УДК 004.7

А.А. Сапожников

Обнаружение аномальной сетевой активности

Основная цель данной работы – создание системы мониторинга ИТ-инфраструктуры предприятия на основе различных продуктов с открытыми исходными кодами. Элементы данной системы должны динамически адаптироваться к изменяющимся параметрам наблюдаемых систем и выявлять аномалии в их поведении.
Ключевые слова: сетевая безопасность, информационные технологии, автоматизированная система.

Локальные вычислительные сети современных предприятий наполнены различными приложениями и решают множество задач. Поведение сети формируется пользователями, сервисами программно-аппаратных средств, другими сетевыми устройствами. Под нормальным функционированием сети имеется в виду следующее: гарантированное предоставление сервисов и устойчивость к различным стрессовым воздействиям, которые в самом общем рассмотрении можно разделить на непроизвольные (отказ оборудования, ошибки в программах) и произвольные (целенаправленные атаки) [1, 2].

Наблюдаемые события. Как правило, предотвратить атаку невозможно, поэтому есть смысл сконцентрировать все усилия на мониторинге последствий атаки. Атаки можно разделить на три уровня:

– транспортный. Под атаками на транспортный уровень будем понимать атаки на протоколы канального, сетевого и транспортного уровней стека TCP/IP. К этому уровню относятся, например, различные виды сканирования, arp-spoofing, ip spoofing [4];

– прикладной. Под этим уровнем будем понимать атаки, направленные на ошибки в реализации различных протоколов прикладного уровня стека TCP/IP. Примерами подобных атак могут быть dns cache-poisoning, smb-die, http-response splitting;

– уровень сервиса. К атакам данного уровня отнесем всевозможные атаки, вызванные ошибками в некорректной обработке пользовательских данных. Примеры подобных атак – XSS, SQL-injection, различные переполнения и т.д. [5, 6].

Обнаружить атаку можно двумя методами:

– сигнатурным. Данный метод сводится к поиску признаков уже известных атак. Преимущество сигнатурного метода в том, что он практически не подвержен ложным срабатываниям. Минусом данного метода является невозможность обнаруживать незаложенные в систему атаки.

– аномальным. Заранее известно, какими функциональными параметрами обладает то или иное приложение или сервис в нормальном состоянии, и любое отклонение от него считается атакой. Метод поиска аномалий позволяет реагировать на ранее неизвестные атаки, но подвержен ложным срабатываниям и требует точной настройки для каждого наблюдаемого объекта.

Оба метода обнаружения атак могут работать на всех трех уровнях.

Результатом любой атаки, в случае успеха, являются утечка информации, например, атака ether-leak, либо изменение каких-либо параметров атакованной системы, например открытие порта, прекращение работы некоторой программы, значительное изменение объемов использования некоторого ресурса системы программой (например, памяти, процессорного времени и т.п.), запуск новой программы на выполнение. Подобные события, происходящие в системе, можно отслеживать с помощью программных средств [2].

Так как значительное изменение объемов использования ресурсов может происходить и при нормальном режиме работы системы (например, увеличение обращений к почтовому серверу в начале рабочего дня), то возникает проблема определения поведения программы: нормального или аномального. Предлагается решение данной проблемы на основе статистических методов анализа.

Обнаружение аномалий. Идея заключается в следующем. В основном все реальные автоматизированные информационные системы имеют циклический характер функционирования, который определяется рабочей неделей или производственным технологическим процессом.

Предположим, что существует отдельный период на начальном этапе работы системы, в течение которого мы можем утверждать, что система работает в нормальном режиме. Если такой интервал времени существует, то назовем его периодом обучения [7]. В течение периода обучения будем отслеживать использование различных ресурсов программами и на базе накопленной информации сможем построить функцию прогнозирования дальнейшего поведения программ. В период рабочей эксплуатации системы будем постоянно производить мониторинг использования различных ресурсов программами. Полу-

ченные данные будем сравнивать с прогнозируемыми. Если различие между прогнозируемым и фактическим использованием ресурсов превышает некоторое допустимое значение, то поведение программы считается аномальным. При этом принимается решение об изменении режима функционирования программы с целью предотвращения нарушения стабильности работы всей системы в целом.

