УДК 004.652.4

05.00.00 Технические науки

ДИАГНОСТИКА АНОМАЛИЙ В СЕТЯХ ПЕРЕДАЧИ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ РАЗНООБРАЗИЙ ИНФОРМАЦИОННОГО ОБМЕНА

Кучер Виктор Алексеевич
к.т.н

Магомадов Алексей Сайпудинович
д.т.н.

Чигликова Надежда Дмитриевна
к.т.н.

Степанов Давид Игоревич
студент-магистр
Кубанский государственный технологический университет, Краснодар, Россия

Работа посвящена поиску эффективных методов выявления аномальных состояний в работе сетей передачи данных. Представлена структура современной системы обнаружения информационных атак. Приведен краткий обзор и анализ средств сетевой безопасности информационных систем. Описаны две основные технологии обнаружения атак: обнаружение аномалий и обнаружение злоупотреблений. Показано, что обнаружение аномалий основано на предположении, что любое аномальное поведение есть отклонение от профиля нормального поведения. Эта технология трудно реализуема на практике, хотя в последнее время наметился некоторый прогресс при использовании для этих целей экспертных систем, нечеткой логики и т.д. В методе обнаружения злоупотреблений в качестве сигнатуры атак используются шаблоны действий или набор символов, характеризующих аномальную деятельность. Для решения проблемы авторы предлагают использовать комплексно достоинства обоих методов

Ключевые слова: ИНФОРМАЦИОННЫЕ СИСТЕМЫ, СИСТЕМЫ БЕЗОПАСНОСТИ, ОБНАРУЖЕНИЕ АНОМАЛИЙ И ЗЛОУПОТРЕБЛЕНИЙ

UDC 004.652.4

Technical sciences

DIAGNOSTIC OF ANOMALIES IN DATA-PROCESSING NETWORKS WITH USE OF VARIETY OF INFORMATION EXCHANGE

Kucher Viktor Alekseevich
Cand.Tech.Sci.

Magomadov Aleksej Saipudinovich
Dr.Sci.Tech.

Chiglikova Nadezhda Dmitrievna
Cand.Tech.Sci.

Stepanov David Igorevich
master student
Kuban State Technological University, Krasnodar, Russia

The work is devoted to searching efficient detection methods of anomalous state in data networks. There is a structure of modern informational attacks detecting system. There are short review and analysis of information system network security facilities. Two main technologies of attack detection are described: anomaly detection and misuse detection. It is shown that every detection of anomalies is based on assumption that anomalous behavior is deflection from normal profile of behavior. It is hard to implement this technology, although there is some progress when expert system, fuzzy logic and so on are used for this purpose. Action patterns or symbols assets which describe anomaly activity are used as attack signature in misuse detection method. Author offers to use benefits of both methods for solving the problem

Keywords: INFORMATION SYSTEMS, SECURITY SYSTEMS, ANOMALY AND MISUSE DETECTION

Поиск эффективных методов выявления аномальных состояний в работе сетей передачи данных (СПД) в настоящее время остается актуальной научной задачей. Подобные нарушения являются следствием программных сбоев, отказов аппаратуры или нарушений информационной защиты. Из всего множества возможных сетевых аномалий (СА)

рассмотрим только аномалии, связанные с нарушениями политики безопасности СПД за счет сетевых вторжений (атак).

Отметим также, что до сих пор отсутствуют математические основы технологии детектирования сетевых вторжений (атак). Все существующие методы основаны в первую очередь на различных предпочтениях разработчиков информационных систем (ИС) и средств сетевой безопасности. Под разработанные средства и механизмы пока не подведен научный базис, что не позволяет подтвердить или опровергнуть эффективность предполагаемых решений. Сейчас наметились изменения в лучшую сторону в этой области, но до окончательного завершения работ еще далеко.

Предлагаемая статья посвящена попытке описать основные методы, которые используются для диагностики сетевых атак, и предложить комплексный подход к решению этой проблемы.

