 ISSN 2226-3780

УДК 004.056.53
DOI: 10.15587/2312-8372.2015.51120

Балакин С. В.

ВЫЯВЛЕНИЕ КОМПЬЮТЕРНЫХ АТАК С ПОМОЩЬЮ МОНИТОРИНГА СЕТЕВЫХ ОБЪЕКТОВ

Представлен анализ результатов обнаружения компьютерных атак на основе анализа мониторинга сетевых объектов. Определены погрешности в расчетах вероятности формулы атак и внесены корректировки, которые значительно повышают показатели производительности, полученные ранее. Разработана модель обнаружения атак на основе информации о поведении объектов сети и их взаимодействии.

Ключевые слова: *атака, компьютерная система, сетевые объекты, вторжение, информационная система, состояние объекта.*

1. Введение

Способов обнаружения вторжений сейчас очень много, но большинство из них либо невозможно применить на практике, либо настолько громоздкие, что существенно снижают производительность системы пользователя, либо самой сети. Поэтому вопрос актуальности данных разработок кроется по большей степени в конкретизации и модернизации существующих методов, которые теоретически выполняют поставленные цели, но на практике трудно применимы.

Также использование инструментов обнаружения аномалий и атак затруднено сферами назначения. Чем уже и более конкретизирована специальность — тем проще применять к ней те или иные инструменты. Чаще всего от самой конкретики и исходят те или иные методы, которые наилучшим способом могут «покрыть» все дыры в обеспечении безопасности.

Рассматривалась также возможность работы с нейронными сетями. Но огромным минусов при работе с ними стала трудность верификации результатов работы обучаемых выборок.

Для работы с сетевыми элементами отлично подходит адаптивный метод, который даже с низкой вычислительной сложностью будет иметь низкий уровень ложных оповещений. Так как этот метод имеет высокую производительность и минимальные вычислительные мощности, то он отлично подойдет не только для работы с базами данных (для чего он изначально был разработан), а и для описания поведения сетевых элементов. Такой метод сохранит высокую отказоустойчивость и минимальную нагрузку на процессор при выявлении атак или незапротоколированных действий. Адаптивность в свою очередь поможет задействовать решение проблемы на одной системе — для ряда других. Именно проблема адаптивности является критической для большинства готовых решений, но комбинируя этот метод можно сохранить и усовершенствовать саму формулу атак с помощью сетевых элементов. Актуальность проведенных исследований является востребованной, так как автор статьи получит продукт, который можно использовать для любых систем именно благодаря адаптивности.

2. Анализ литературных данных и постановка проблемы

Одной из первых работ в этой отрасли была [1], которая и определила основные понятия и решения проблемы. Первые работы были скорее концептуальными — в них пытались не построить определенные фильтры или методы, а попытаться применить теорию вероятности и математические подходы к решению данной задачи.

В труде Шейнера [2] внимание сосредоточено на вопросах автоматического поиска уязвимости программ и протоколов критериями поведения самой системы.

Множество методик построены на неформальных методах [3], таких как сигнатурный, в котором трудно получить теоретические оценки эффективности, корректности и конечности [4]. Модель, изложенная в работе решает эту проблему. В основу модели взяты наработки работ [5, 6].

Труды Вигны и Кемерера [7] касаются языка STATL и моделей атак, основанных на нем. Авторы отталкиваются от того, что атака базируется на состояниях и переходах. Главный минус предложенной системы в отсутствии инструментов для распределения потоков атак и действий самой системы и пользователя.

Работа Городецкого и Котенко [8] описывает атаку с точки зрения атакующего, и оперирует формализованным понятием цели.

3. Объект, цель и задачи исследования

Объектом работы является выявление атак.

Цель работы — создание метода обнаружения атак с помощью элементов сети. При этом особенно важно оставить уровень производительности на прежнем высоком уровне, так как будет недопустимым израсходовать все ресурсы пользователя на решение одной задачи.

В ходе работы поставлены задачи:

— выделить классы атак для тестирования представленной модели;

— разработать комбинированный метод обнаружения атак на основе информации о поведении объектов сети.

4. Результаты обзора методов выявления атак с помощью мониторинга сетевых объектов

Рассмотрена модель работы сети при атаках в виде системы переходов [9]:

— работа сети определяется состояниями переходов объектов;

— состояния делятся на безопасные и опасные;

— вводится понятие траектории и поведения объекта;

— под атакой понимается переход из безопасного состояния в опасное;

— для каждого вида атак вводится понятие автомата первого рода, он принимает любую траекторию данного класса;

— для каждого класса объектов вводится понятие автомата второго рода, он принимает любую траекторию данного объекта и позволяет различать траектории двух классов — опасных и аномальных.

Предложен язык описания поведения объектов сети, который может описывать состояния объектов и переходы.

