Эссе по курсу «Защита информации»,
кафедра радиотехники, Московский физико-технический институт (ГУ МФТИ),
http://www.re.mipt.ru/infsec

Обнаружение атак в локальной сети по анализу их сигнатур.

Выполнил:

Студент: *Кондрашин Александр Александрович*
Группа: *212*

23.03.2006 г.

0. Введение.

В настоящее время особую роль в нормальном функционировании организации и благополучии конкретных людей играет информационная безопасность. За последнее время мы можем наблюдать множество случаев атак на информационные ресурсы как со стороны внешних субъектов, так и со стороны авторизованных пользователей, злоупотребляющих своим служебным положением.

Обеспечение защищенности информации , обрабатываемой вычислительными комплексами или автоматизированными системами, от внешних и внутренних угроз базируется на организационно-правовых нормах и на обеспечении компьютерной безопасности.

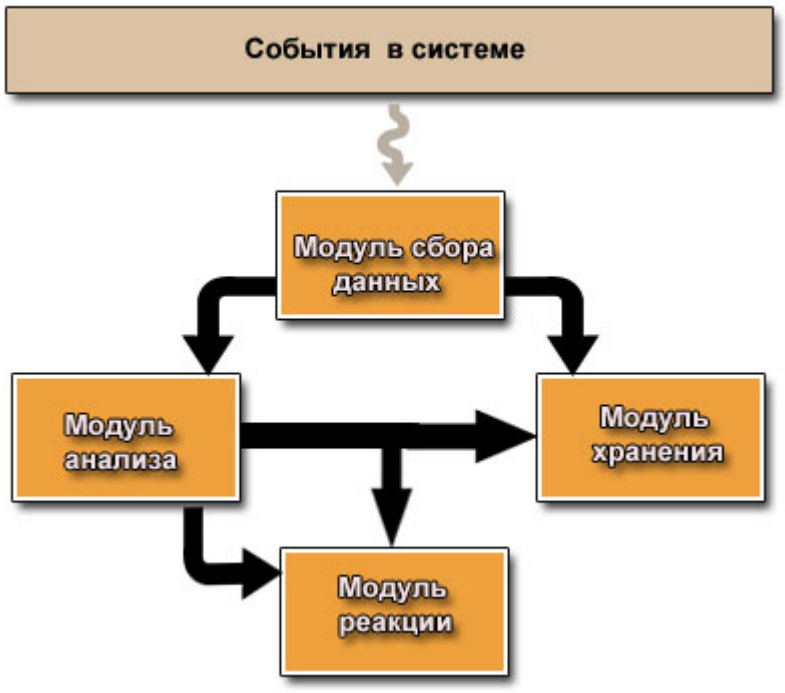
Системы обнаружения атак призваны защитить с определенной степенью надежности организации и физические лица от потерь, связанных с несанкционированным доступом.

1. Структура системы обнаружения вторжения.

Системы обнаружения вторжений (СОВ) решают задачи по оперативному приему и отражению атак. СОВ собирает информацию о ряде сетевых ресурсов и систем. Затем, анализируя данные на предмет наличия признаков вторжения, позволяет принять ответные меры в случае обнаружения атаки.

Функционирование системы обнаружения вторжений можно разделить на четыре структурных модуля:

- модуль сбора данных;
- модуль анализа;
- модуль хранения;
- модуль реакции;



Системы обнаружения атак выполняют следующие функции:

- контроль и анализ активности пользователей и вычислительных систем;
- аудит конфигураций системы и уязвимостей;
- тестирование на предмет целостности системных файлов и файлов данных, имеющих наибольшую важность;
- распознавание характера активности, соответствующего уже известным атакам;
- обнаружение характерных последовательностей аномалий;
- распознавание деятельности пользователей, нарушающей политику безопасности;

Анализируя собранные данные о событиях в системе, СОВ может принять решение об ответной реакции либо сохранить (в модуле хранения) данные для последующего их дополнения и дальнейшего анализа.

2. Модуль анализа. Сигнатурный метод.

Модуль анализа представляет собой по существу систему распознавания и является самым важным в любой системе обнаружения. Этот модуль определяется алгоритмом, позволяющим выявить факт атаки или вторжения.

Существуют несколько методов анализа. К основным относят сигнатурный метод, метод выявления аномального поведения, к «экзотическим» - метод, основанный на использовании искусственного интеллекта.

В рамках темы настоящего эссе, мы остановимся подробно на сигнатурном методе обнаружения вторжений.

2.1. Общие требования к методу анализа.

В общем случае выбранный метод анализа должен отвечать основным требованиям системы, использующей технику выявления атак. К числу таких требований относят:

- *общность* – система должна быть универсальной и способной к обнаружению всех типов известных и неизвестных атак;
- *эффективность* – система должна быть высокопроизводительной;
- *работа в реальном времени* – система должна функционировать постоянно и оперативно решать поставленные задачи;
- *переносимость* – система должна использовать стандартные форматы сигнатур;
- *масштабируемость* – необходима возможность пополнения базы сигнатур, не приводящая к трудностям в процессе работы;
- *ресурсоемкость* – система не должна использовать неразумное количество ресурсов для обеспечения эффективного функционирования.

