Содержание:

Введение

Системы выявления признаков компьютерных атак и обнаружения сетевых вторжений для информационных систем уже давно применяются в качестве ключевого из необходимых рубежей обороны информационных систем. Разработчиками систем защиты информации и консультантами в этой области активно применяются такие понятия, как защита по периметру, динамическая и стационарная защита. Помимо этого, стали появляться собственные термины, такие как, например, проактивные средства защиты.

Исследования в области обнаружения атак на компьютерные системы и сети по большому счету ведутся за рубежом уже более 25 лет: исследуются признаки атак, а также эксплуатируются и разрабатываются средства и методы обнаружения попыток несанкционированного проникновения через системы межсетевой и локальной защиты — на физическом и логическом уровнях. На самом деле сюда можно отнести в том числе исследования в области побочных электромагнитных излучений и наводок, так как электромагнитный тампериг имеет свои прямые аналоги в уже ставшей обычной для рядового компьютерного пользователя сетевой среде. На российском рынке широко представлены коммерческие системы обнаружения атак и вторжений от иностранных компаний, таких как NetPatrol, ISS RealSecure, Cisco, Snort и другие, и в тоже время практически не представлены комплексные решения от разработчиков из России. Данный аспект вызван тем, что многие отечественные разработчики и исследователи реализуют системы обнаружения атак с сохранением аналогии типовых решений и архитектур уже известных систем, не стараясь особенно увеличить эффективность превентивного обнаружения атак и алгоритмов реагирования на них. Конкурентные преимущества в данном сегменте российского рынка достигаются обычно за счет существенного снижения цены и надежд на стремление покупателей к поддержке отечественного производителя.

На сегодняшний день системы обнаружения атак и вторжений обычно являются аппаратно-программными или программными решениями, которые автоматизируют процесс контроля протекающих в компьютерной сети или системе событий, а также самостоятельно анализируют данные события с целью поиска признаков

проблем безопасности. Так как количество различных способов и типов организации несанкционированных проникновений в чужие компьютерные сети за последние годы значительно увеличилось, системы обнаружения атак стали необходимым компонентом инфраструктуры безопасности большинства организаций. Этому способствует огромное количество литературы по данному вопросу, которую потенциальные злоумышленники внимательно изучают, а также все более изощренные методы и сложные подходы к обнаружению попыток взлома информационных систем.

Современные системы обнаружения вторжений имеют различную архитектуру. Классификации систем обнаружения атак следует уделить отдельное внимание, так как часто используя общепринятую классификацию систем обнаружения атак, специалисты принимают решение о том, какой из программных продуктов применить в той или иной ситуации.

На данный момент существует деление всех систем на локальные и сетевые. Локальные системы обнаружения атак размещаются на отдельных нуждающихся в защите компьютерах и анализируют различные события, такие как программные вызовы или действия пользователя. Сетевые системы обычно устанавливаются на выделенных для этих целей компьютерах для анализа трафика, циркулирующего в локальной вычислительной сети. Также различают методики обнаружения злоумышленного и аномального поведения пользователей.

Системы обнаружения аномального поведения основаны на том, что системы обнаружения атак известны некоторые признаки, которые характеризуют допустимое или правильное поведение объекта наблюдения. Под правильным или нормальным поведением понимаются действия, которые не противоречат политике безопасности и выполняются объектом. Системы обнаружения злоумышленного поведения основаны на том, что заранее известны некоторые признаки, которые характеризуют поведение злоумышленника. Экспертные системы являются наиболее распространенной реализацией технологии обнаружения злоумышленного поведения.

Целью данной работы является изучение разновидностей видов и угроз информационной безопасности и методов борьбы с ними.

Объектом исследования является понятие угроз безопасности в целом, предметом исследования – технологии обнаружения данных угроз.

В рамках исследования рассмотрены задачи:

- рассмотрение классификации сетевых атак;
- изучение методов обнаружения сетевых атак;
- классификация систем обнаружения атак;
- обзор методов реагирования на атаки.

1. Классификация сетевых атак

Эффективная защита от потенциальных сетевых атак невозможна без их детальной классификации, которая облегчает задачу противодействия им и их выявление. На сегодняшний день известно большое количество различных типов классификационных признаков. В качестве таких признаков может быть выбрано, например, разделение на активные и пассивные, внутренние и внешние атаки, неумышленные и умышленные и другие подобные классификации. К сожалению, несмотря на мало применимость на практике некоторых из существующих классификаций, они активно используются при выборе системы обнаружения атак и их эксплуатации[1] [1].

