УДК 65.012.45

В.П. Пасько, В.И. Приймак

ИССЛЕДОВАНИЕ ПОДСИСТЕМЫ ВЫЯВЛЕНИЯ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В КОРПОРАТИВНУЮ СЕТЬ

Введение

Развитие современных информационных технологий в организации ведет к тому, что происходит постепенный переход к объединению автономных компьютеров и локальных сетей филиалов и отделений компании в единую корпоративную сеть. Помимо явных преимуществ, такой переход несет с собой и ряд специфичных проблем, с которыми уже не справляются в полной мере ставшие традиционными средства обеспечения безопасности корпоративных сетей (межсетевые экраны, системы контроля локального доступа, сервера и системы аутентификации, антивирусное программное обеспечение, шифрование данных).

Как реакция на возникновение этих проблем в последнее время активно развиваются новые подходы в обеспечении безопасности корпоративных сетей. Одним из важнейших элементов систем информационной безопасности сетей любого современного предприятия становятся системы обнаружения компьютерных атак (IDS - Intrusion Detection Systems) . И хотя рынок этих систем начал бурно развиваться ещё в 1997 году, следует отметить, что современные системы обнаружения атак ещё далеки от совершенства. Зачастую они не только не могут быть адаптированы к конкретной информационной среде предприятия (имеют жёсткую специализацию, ограничения по возможности применения, не могут быть интегрированы в подобную HP OpenView комплексную систему для мониторинга состояния сети и управления ею, неспособны в автоматическом режиме реагировать на обнаруженные атаки), но и не могут обнаружить неизвестные атаки, в том числе известные им атаки, реализованные с небольшими отклонениями от шаблона.

К сожалению, на рынке информационных технологий сейчас не существует ни одного продукта, который бы соединял в себе перечисленные выше функциональные возможности.

Постановка задачи

Задачей данной работы является разработка методики построения комплексного программного обеспечения для обнаружения несанкционированного доступа, его интеграцию в корпоративную сеть и его исследование. Основными требованиями к исследуемой концепции программное обеспечение являются:

- высокая степень интеграции программных подсистем информационной системы;

 ISSN 1562-9945

- модульность структуры IDS для обеспечения возможности её интеграции в корпоративную информационную инфраструктуру посредством подключения интерфейсных модулей взаимодействия;
- легкость управления системой защиты;
- возможность автоматического обновления сигнатур атак и злоупотреблений;
- эффективность обнаружения атак и злоупотреблений (несанкционированного доступа).

Построенное на основе предлагаемой методики программное обеспечение должно обладать следующими функциями:

- выявление атак и злоупотреблений, а также своевременное противопоставление им соответствующих средств защиты;
- обеспечение в реальном времени возможности реконфигурации программного и аппаратного обеспечения сети, других способов реакции на возникновения угрозы;
- обеспечение своевременного уведомления ответственных за сетевую безопасность о возникающих проблемах;
- предоставление гибкой системы регистрации инцидентов, а также механизма для их анализа.

Задача исследования программного обеспечения заключается в определении эффективности предложенной методики путем экспериментальных исследований на имитационной модели. Цель экспериментальных исследований – определение зависимости между параметрами системы обнаружения несанкционированного доступа в корпоративную сеть (количеством агентов систем обнаружения атак, схемами размещения модулей IDS, подходами к обнаружению атак и злоупотреблений, используемыми вариантами реагирования) и эффективностью защиты.

Решение данных задач позволит сформировать техническое задание на проектирование программного обеспечения системы обнаружения несанкционированного доступа в корпоративную сеть. Такое программное обеспечение позволит повысить защиту за счет создания подхода, который позволяет контролировать, обнаруживать и реагировать в реальном режиме времени на риски безопасности.

Актуальность решения поставленных задач заключается в том, что на сегодняшний день отсутствует единое готовое решение, которое бы удовлетворяло всем требованиям, предъявляемым к системам обнаружения несанкционированного доступа. Абсолютное большинство таких систем можно эффективно применять для решения узкого круга задач, они базируются на использовании только одной из возможных технологий, что, в свою очередь, не даёт возможности этой системе обнаруживать все возможные виды атак.

