т.п.) и правил, описывающих функционирование сети. *БД о конфигурации сети* является внутренним представлением спецификации анализируемой сети, которое используется для определения результатов выполнения атакующих действий во время построения общего графа атак. *БД нарушителя о конфигурации* анализируемой сети является ее внутренним представлением (так, как ее представляет себе нарушитель). Данное представление является результатом выполнения последовательности атакующих действий. *БД о политике безопасности*, реализуемой в анализируемой сети, содержит общие правила, описывающие функционирование сети, например, "локальные пользователи хоста H не могут запускать приложение A". На основе *БД нарушителя о политике безопасности* возможно планирование последовательности выполняемых нарушителем действий (например, если согласно политике безопасности только локальные администраторы могут читать файл F, тогда нарушитель должен получить эти права, т.е. должен реализовать некоторую последовательность действий, направленных на получение прав администратора).

Группа баз данных атакующих действий состоит из следующих баз: (1) БД действий, использующих уязвимости; (2) БД разведывательных действий. *БД действий, использующих уязвимости* (в отличие от других баз данной группы) строится на основе внешней базы данных уязвимостей. Атакующие действия в данной базе делятся на следующие группы: (1) действия, направленные на получение прав локального пользователя; (2) действия, направленные на получение прав администратора; (3) действия, направленные на нарушение конфиденциальности, (4) целостности и (5) доступности. *БД разведывательных действий* содержит действия, направленные на удаленное получение информации о хосте или сети. Описание разведывательных действий не содержится во внешних базах уязвимостей. Информацию о методах и средствах реализации нарушителем разведывательных действий можно получить лишь экспертным путем.

NetworkModel Initialization преобразует информацию о конфигурации сети и реализуемой в ней политике безопасности, задаваемых пользователем (эта информация задается при помощи специализированных языков System Description Language (SDL) и Security Policy Language (SPL)) во внутреннее представление.

DataControl используется для обнаружения некорректно заданных или отсутствия необходимых для процесса анализа защищенности данных. Например, пользователь может ввести ошибочное имя сервиса или

указать, что порт 21 открыт, но не определить какое приложение обрабатывает поступающие на данный порт запросы.

GraphBuilder строит общий граф атак, эмулируя действия нарушителя в анализируемой компьютерной сети и используя информацию о доступных атакующих действиях различных типов (атакующие действия, использующие уязвимости, разведывательные действия, обычные действия легитимных пользователей), о конфигурации сети и реализуемой в ней политике безопасности. Данный модуль расставляет в вершинах графа метрики защищенности базовых объектов, на основе которых *GraphAnalyzer* рассчитывает метрики составных объектов.

ReportGenerator служит для агрегации полученных в процессе анализа защищенности данных (информации об обнаруженных уязвимостях, рекомендаций по повышению уровня защищенности) и формирования на их основе единого отчета.

Подсистема сбора информации служит для сбора информации от программных хостовых агентов и формирования на основе данной информации спецификаций, описывающих конфигурацию сети и реализуемую в ней политику безопасности. *Хостовые программные агенты* используются для сбора необходимых для создания модели анализируемой компьютерной сети данных. Так, например, данные агенты могут реализовывать анализ конфигурационных файлов операционной системы и различных программных средств. *InformCollector* служит для сбора информации, поступающей от хостовых агентов, ее представления на SDL и SPL и ее передачи компонентам САЗ (модулю *NetworkModel Initialization*).

3. Тестовый пример

Рассмотрим компьютерную сеть, структура которой представлена на рис. 2. Во время построения общего графа атак происходит следующие основные изменения в представлениях нарушителя об атакуемой сети (рис. 3):

(1) после реализации атаки “ping” (с учетом таблицы маршрутизации трафика) нарушитель узнает о существовании хоста “Server”;

(2) нарушитель реализует атаку, использующую уязвимость в ftp-сервисе и позволяющую получить удаленному злоумышленнику права локального администратора (хост “Server” выделен красным цветом);

(3) нарушитель использует полученные права на хосте “Server” для сбора всей доступной информации, анализируя которую, злоумышленник понимает, что используется перенаправление портов (port forwarding), и хост “Server” подключен к другому сетевому концентратору. Следовательно, нарушителю выгодно перейти на хост “Server”, так как такой переход открывает нарушителю доступ в другой сегмент сети;