Способы обнаружения атак, применяемые в современных системах обнаружения атак (IDS – Instruction Detection System), основаны на нескольких общих методах. Следует отметить, что эти методы не являются взаимоисключающими. Структура современной системы обнаружения атак представлена на рис. 1. Конкретная реализация той или иной системы может отличаться от приведённой схемы, но, в общем, каждая система состоит из следующих модулей:

- модуль слежения – предназначен для сбора данных для анализа (сетевой трафик, записи из журналов событий и т.д.) и их приведения к одному общему виду;
- подсистема обнаружения атак – осуществляет анализ полученных данных от модуля слежения;
- подсистема реагирования – осуществляет реагирование на распознанные атаки;

- хранилище данных – содержит информацию необходимую для работы системы, а также информацию об обнаруженных атаках;
- подсистема управления – с её помощью осуществляется управление всеми модулями системы;
- графический интерфейс.

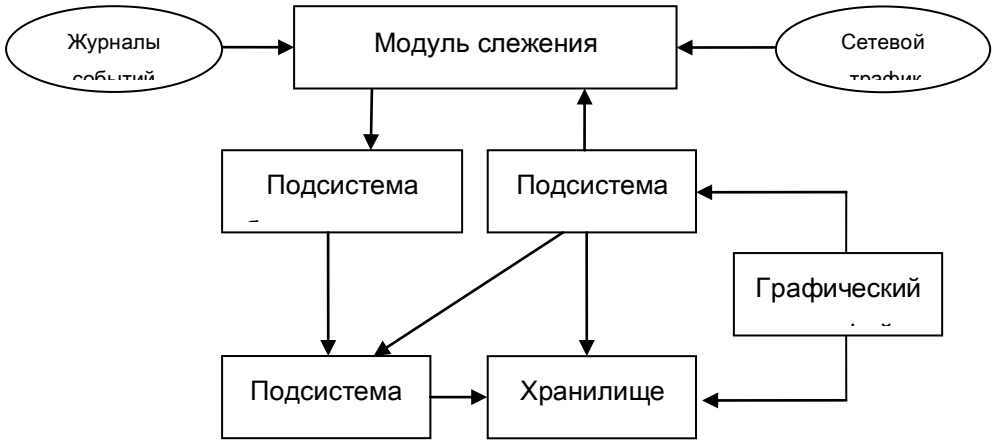

Рисунок 1 – Структурная схема современной системы обнаружения

В настоящее время технологии обнаружения атак принято делить на две категории [1-4]: обнаружение аномалий и обнаружение злоупотреблений.

Обнаружение аномалий основано на предположении, что любое аномальное поведение есть отклонение от профиля нормального поведения. Эта технология, как правило, включает в себя создание базы данных, которая содержит профили контролируемой деятельности. Для этих целей используются статистические методы (аппарат математической статистики). В случае однозначного описания профиля нормального поведения пользователя, любое отклонение от него можно идентифицировать как аномальное. К сожалению, это не всегда так. При использовании систем на основе аномального поведения возможны два крайних случая:

- ложное срабатывание, т.е. отнесение нормального поведения к аномальному;
- пропуск атаки, т.е. случай, когда аномальное поведение не может быть однозначно идентифицировано.

При настройке и эксплуатации систем данной категории администраторы вычислительных сетей сталкиваются со следующими проблемами:

- создание профилей нормального поведения является трудоёмкой задачей;
- необходимо определение граничных значений характеристик поведения пользователей для снижения вероятности появления одного из двух вышеназванных крайних случаев.

Представленная технология обнаружения сетевых аномалий в наше время не получила широкого распространения и не используется ни в одной из коммерчески распространяемой IDS. Связано это с тем, что данная технология трудно реализуема на практике. Но в последнее время наметился некоторый прогресс, и появились первые публикации о возможность использовании для этих целей экспертных систем, нечеткой логики, генетических алгоритмов и нейронных сетей [2-4].