2.2.Реализация метода сигнатур. Принципы работы.

Рассмотрим принципы, на которых основывается сигнатурный анализ. Базовым в этом методе является тот факт, что большинство атак на системы развиваются по похожим сценариям и на данный момент уже известны, т.е. известны характерные особенности и взаимосвязь событий, приводящих к попыткам атак.

В наиболее простом случае метод, основанный на анализе сигнатур, реализуется следующим образом:

- Поддерживается база данных сигнатур для известных атак с возможностью пополнения без потерь в производительности.
- В результате анализа происходит сопоставление регистрируемой последовательности событий известным сигнатурам атак.
- В случае соответствия выдается сигнал о попытке вторжения. Дальнейшие действия определяются алгоритмами модуля реакции: могут быть предприняты ответные меры, а можно ограничиться просто оповещением.

Рассмотрим принцип сигнатурного анализа на следующем примере. Пусть поток входных данных (событий) имеет вид:

ABCDDABACCBC.

Пусть теперь распознавание происходит относительно сигнатуры:

ADAC.

Тогда, в случае работы алгоритма по правилам дискретной аппроксимации получим:

AxxDxAxxCxxx

x – обозначает отсутствие символа, образующего сигнатуру в потоке исходных данных. Т.е. атака распознана.

Стоит отметить, что в случае использования правила «немедленного следования» распознавания бы не произошло. Но такой способ распознавания малоэффективен, т.к. регистрируемые данные (события) , относящиеся к атаке часто зашумлены из-за возможных вариаций действий нарушителя.

Такой же алгоритм, но работающий согласно правилам дискретной аппроксимации, позволяет более эффективно решать поставленные задачи распознавания. За это приходится заплатить ресурсами, т.к. требуется поддержание большого объема «частично распознанных» сигнатур атак.

Время распознавания сигнатур оценивают как O(mn),

где m – размер входных данных, а n – размер сигнатуры.

2.3.Основные характеристики сигнатур.

Выделяют следующие основные характеристики сигнатур:

- *Линейность событий* – события, составляющие сигнатуру, должны представлять собой строго определенную последовательность без операций выбора, объединения, повторений т.д.
- *Унификация событий* – свойство сигнатуры описывать события, используя переменные. Например, событие, заключающееся том, что происходят события A,B, потом любое событие, потом C,D можно записать сигнатурой: ABXCD, где X – событие, описываемое переменной X, любое.

- *Упорядоченность событий* – характеризует время появления входящего в сигнатуру события относительно предыдущих событий. Позволяет наложить ограничения на время распознавания сигнатуры.
- *Начало распознавания* – показывает абсолютное время начала распознавания сигнатуры.
- *Длительность распознавания* – накладывает ограничения на время появления события в сигнатуре.
- *Динамический ввод данных* – входные данные генерируются динамически, т.е. являются неизвестными до начала распознавания. Диктуется необходимостью функционирования в режиме реального времени.
- *Динамика сигнатуры* – определяет возможность динамического (т.е. прямо в процессе распознавания) добавления или удаления сигнатур.

2.4.Основные алгоритмы поиска сигнатур атак.

На сегодняшний день существуют несколько наиболее продуктивных алгоритмов поиска сигнатур атак. Это следующие алгоритмы:

- *Существование* – распознавание факта является основанием для регистрирования попытки атаки.
- *Последовательность* – распознавание строго определенной последовательности событий достаточно для обнаружения атаки.
- *Частичный порядок* – поводом для сигнализации атаки служит распознавание сигнатуры, состоящей из частично упорядоченных событий.
- *Интервал времени* – учитываются временные соотношения между событиями.
- *Период* – учитываются непосредственно моменты времени, в которые происходят события.

В настоящее время для реализации сигнатурного метода используют в основном первые два способа.

3. Заключение

На основании краткого обзора технологии сигнатурного метода анализа можно сделать выводы о главных достоинствах и недостатках этого метода.

3.1. Достоинства метода сигнатурного анализа.

- Количество и тип событий которые необходимо подвергать тестированию ограничиваются определенными в сигнатурах данным.

- Метод является более быстрым и эффективным, т.к. не предполагает вычислений с плавающей точкой (по крайней мере, над большими объемами данных)

3.1. Недостатки метода сигнатурного анализа.

- Размер базы данных сигнатур существенно влияет на масштабируемость и производительность метода.
- Трудности с обновлением баз данных, вызванные отсутствием общепринятого языка описания.
- При обнаружении нового типа атак необходимо обновлении базы данных, следовательно период обновления должен быть небольшой.

4. Используемая литература.

1) Корт С.С. «Теоретические основы защиты информации.» – М.: Гелиос-АРВ, 2004 (печатное издание)
2) Ребекка Бейс(Rebecca Base), ICSA .перевод Алексея Лукацкого, Юрия Цаплева, «Введение в обнаружение атак и анализ защищенности» http://bugtraq.ru/library/books/icsa/
3) А.В.Лукацкий «Обнаружение атак своими силами» http://bugtraq.ru/library/security/luka/autodetect.html
4) Корт С.С. «Методы выявления нарушений безопасности» http://www.kiev-security.org.ua/box/12/113.shtml