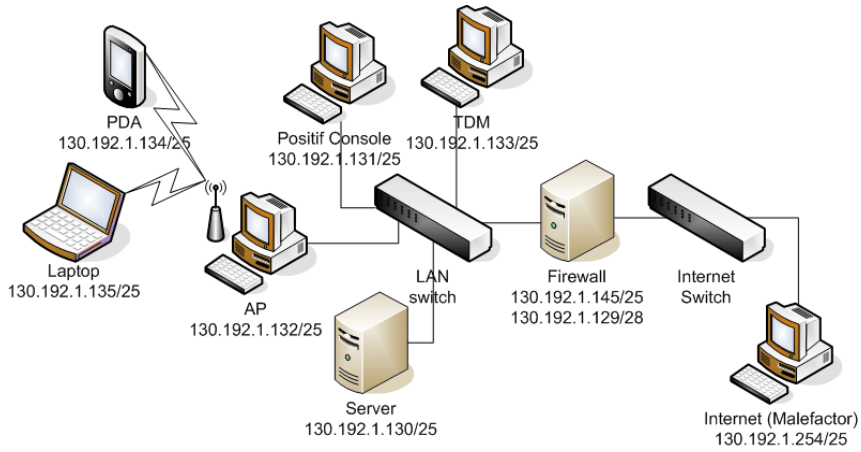

Рис. 2. Структура тестовой компьютерной сети

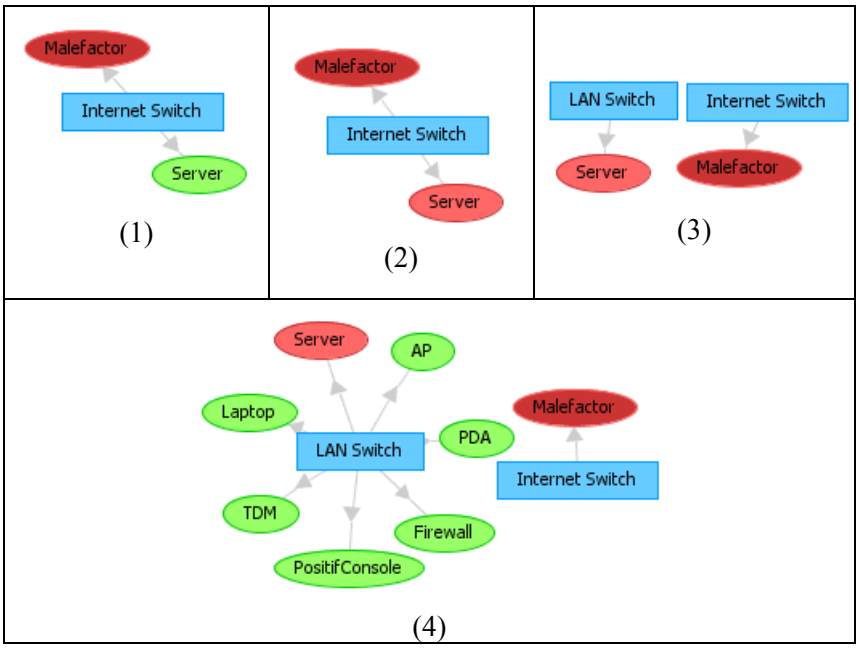

Рис. 3. Изменение представлений нарушителя об атакуемой компьютерной сети

(4) перейдя на “Server”, нарушитель реализует атаку “ping” и узнает о существовании множества других хостов, которые он последовательно пытается атаковать.

Основными результатами процесса анализа защищенности являются: (1) множество обнаруженных уязвимостей (например, уязвимость “ServU-MDTM” на рис. 4); (2) множество метрик защищенности (например, количество трасс атак, проходящих через хост “Server”). В результате анализа защищенности для тестовой компьютерной сети был получен “красный” уровень защищенности. Дальнейшими действиями пользователя должны стать: (1) устранение обнаруженных уязвимостей и “узких” мест (обновление конфигурации сети и реализуемой политики защищенности); (2) повторный анализ защищенности сети, заданной обновленными спецификациями. Общий граф атак для тестовой компьютерной сети представлен на рис. 4.