Метод обнаружения злоупотреблений заключается в описании атаки в виде сигнатуры и поиске её в контролируемом пространстве (в сетевом трафике или журнале событий). В качестве сигнатуры атаки может выступать шаблон действий или набор символов, характеризующих аномальную деятельность. Сигнатуры могут строиться исходя из анализа данных по следующим направлениям:

- повтор определённых событий – этот механизм основан на предпосылки, согласно которой следует, что если нарушитель не знает, как точно получить доступ к какому-либо ресурсу, то он будет это делать во

второй, третий и т.д. раз. Например, сканирование портов, зафиксированное межсетевым экраном (МЭ) Cisco PIX Firewall представлено на рис. 2;

- неправильные или несоответствующие текущей ситуации команды – в случае если при информационном обмене выявляется несоответствие заранее ожидаемым реакциям, то можно сделать вывод, что один из участников подменён, т.е. является злоумышленником;
- использование уязвимостей – в программном или аппаратном обеспечении компонентов сети содержаться неумышленные ошибки, как правило, заложенные на этапе проектирования или создания, которые могут в определённых случаях дать злоумышленнику несанкционированный доступ;
- несоответствующие параметры сетевого трафика – например большой объём входящего или исходящего трафика, нестандартные комбинации флагов и т.д.;
- непредвиденные атрибуты.

```
…Teardown TCP connection 828470317 for ouside:162.63.10.219/445 to
inside:192.168.0.228/2034 duration 0:00:31 bytes 0 TCP Reset-O

…Teardown TCP connection 828470318 for ouside:162.63.10.220/445 to
inside:192.168.0.228/2035 duration 0:00:31 bytes 0 TCP Reset-O

…Teardown TCP connection 828470319 for ouside:162.63.10.221/445 to
inside:192.168.0.228/2036 duration 0:00:31 bytes 0 TCP Reset-O

…Teardown TCP connection 828470320 for ouside:162.63.10.222/445 to
inside:192.168.0.228/2037 duration 0:00:31 bytes 0 TCP Reset-O
```

Рисунок 2 – Сканирование портов, зафиксированное журналом событий МЭ Cisco PIX

По принципу реализации данного метода IDS можно разделить на:

- обнаружение атак на уровне сети;
- обнаружение атак на уровне хоста.

На рисунке 3 показана сеть Петри, описывающая сигнатуру атаки, которая выполняет подбор пароля для получения несанкционированного доступа к ресурсам системы. Каждый переход системы в новое состояние в

этой сети Петри связан с вводом пароля. Если пользователь в течении 1 минуты четыре раза подряд ввёл пароль неправильно, то метод зафиксирует факт осуществления атаки.

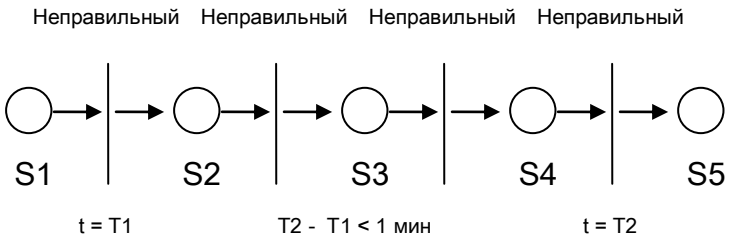

Рисунок 3 – Сеть Петри, описывающая сигнатуру атаки, осуществляющей

Основные преимущества статистического подхода – это использование аппарата математической статистики и адаптация к поведению объекта. В качестве объектов исследования анализируемой системы берутся отдельные сетевые устройства, характеристики трафика которых являются случайными величинами, изменяющимися во времени и определяющими работу сетевых устройств по сетевым протоколам (например, TCP, UDP, ICMP). Характеристиками объектов выступают такие величины как: число IP-адресов, с которыми были взаимодействия, объемы переданного/полученного трафика/пакетов, число клиентских/серверных портов и др. Метод основан на следующих утверждениях:

- статистические оценки характеристик имеют постоянный характер;
- резкое отклонение значений дисперсии и математического ожидания является указанием на аномалию.