1.1. Классификация Питера Мелла

Рассмотрение существующих классификаций стоит начать с работы Питера Мелла под названием: «Компьютерные атаки: что это и как им противостоять». В этой работе все возможные сетевые атаки делятся на следующие типы:

- удаленное проникновение представляет собой тип атак, позволяющих реализовать удаленное управление компьютером через сеть; в качестве примеров можно привести атаки с использованием программ BackOrifice или NetBus;
- локальное проникновение является типом атак, приводящих к получению несанкционированного доступа к узлу, на который они направлены; в качестве примера можно привести атаку с использованием программы GetAdmin;
- удаленный отказ в обслуживании является типом атак, позволяющим нарушить функционирование системы в рамках глобальной сети; в качестве примеров можно привести атаки trinOO или Teardrop;
- локальный отказ в обслуживании является типом атак, позволяющим нарушить функционирование системы в рамках локальной сети. Примером такой атаки является запуск и внедрение враждебной программы,

загружающей центральный процессор бесконечным циклом, приводящим к невозможности обработки запросов других приложений;

- атаки с использованием сетевых сканеров являются типом атак, которые основаны на использовании сетевых сканеров, представляющих собой программы, анализирующие топологию сети и обнаруживающих доступные для атаки сервисы; в качестве примеров можно привести атаку с использованием утилиты nmap;
- атаки с использованием сканеров уязвимостей являются типом атак, которые основаны на использовании сканеров уязвимостей, представляющих собой программы, осуществляющие поиск уязвимостей на узлах сети, которые в дальнейшем могут быть применены для реализации сетевых атак; в качестве примеров сетевых сканеров можно привести системы Shadow Security Scanner и SATAN;
- атаки с использованием взломщиков паролей являются типом атак, которые основаны на использовании взломщиков паролей, представляющих собой программы, подбирающие пароли пользователей; например, программа Crack для ОС Unix или программа LOphtCrack для ОС Windows;
- атаки с использованием анализаторов протоколов являются типом атак, которые основаны на использовании анализаторов протоколов, представляющих собой программы, «прослушивающие» сетевой трафик. С их помощью можно автоматизировать поиск в сетевом трафике такой информации, как информацию о кредитных картах, идентификаторы и пароли пользователей и другие подобные данные. В качестве примерамов анализаторов сетевых протоколов можно привести программы NetXRay компании Network Associates, Microsoft Network Monitor или Lan Explorer[2].

Данная классификация с практической точки зрения является достаточно полной, так как она охватывает почти все возможные действия злоумышленника. Но для противодействия сетевым атакам этой классификации недостаточно, за счет того, что ее использование в данном виде не позволяет определять элементы сети, которые подвержены воздействию той или иной атаки, а также последствия, к которым может привести успешная реализация атак. В этом случае в анализ не включается самый важный компонент, который является моделью угроз безопасности, с построения которой должны начинаться все мероприятия по обеспечению защиты информации[3] [1].

1.2. Классификация Internet Security Systems

Аналогичным классификации Питера Мелла недостатком страдает и более компактная классификация, которая предложена компанией IBM Internet Security Systems, Inc., содержащая всего лишь пять типов атак:

- попытки несанкционированного доступа;
- сбор информации;
- системные атаки;
- подозрительная активность;
- отказ в обслуживании [4].

В своих продуктах, предназначенных для защиты серверов, сетей, и рабочих станций (таких как, к примеру, System scanner, Real Secure и другие подобыне) компания IBM Internet Security Systems использует несколько других классификационных признаков возможных сетевых атак, более эффективных с точки зрения защиты от вторжений. Опишем их подробнее.