Система выявления атак состоит из разделов:

— алгоритм обнаружения атак (описывающий обнаружения атак на основе поведения объектов сети в режиме реального времени);

— архитектура системы обнаружения атак;

— оценка эффективности.

Для всех типов объектов определены операции доступа (открытие, чтение, запись, запуск на исполнение). Доступ может быть прямым или непрямым (использует иные объекты). Под доступом понимается набор действий в виде: открыть доступ по задачи, выполнить задачу, закрыть доступ по задачи.

Для каждого объекта (особенно это касается баз данных) есть набор правил на доступ, которые определяют какие элементы могут взаимодействовать. Доступ к объекту, не попадающий под эти правила будем называть несанкционированным.

Объекты в системе характеризуется состоянием. Состояние объекта — это множество объектов, имеющих доступ к нему, а также характеристика его загруженности.

Основываясь на разработках при работе с состояниями объекта в работе [9], объекты разделим на два вида: активные и пассивные. Пассивный объект не имеет доступа к объектам, а активный имеет. Выходя из определения состояний объекта, атаку на сети представим следующей формулой [9]:

$$K: (S,\Sigma,Tr,S_o,Q),$$

где S — множество состояний объекта; Σ — множество действий объекта; Tr —переходы из состояний; S_0 — первоначальное состояние; Q — конечные состояния; K — опасное состояние объекта.

Данная формула описывает возможности переходов объектов из разных состояний, но для более детального описания атак стоит добавить время активности элементов сети (T). Новый элемент позволит детальнее описать действия и упростить анализ и разбор активности в самой сети. В таком случае формула атаки будет конкретизирована и примет вид:

$$K: (S,\Sigma,T,Tr,S_o,Q).$$

Атака на объект будет выявлена при выполнении условий:

1. Атака принадлежит множеству K.
2. Параметры атаки были под наблюдением распознающих автоматов и действия наблюдались в порядке выполнения.

При соблюдении данных условий предложенный вариант обнаружения атак будет корректен. Для каждой атаки на входе, результатом работы алгоритма будет являться хотя бы одно сообщение об атаке. На рис. 1 указана упрощенная модель сравнения опасного и конечного состояния элемента сети. В выборке внимание уделялось таким типам атак, как Remote root, DoS и Port Scan.

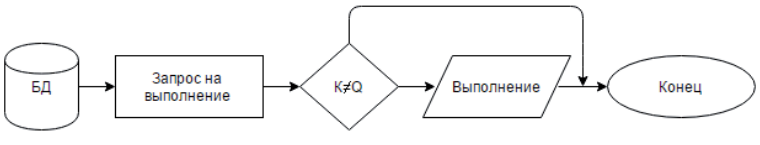

Рис. 1. Блок схема выборки и сравнения состояний записей БД

В случае со множеством объектов скомбинируем элементы подхода на основе data-mining [10]. В таком случае множество действий — это выражения вида:

$$[X \rightarrow Y,\ C],$$

где X, Y — подмножества множества значений на множестве атрибутов, а C — процент записей в базе $[X, Y]$:

$$C = \frac{Support(X \cup Y)}{Support(X)}.$$

Этот метод позволяет еще более конкретизировать условия выборки атак с помощью использования выборок записей баз данных и конкретизации множества действий объекта Σ.

На рис. 2 проиллюстрированы результаты работы первой и второй формулы.

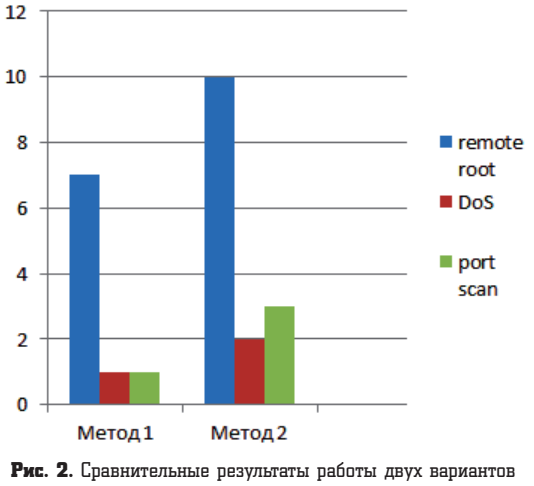

Рис. 2. Сравнительные результаты работы двух вариантов формулы

Отчетливо видно, что второй метод дает более корректные результаты. Это связано с детальной конкретизацией формулы атак. При этом следует из расчетов, что именно вторая формула позволяет определять на 20 % атак больше.

5. Выводы

В статье обсуждается применение выявления компьютерных атак с помощью анализа поведения сетевых элементов, и приводятся результаты исследований в этой области. Основной целью исследования является разработка модели выявления атак на основе поведения элементов сети и их связей, и использовании знаний, полученных из различных источников и сфер деятельности, для диагностики и усовершенствовании результатов. Объектом работы является обнаружение компьютерных атак.