Выбор принципов реализации проектируемой IDS

На данный момент существует два подхода к построению архитектуры IDS [1]: размещение модулей слежения (сенсоров, датчиков, детекторов) – программ, занимающихся сбором данных, – на одном узле с управляющими модулями (консолями, менеджерами) или их распределённое размещение на нескольких узлах.

Также системы обнаружения несанкционированного доступа можно классифицировать и по источнику данных [2]:

- на базе сетевого сегмента (network-based) – системы, анализирующие сетевой трафик с целью поиска признаков атак;
- на базе узла (host-based) – системы, ориентированные на защиту отдельного узла, входными данными для которых могут быть журналы регистрации, действия пользователей защищаемого узла:
  - системы, обнаруживающие атаки на операционные системы;
  - системы, обнаруживающие атаки на СУБД;
  - системы, обнаруживающие атаки на приложения.

В рабочем режиме IDS анализирует собранную информацию и делает заключение о том, произошла атака, или нет. При этом обычно используется одна из двух технологий [3]:

- обнаружение аномалий – обычно реализуется средствами статистического анализа;
- обнаружение злоупотреблений (экспертный, сигнатурный метод) – основывается на анализе сигнатур атак и злоупотреблений.

В первом случае известно поведение контролируемого объекта и любое поведение считается атакой, во втором случае известным считается перечень атак используемых при обнаружении атак и злоупотреблений, – статистический и сигнатурный.

В проектируемой системе обнаружения несанкционированного доступа были предложены нижеизложенные принципы реализации.

Предлагается использовать трёхуровневую архитектуру схемы управления сенсорами системы обнаружения атак. В данном случае сенсор посылает информацию об атаках не на консоль администратора, а на специальный сервер управления, к которому и подключается администратор безопасности. Такой подход даёт возможность хранить всё сведения о политиках безопасности, загружаемые на сенсоры, и события, ими зафиксированные, используя средства СУБД на сервере управления (с функциями резервирования).

Поскольку network-based IDS и host-based IDS [2] являются скорей дополняющими друг друга технологиями реализации IDS (т.к. эффективно обнаруживают различные типы атак), чем конкурирующими, то целесообразным было бы их совместное применение в рамках комплексной системы обнаружения несанкционированного доступа. Однако

 ISSN 1562-9945

такой подход помимо дополнительных затрат, связанных с приобретением устройств, используемых для реализации сетевых IDS, накладывает также и некоторые другие ограничения:

- неприменимость в сетях, использующих шифрование данных;
- неэффективность работы в коммутируемой среде;
- зависимость от конкретных сетевых протоколов передачи данных;
- невозможность работы в высокоскоростном сегменте сети (например Gigabit Ethernet) ввиду необходимости обработки данных от десятков, а то и от сотен узлов;
- отсутствие больших ресурсов для хранения сагрегированной информации (журналов регистраций);
- возникновение сложностей с сокрытием от злоумышленников устройства, на котором установлен агент network-based IDS, т.к. оно имеет свой IP-адрес.

Поэтому для реализации проектируемой IDS был предложен подход, совмещающей в себе обе эти технологии, при котором на каждый контролируемый узел устанавливался бы агент системы обнаружения атак и отслеживал не только атаки на прикладном уровне (ОС, приложений и СУБД), но и сетевые атаки, направленные на данный узел. Этот подход (гибридная система обнаружения несанкционированного доступа – hybrid IDS) нивелирует все вышеизложенные проблемы и может быть реализован в критических узлах сети.

Как показали исследования, наиболее эффективным для выявления несанкционированного доступа есть комбинированное использование сразу двух технологий обнаружения атак: как обнаружения аномалий, так и злоупотреблений, что и продемонстрировано на рис. 1.

Однако здесь в качестве альтернативы компонентам статистического анализа модуля обнаружения аномальной активности (рис. 1) целесообразно использовать искусственные нейронные сети. Для реализации проектируемой системы была предложена архитектура нейронной сети, представляющая самоорганизующуюся карту (“сеть Кохонена”), которая использует один слой нейронов для представления сведений от отдельного домена в форме геометрически организованной карты.

В модуле сигнатурного обнаружения атак (рис. 1) для организации быстрого поиска по шаблонам (сигнатурам атак и злоупотреблений) предлагается использовать алгоритм Бойера-Мура.