1. Классификация по степени риска имеет большое практическое значение, за счет возможности ранжирования опасностей атак по таким классам, как:
    - высокий класс, при котором, успешная реализация атаки позволяет атакующему немедленно получить права администратора, доступ к машине или обойти межсетевые экраны. В качестве примеров можно привести атаку, которая основана на использовании ошибки в программном обеспечении Sendmail и позволяет атакующему исполнять любую команду на сервере;
    - средний класс, при котором успешная реализация атаки потенциально может дать атакующему доступ к машине. В качестве примеров можно привести ошибки в сервере NIS, которые позволяют атакующему получить файл с гостевым паролем;
    - низкий класс, при котором успешная реализации атаки даст атакующему возможность получить облегчающие задачу взлома сведения. В качестве примеров можно привести использование сервиса finger, с помощью которого атакующий может определить список пользователей сервера и попытаться получить доступ к машине с использованием атаки по словарю.
2. Классификация по типу атаки позволяет судить о том, может ли атака быть осуществлена только локально или удаленно:
    - осуществляемые удаленно;
    - осуществляемые локально;

3. Классификация по подверженному данной атаке программному обеспечению. Например: Microsoft Internet Explorer.

Кроме того, существует классификация по характеру используемых в атаке действий:

- "черные ходы" — атаки, которые основаны на использовании недокументированных разработчиками возможностях программного обеспечения, имеющих возможность приведения к выполнению пользователем несанкционированных операций на атакуемом сервере;
- атаки типа "отказ в обслуживании" — атаки, которые основаны на использовании ошибок, позволяющих атакующему сделать какой-либо сервер недоступным для легитимных пользователей;
- распределенные атаки типа "отказ в обслуживании", при которых несколько программ или пользователей посылают большое количество фиктивных запросов на сервер, приводя его тем самым в нерабочее состояние;
- неавторизованный доступ;
- потенциально незащищенная операционная система[5].

К недостаткам данных классификационных признаков можно отнести то, что они не позволяют описать цель и последствия атаки. К примеру, классификационный признак по характеру действий содержит два класса атак типа «отказ в обслуживании», но вместе с тем не содержит классов, описывающих атаки, направленные на перехват трафика[6] [1, 2].

1.3. Классификация Nessus

В классификации, использованной в известном программном продукте Nessus, который предназначен для анализа безопасности серверов, был применен отличный от предыдущих классификаций подход. В нем используется классификация "по характеру уязвимости", где берется используемая для реализации атаки уязвимость:

- ошибки в CGI скриптах;
- "черные ходы";
- ошибки в программах — FTP-серверах;
- атаки типа "отказ в обслуживании";
- ошибки в реализации межсетевых экранов;

- наличие на компьютере сервиса Finger или ошибки в реализующих этот сервис программах;
- ошибки, которые позволяют атакующему удаленно получить права администратора;
- ошибки, которые позволяют имеющему терминальный вход на сервер пользователю получить права администратора;
- уязвимости, которые позволяют атакующему удаленно получить любой файл с сервера;
- ошибки в программах — SMTP-серверах;
- ошибки в программах — RPC-серверах;
- ошибки в программах — NIS-серверах;
- неиспользуемые сервисы
- не вошедшие в другие категории прочие ошибки.

Кроме того, по типу программной среды они подразделяются на:

- уязвимости в определенном сервисе;
- уязвимости в определенном программном обеспечении;
- уязвимости в операционной системе [7].

С целью определения уязвимости в операционной системе используется параметр Host/OS, уязвимости в определенном программном обеспечении и в конкретных сервисах классифицируются по группам.

В данной классификации, по сравнению с предыдущими, более детально проработаны атаки, которые используют уязвимости в сетевом, прикладном и системном программном обеспечении. Но данная классификация не охватывает всех существующих сетевых атак. За пределами рассмотрения остаются такие опасные атаки, как направленные на сетевое оборудование атаки, перехват данных и атаки типа "отказ в обслуживании". Положительной чертой данной классификации является наличие класса " не вошедшие в другие категории прочие ошибки", так как благодаря этому классу данная классификация формально применима к любой, в том числе новой, атаке. Но, с другой стороны, этот класс не несет пользы, поскольку не содержит никакой дополнительной информации[8].

Как видно из приведенных выше классификаций, далеко не все они являются полными. В некоторых случаях под видом единой классификации делается попытка объединения нескольких проведенных по разным характеристическим параметрам классификаций.

Появление новых атак приводит к снижению эффективности применения существующих классификаций, поэтому их использование без внесения изменений не представляется возможным. Данная ситуация объясняется огромным количеством различных сетевых атак и постоянным появлением новых атак, некоторые из которых не подчиняются критериям существующих классификаций.

Таким образом, применение существующих классификаций нельзя назвать рациональным. Существует объективная необходимость в создании новой гибкой классификационной схемы возможных сетевых атак, построенной с учетом указанных выше недостатков[9] [2, 3].