В соответствии с этим, должны быть реализованы следующие этапы:

- выбор анализируемых характеристик трафика, которые в дальнейшем будут выступать в качестве значений соответствующего признака генеральной совокупности;
- определение законов распределения отдельных характеристик, для этого можно воспользоваться критерием согласия Пирсона [5]:

$$\chi^2 = \sum_{i=1}^{k}((n_i - n_i^{|})^2 / n_i^{|});$$

- оценка математического ожидания, дисперсии и среднеквадратического отклонения для отдельных характеристик трафика устройств за различные интервалы времени – для этого используются формулы, зависящие от вида распределения, в состав которых входит значение выборочной средней:

$$\overline{\chi}_B = \sum_{i=1}^{k} n_i x_i / n.$$

Однако при использовании данной методики возникают проблемы:

- статистические системы не чувствительны к порядку следования событий: одни и те же события, но в разной последовательности, могут характеризовать аномальную и нормальную деятельность;
- очень трудно задать пороговые значения отслеживаемых системой характеристик, чтобы адекватно идентифицировать аномальную деятельность;
- статистические системы могут быть с течением времени «обучены» нарушителями так, чтобы атакующие действия рассматривались как нормальные.

Методы, базирующиеся на экспертных системах (ЭС), позволяют описывать модели атак на естественном языке с высоким уровнем абстракции. ЭС состоит из набора фактов и правил, которые охватывают знания специалистов-экспертов в области сетевой безопасности. Факты

представляют собой исходные данные о работе информационных систем, а правила – алгоритмы логических решений о факте атаки на основе поступившего набора фактов. База знаний ЭС должна содержать сценарии большинства известных атак. Для этого она должна постоянно обновляться. Основным недостатков в использовании ЭС для обнаружения атак является невозможность идентифицировать неизвестную атаку, которая ещё не записана в базе знаний. При этом даже небольшое изменение известной атаки может стать серьёзным препятствием для функционирования системы.

В последнее время для поиска аномалий начинают использоваться методы, основанные на биологических моделях. Для их описания могут использоваться генетические и нейросетевые алгоритмы. Первые предназначены для поиска оптимального решения на основе механизма естественного отбора в популяции. Популяция атак (как и в биологическом мире) представляется как множество хромосом, каждая из которых моделируется битовой строкой. Популяция развивается на основе трёх генетических операций – скрещивания, селекции и мутации, и её развитие продолжается до тех пор, пока не будет достигнут заданный критерий оптимальности. При использовании генетических алгоритмов для выявления атак в качестве хромосом популяции выступают векторы определённой длины, каждый элемент которых соответствует определённой атаке. В результате развития такой популяции можно получить оптимальный вектор, который будет указывать, какие атаки происходят в системе в текущий момент.

Нейросетевой метод основан на создании сети взаимосвязанных друг с другом искусственных нейронов, каждый из которых представляет собой пороговый сумматор атак. После создания нейросеть проходит период обучения, в течении которого она учится распознавать определённые типы атак: на её вход подаются данные, указывающие на определённую атаку,

после чего параметры нейросети настраиваются таким образом, чтобы на выходе она смогла определить тип этой атаки. Использование нейросетей имеет ряд недостатков. Первая причина связана с требованиями к обучению нейросети: порядок обучения требует большого количества данных с тем, чтобы убедиться, что результаты являются статистически значимыми. Другая причина связана с проблемой «черного ящика».

Но ни одна из систем не даёт 100% защищённости. Чем эта защищенность выше, тем более разнообразные методы используются для обнаружения сетевых атак и аномального сетевого трафика. На рис. 4 представлена структура модифицированной системы обнаружения атак. Основное её отличие заключается в подсистеме обнаружения, в которой используется сразу несколько различных методов. Данные, получаемые от модуля слежения, сначала анализируются с помощью одного метода, затем с помощью другого и т.д., тем самым достигается большая точность в обнаружении злоумышленных или аномальных действий, снижается количество ложных срабатываний. На представленной схеме показаны только три модуля в подсистеме обнаружения атак, конечно, их может быть больше и используемые методы обнаружения могут отличаться от предложенных.