Заключение

Результаты исследования принципов построения эффективной системы обнаружения несанкционированного доступа и влияния на ее эффективность различных параметров и информационного окружения дают основание сделать следующие выводы:

1) Существенное влияние на качество системы адаптивной защиты информации в корпоративных сетях оказывает конфигурация системы.

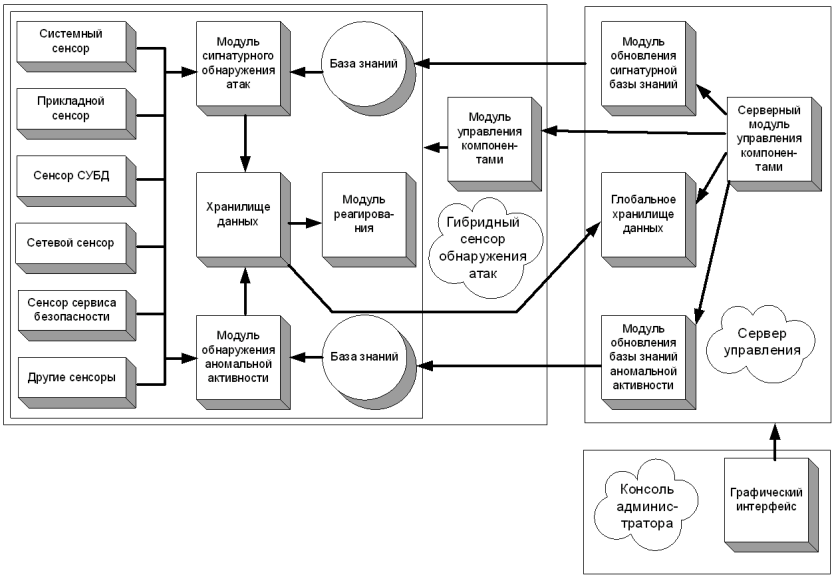

Рис. 1 – Схема спроектированной системы обнаружения атак

Использование распределенной структуры системы позволяет увеличить отказоустойчивость системы, а также степень обнаружения рисков безопасности. Сильное влияние на отказоустойчивость и пропускную способность системы оказывает способ размещения модулей обработки данных и реагирования. Расположение вышеперечисленных модулей на агентах повышается отказоустойчивость, так как в случае выходя из строя сервера управления или канала связи между сервером управления и агентом, функция последнего никак не нарушится. В этом случае агент продолжает работать в автономном режиме, по-прежнему обнаруживая риски безопасности и реагируя на них.

2) Наилучшие показатели степени обнаружения атак достигаются при использовании комплексного подхода к выявлению злоупотреблений, хотя при этом незначительно ухудшается по сравнению с сигнатурным и статистическими подходами пропускная способность системы.

3) Количество агентов системы влияет на степень обнаружения рисков, а также повышает общую отказоустойчивость системы. Поэтому желательно устанавливать агентов на все критические узлы информационной системы.

4) Вид сетевых пакетов, передаваемых через систему, не влияет на параметры качества ее функционирования. Это касается прикладных протоколов основанных на одном транспортном протоколе.

5) Интенсивность сетевых запросов к ресурсам не влияет на интенсивность отказов системы. На пропускную способность системы адаптивной

защиты информации этот параметр оказывает прямое влияние. Увеличение интенсивности запросов приводит к увеличению пропускной способности, что объясняется наличием на системе свободных вычислительных ресурсов. При дальнейшем увеличении интенсивности запросов происходит насыщение параметра пропускной способности, то есть достигается граничная пропускная способность системы.

6) С ростом интенсивности отказов агентов общая интенсивность отказов заметно возрастает. Пропускная способность при этом падает за счет появления пауз в работе системы. Очевидно, что в реальной системе интенсивность аппаратных и программных отказов должна быть минимальной.

Литература

1. Лукацкий А.В. Новые подходы к обеспечению информационной безопасности сети. НИП “Информзащита” - 2000. - http://www.infosec.ru/press/pub/p57.htm
2. Лукацкий А.В. Обнаружение атак. – 2-е изд., - СПб.: БХВ-Петербург, 2003. – 215-218с.
3. Домарев В.В. Защита информации и безопасность компьютерных систем. – К.: ДиаСофт, 1999. – 480 с.