1.4. Классификация Милославской и Толстого

Из отечественных вариантов наиболее краткая и информативная классификация приведена в книге Толстого и Милославской. В ней все системы обнаружения атак делятся на минимальное количество классов. Из таких классов можно назвать деление на активные и пассивные атаки по поведению после обнаружения, деление атак по расположению источника результатов аудита в регистрационных файлах хоста или сетевых пакетах, деление атак на поведенческие и интеллектуальные по методу обнаружения[10].

Данная классификация наилучшим образом подходит для построения первичных фильтров систем обнаружения атак, поскольку позволяет ответить на вопрос о том, как должны различать атаки, как именно системы обнаружения атак анализируют информацию, какие технологии для этого использовать[11] [1, 4].

2. Технологии обнаружения атак

Информационные и сетевые технологии меняются так быстро, что статичные защитные механизмы, к которым относятся системы аутентификации, МЭ, системы разграничения доступа во многих случаях не могут обеспечить эффективной защиты. По этой причине требуются динамические методы, которые позволяют оперативно предотвращать и обнаруживать нарушения безопасности. Одной из технологий, которая позволяет обнаруживать нарушения, не имеющие возможности быть идентифицированными при помощи традиционных моделей контроля доступа, является технология обнаружения атак.

По существу, процесс обнаружения атак является процессом оценки подозрительных действий, происходящих в корпоративной сети. Иначе говоря, обнаружение атак является процессом реагирования и идентификации подозрительной деятельности, которая направлена на сетевые или вычислительные ресурсы[12] [2].

2.1. Методы анализа сетевой информации

Эффективность системы обнаружения атак во многом зависит от применяемых методов анализа полученной информации. В первых системах обнаружения атак, которые были разработаны в начале 80-х годов 20 века, использовались статистические методы обнаружения атак. В настоящее время к статистическому анализу добавился ряд новых методик, начиная с нечеткой логики и экспертных систем и заканчивая использованием нейронных сетей[13] [5].

2.1.1. Статистический метод

Основным преимуществом статистического подхода является использование уже зарекомендовавшего себя разработанного аппарата адаптация к поведению субъекта и математической статистики.

Сначала для всех субъектов анализируемой системы определяются профили. Любое отклонение используемого профиля от эталонного считается несанкционированной деятельностью. Статистические методы универсальны, так как для проведения анализа не требуется знания о возможных атаках и используемых ими уязвимостях. Но при использовании этих методик могут возникать проблемы:

- «статистические» системы могут быть с течением времени «обучены» нарушителями так, чтобы атакующие действия рассматривались как нормальные;
- трудно задать граничные значения отслеживаемых системой обнаружения атак характеристик для адекватной идентификации аномальной деятельности;
- «статистические» системы не чувствительны к порядку следования событий; в некоторых случаях одни и те же события в зависимости от порядка их следования могут характеризовать или нормальную, или аномальную

деятельность.

Следует также учитывать не применимость статистических методов в тех случаях, когда для пользователя типичны несанкционированные действия или, когда для пользователя отсутствует шаблон типичного поведения[14] [5].

2.1.2. Экспертные системы

Экспертные системы состоят из набора правил, охватывающих знания человека-эксперта. Использование экспертных систем представляет собой распространенный метод обнаружения атак, при котором информация об атаках формулируется в виде правил. Данные правила могут быть записаны, к примеру, в виде сигнатуры или в виде последовательности действий. При выполнении любого из этих правил принимается решение о наличии несанкционированной деятельности. Важным достоинством такого подхода является практически полное отсутствие ложных тревог[15].

База данных экспертной системы должна содержать сценарии большинства известных на сегодняшний день атак. Экспертные системы требуют постоянного обновления базы данных с целью оставаться постоянно актуальными. Несмотря на то, что экспертные системы предлагают хорошую возможность для просмотра данных в журналах регистрации, требуемые обновления могут выполняться администратором вручную или игнорироваться. Это приводит, как минимум, к экспертной системе с ослабленными возможностями. В худшем случае отсутствие надлежащего сопровождения снижает степень защищенности всей сети, вводя ее пользователей в заблуждение относительно действительного уровня защищенности.

Основным недостатком является невозможность отражения неизвестных атак. При этом даже небольшое изменение уже известной атаки может стать серьезным препятствием для функционирования системы обнаружения атак[16] [4, 5].