Построение функции прогнозирования. Функция прогнозирования строится на базе функциональной зависимости использования ресурса элементом сети от времени в течение периода обучения (далее исходная функция) следующим образом. Вначале производится сглаживание исходной функции для отфильтровывания случайных шумов. Сглаживание выполняется вычислением скользящего взвешенного пятиточечного среднего с оптимально подобранными весовыми коэффициентами.

Далее производится разделение исходной функции на две составляющих. Первая – тренд – определяет тенденцию в использовании ресурса. Вторая – сезонная компонента – определяет периодическую составляющую исходной функции. Выделение тренда осуществляется вычислением математического ожидания значений исходной функции на достаточно большом временном отрезке. Сезонная компонента находится как разность сглаженной исходной функции и тренда. При дальнейшем анализе сезонной компоненты производится выделение основных гармонических составляющих. Для этого используется дискретное преобразование Хартли (аналог преобразования Фурье) с последующим отбрасыванием малозначимых коэффициентов.

Функция прогнозирования строится как сумма тренда и основных гармонических составляющих сезонной компоненты с соответствующими коэффициентами. Затем производится расчет среднеквадратичного отклонения сглаженной исходной функции от функции прогнозирования, на основе которого определяется качество прогноза и вычисляется максимально допустимое отклонение фактического поведения от ожидаемого.

Выводы. Данная разработка является инструментом, позволяющим повысить отказоустойчивость и облегчить администрирование автоматизированных систем. Следствием этого является снижение затрат на обслуживание АС в целом [8]. Кроме того, кратковременный сбой в работе большинства существующих информационных систем может привести к потере важной информации, значительному экономическому ущербу, уменьшению количества клиентов и т.п. [3]. Поэтому, любое увеличение отказоустойчивости системы способно снизить потери, возникающие в результате сбоев АС [4].

Литература

1. Белов Е.Б. Основы информационной безопасности: учеб. пособие для вузов / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. – М.: Горячая линия – Телеком, 2006. – 544 с.

2. Гайдамакин Н.А. Разграничение доступа к информации в компьютерных системах. – Екатеринбург: Изд-во УрГУ, 2003. – 328 с.

3. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. – СПб.: Наука и техника, 2004. – 384 с.

4. Garfinkel S. Practical Unix & Internet Security, O'Reilly / S. Garfinkel, A. Schwartz, G. Spafford. ISBN 0-596-00323-4. – 2003. – 984 p.

5. Hoglund G. Exploiting Software. How to Break Code / G. Hoglund, G. McGraw, A. Wesley. – 2004. – 512 p.

6. Foster J.C., Programmer's Ultimate Security DeskRef / J.C. Foster, C. Steven, F. Syngress. – 2004. – 700 p.

7. Сапожников А.А. Мониторинг состояния автоматизированной системы и обеспечение стабильности / А.А. Сапожников, А.В. Жуков, М.Л. Карманов, П.В. Збицкий // Сб. матер. Всерос. конкурса инновационных проектов аспирантов и студентов по приоритетному направлению развития науки и техники «Информационно-телекоммуникационные системы». – М.: ГНИИ ИТТ «Информика», 2005. – С. 123–124.

8. Сапожников А.А. Практика централизованного мониторинга сетей // Матер. междунар. конф. «Проблемы функционирования информационных сетей». – Новосибирск: ЗАО РИЦ Прайс Курьер, 2006. – С. 257–260.

Сапожников Антон Александрович
ГОУ ВПО «Южно-Уральский государственный университет»,
аспирант каф. цифровых радиотехнических систем
Эл. адрес: anton.sapozhnikov@kb.susu.ac.ru

A.A. Sapozhnikov

Anomaly network activity detection

That paper discusses one of network monitoring problem decision based on various open source software. Monitoring system is easily configurable, dynamically adopts to variations of monitored network and detects deviations of them.

Keywords: network safety, information technology, automated system.