Использование современных средств обнаружения атак позволяет безопасно осуществлять сбор и анализ информации в компьютерных сетях по всему миру. В этой статье предлагается модель функционирования сетей в условиях воздействия компьютерных атак в форме системы переходов сетевых элементов из безопасных в опасные состояния, для проведения фильтрации действий и диагностики системы.

Представлен анализ результатов выявления атак на основе анализа поведения этих элементов. Определены погрешности в расчетах вероятности формулы атак и внесены корректировки, которые значительно улучшают показатели производительности, полученные ранее. Разработана модель обнаружения атак на основе информации о поведении объектов сети и их взаимодействии.

Результаты исследований могут быть применены для защиты информации, а также специалистами в высокоскоростных системах, использующих каналы передачи данных с высокой пропускной способностью.

Достигнута одна из основных целей данной работы, которая и заключалась в создании метода обнаружения атак на основе анализа поведения сетевых объектов. Данный метод отлично проявил себя на практике, позволяя определять на 20 % больше опасных переходов, чем в ранее предложенных работах.

Литература

1. Denning, D. E. An intrusion-detection model [Text] / D. E. Denning // In Proc. IEEE Symposium on Security and Privacy. — 1986. — P. 118–131. doi:10.1109/sp.1986.10010
2. Sheyner, O. Scenario Graphs and Attack Graphs [Text]: PhD thesis / O. Sheyner. — SCS, Carnegie Mellon University, 2004. — 141 p.
3. Kvarnström, H. A survey of commercial tools for intrusion detection [Text]: Technical Report / H. Kvarnström. — Chalmers University, 1999. — 99 p.
4. Edward, G. Intrusion Detection: An Introduction to Internet Surveillance, Correlation, Trace Back, Traps, and Response [Text] / G. Edward. — Sparta, New Jersey, USA: Intrusion Net Books, 1999. — 224 p.
5. Eckmann, S. T. STATL: An Attack Language for State-based Intrusion Detection [Text] / S. T. Eckmann, G. Vigna, R. A. Kemmerer; Dept. of Computer Science. — Santa Barbara: University of California, 2000. — P. 71–103.
6. Mizutani, M. The design and implementation of session-based IDS [Text] / M. Mizutani, S. Shirahata, M. Minami, J. Murai // Electronics and Communications in Japan (Part I: Communications). — 2006. — Vol. 89, № 3. — P. 46–58. doi:10.1002/ecja.20251
7. Vigna, G. NetSTAT: a network-based intrusion detection approach [Text] / G. Vigna, R. A. Kemmerer // Proceedings 14th Annual Computer Security Applications Conference (Cat. No.98EX217). — Institute of Electrical & Electronics Engineers (IEEE), 1998. — P. 25–34. doi:10.1109/csac.1998.738566
8. Gorodetski, V. Attacks against Computer Network: Formal Grammar-Based Framework and Simulation Tool [Text] / V. Gorodetski, I. Kotenko // Lecture Notes in Computer Science. — Springer Science + Business Media, 2002. — P. 219–238. doi:10.1007/3-540-36084-0_12
9. Гамаюнов, Д. Ю. Модель поведения сетевых объектов в распределенных вычислительных системах [Текст] / Д. Ю. Гамаюнов, Р. Л. Смелянский // Программирование. — 2007. — № 4. — С. 20–31.
10. Lee, W. Data mining approaches for intrusion detection [Text] / W. Lee, S. Stolfo // In Proc. of the 7th USENIX Security Symposium. — 1998. — P. 79–94.

ВИЯВЛЕННЯ КОМП'ЮТЕРНИХ АТАК ЗА ДОПОМОГОЮ МОНІТОРИНГУ МЕРЕЖЕВИХ ОБ'ЄКТІВ

Представлено аналіз результатів виявлення комп'ютерних атак на основі аналізу моніторингу мережевих об'єктів. Визначено похибки в розрахунках ймовірності формули атак і внесені коректування, які значно покращують показники продуктивності, отримані раніше. Розроблено модель виявлення атак на основі інформації про поведінку об'єктів мережі та їх взаємодію.

Ключові слова: атака, комп'ютерна система, мережеві об'єкти, вторгнення, інформаційна система, стан об'єкта.

Балакин Сергей Вячеславович, *аспирант, кафедра компьютерных систем и сетей, Национальный авиационный университет, Киев, Украина,* ***e-mail: desertq@yandex.ru****.*

Балакін Сергій В'ячеславович, *аспірант, кафедра комп'ютерних систем і мереж, Національний авіаційний університет, Київ, Україна.*

Balakin Sergii, *National Aviation University, Kyiv, Ukraine,* ***e-mail: desertq@yandex.ru***