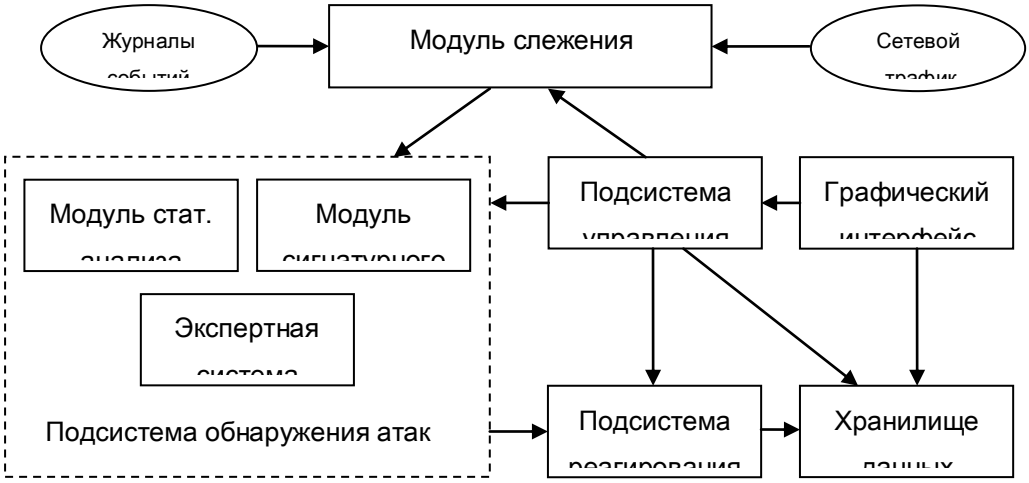

Рисунок 4 – Структурная схема модифицированной системы обнаружения атак

Только комплексный подход к данной проблеме может значительно снизить риск вторжения в ИС предприятий и организаций и исключить наносимый им ущерб.

Литература

1. Милославская Н.Г., Толстой А.И. Интрасети: обнаружение вторжений. – М.: ЮНИТИ-ДАНА, 2001. – 588 с.

2. Норткат С., Новак Д. Обнаружение нарушений безопасности в сетях, 3-е издание.: Пер. с англ. – М.: издательский дом «Вильямс», 2003. – 448 с.

3. Лукацкий А.В. обнаружение атак. – СПб.: БХВ-Петербург, 2001. – 624 с.

4. Соколов А.В., Шаньгин В.Ф. Защита информации в распределённых корпоративных сетях и системах. – М.: ДМК Пресс, 2002. – 656 с.

5. Гмурман В.Е. Теория вероятностей и математическая статистика. Учеб. пособие для вузов. – Изд. 7-е, стер. – М.: Высшая школа, 2001. – 480 с.

References

1. Miloslavskaja N.G., Tolstoj A.I. Intraseti: obnaruzhenie vtorzhenij. – M.: JuNITI-DANA, 2001. – 588 s.

2. Nortkat S., Novak D. Obnaruzhenie narushenij bezopasnosti v setjah, 3-e izdanie.: Per. s angl. – M.: izdatel'skij dom «Vil'jams», 2003. – 448 s.

3. Lukackij A.V. obnaruzhenie atak. – SPb.: BHV-Peterburg, 2001. – 624 s.

4. Sokolov A.V., Shan'gin V.F. Zashhita informacii v raspredeljonnyh korporativnyh setjah i sistemah. – M.: DMK Press, 2002. – 656 s.

5. Gmurman V.E. Teorija verojatnostej i matematicheskaja statistika. Ucheb. posobie dlja vuzov. – Izd. 7-e, ster. – M.: Vysshaja shkola, 2001. – 480 s.