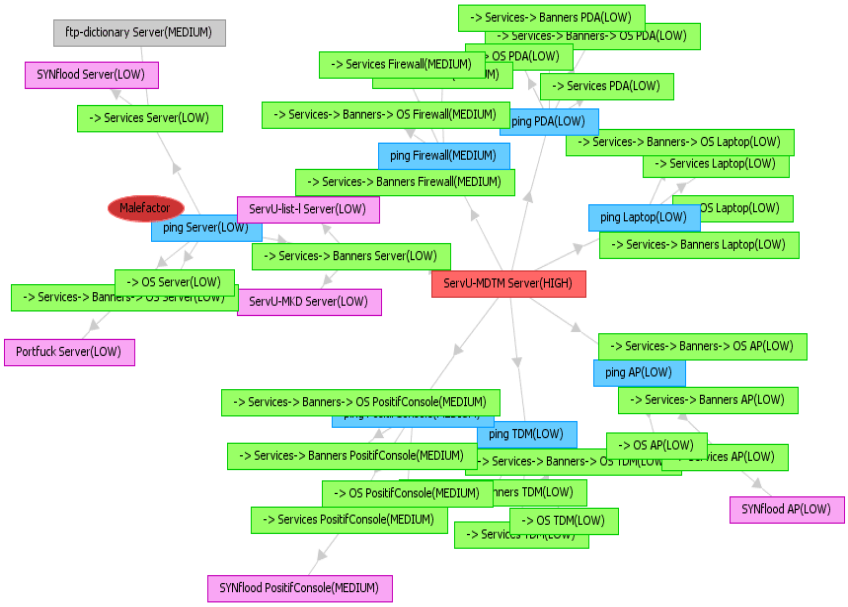

Рис. 4. Общий граф атак для тестовой компьютерной сети

4. Заключение

В работе рассмотрена интеллектуальная система анализа защищенности, предназначенная для реализации анализа уязвимостей и оценки уровня защищенности на различных этапах жизненного цикла

компьютерных сетей. Функционирование предложенной интеллектуальной САЗ основано на подходе, обладающем следующими *особенностями*: (1) использование для анализа защищенности комплекса различных моделей, построенных на экспертных знаниях, в том числе моделей злоумышленника, моделей сценариев атак, формирования графа атак, расчета метрик защищенности и определения общего уровня защищенности; (2) учет разнообразия местоположения, целей и уровня знаний нарушителя; (3) использование при построении общего графа атак не только параметров конфигурации компьютерной сети, но и правил реализуемой политики безопасности; (4) учет как собственно атакующих действий (по использованию уязвимостей), так и разрешенных действий пользователя и действий по разведке; (5) возможность исследования различных угроз безопасности для различных ресурсов сети; (6) возможность определения "узких мест" (хостов, ответственных за большее количество трасс атак и уязвимостей, имеющих наиболее высокую возможность компрометации); (7) возможность задания запросов к системе вида "что если", например, какова будет защищенность при изменении определенного параметра конфигурации сети, правила политики безопасности; (8) применение для построения графа атак актуализированных баз данных об уязвимостях (например, OSVDB [OSVDB, 2006]); (9) использование для расчета части первичных метрик защищенности подхода CVSS [CVSS, 2006]; (10) применение для вычисления метрик защищенности качественных методик анализа риска (в частности, модифицированной методики оценки серьезности сетевой атаки SANS/GIAC и методики FRAP [FRAP, 2006]).

Список литературы

[Котенко и др., 2006] Котенко И. В., Степашкин М. В., Богданов В. С. Анализ защищенности компьютерных сетей на различных этапах их жизненного цикла // Изв. вузов. Приборостроение. № 4. — СПб., 2006.

[CVSS, 2006] CVSS. Common Vulnerability Scoring System. http: // www.first.org / cvss. 2006.

[FRAP, 2006] FRAP. Facilitated Risk Analysis Process. http: // www.peltierassociates.com. 2006.

[Kotenko et al., 2005] Kotenko I. V., Stepashkin M. V. Analyzing Vulnerabilities and Measuring Security Level at Design and Exploitation Stages of Computer Network Life Cycle // Lecture Notes in Computer Science. Springer-Verlag, Vol. 3685. 2005.

[McNab, 2004] McNab C. Network Security Assessment. O'Reilly Media, Inc, 2004.

[OSVDB, 2006] OSVDB: The Open Source Vulnerability Database. http://www.osvdb.org/. 2006.