2.1.3. Нейронные сети

Большинство современных методов обнаружения атак используют некоторую форму анализа контролируемого пространства на основе статистического подхода или правил. В качестве контролируемого пространства может выступать сетевой

трафик или журналы регистрации. Анализ опирается на набор заранее определенных правил, создаваемых самой системой обнаружения атак или администратором[17].

Любое разделение атаки среди нескольких злоумышленников или во времени является трудным для обнаружения при помощи экспертных систем. Из-за большого разнообразия хакеров и атак даже специальные постоянные обновления базы данных правил экспертной системы никогда не дадут гарантии точной идентификации всего диапазона атак.

Использование нейронных сетей является одним из способов преодоления указанных проблем экспертных систем. В отличие от экспертных систем, имеющих возможность дать пользователю определенный ответ о соответствии рассматриваемых характеристик заложенным в базу данных правилам, нейронная сеть проводит анализ информации и предоставляет возможность оценить, согласуются ли данные с характеристиками, которые она научена распознавать. В то время как степень соответствия нейросетевого представления может достигать ста процентов, достоверность выбора полностью зависит от качества системы в анализе примеров поставленной задачи[18].

Изначально нейронная сеть обучает правильной идентификации на предварительно подобранной выборке примеров предметной области. Реакция нейронной сети анализируется, и система настраивается так, чтобы достичь удовлетворительных результатов. В дополнение к начальному периоду обучения, нейронная сеть набирается опыта с течением времени, по мере проведения анализа связанных с предметной областью данных.

Важным преимуществом нейронных сетей при обнаружении злоупотреблений является их способность «изучать» характеристики умышленных атак и идентифицировать не похожие на наблюдаемые в сети прежде элементы[19].

Каждый из описанных методов обладает рядом недостатков и достоинств, поэтому сейчас практически трудно встретить систему, реализующую только один из описанных методов. Как правило, данные методы используются в совокупности[20] [1, 3, 5].

2.2. Классификация систем обнаружения атак IDS

Применяемые в современных системах обнаружения атак IDS механизмы основаны на нескольких общих методах, не являющихся взаимоисключающими. Во многих системах используются их комбинации.

Классификация IDS может быть выполнена:

- по способу выявления атаки;
- по способу реагирования;
- по способу сбора информации об атаке;
- по методу анализа информации[21] [6].

2.2.1. Классификация по способу реагирования

По способам реагирования на обнаруживаемые угрозы системы IDS можно разделить на два типа: активные и. пассивные Пассивные системы в случае идентификации вторжения обычно создают детальный отчет о произошедшем, который включает лог сетевой атаки, оповещают службу безопасности, к примеру, по электронной почте, и предоставляют рекомендации по устранению выявленной уязвимости. Активные IDS помимо всего вышеперечисленного пытаются противостоять вторжению. Их действия могут включать в себя как разрыв текущего злонамеренного соединения, так и полное блокирование атакующего путем изменения конфигурации межсетевого экрана или иным способом[22].

На данный момент самым распространенным типом подобных систем являются активные IDS. Идеология пассивных IDS более подходит к существующим проектам типа систем-ловушек либо сетей на их основе, задача которых представляет как можно более правдоподобную эмуляцию уязвимой системы и сервисов, при этом с сохранением полной истории происходящего, не создавая дополнительной преграды для нарушителя и не выдавая себя. В итоге с высокой долей вероятности удается определить новые методы компрометации системы[23] [6, 7].

2.2.2. Классификация по способу выявления атаки

По способу выявления атаки системы IDS принято делить на две категории:

- обнаружение злоупотреблений;
- обнаружение аномального поведения.

Технология обнаружения аномального поведения основана на следующем. Аномальное поведение пользователя часто проявляется как отклонение от нормального поведения. Примером аномального поведения может служить высокая загрузка центрального процессора, большое число соединений за короткий промежуток времени и другие подобные активности[24].

Если можно было бы однозначно описать профиль нормального поведения пользователя, то любое отклонение от него можно идентифицировать как аномальное поведение. Но аномальное поведение не всегда является атакой. К примеру, одновременную посылку большого числа запросов от администратора сети система обнаружения атак может идентифицировать как атаку типа «отказ в обслуживании».

При использовании системы с такой технологией возможны два случая:

- обнаружение не являющегося атакой аномального поведения и его отнесение к классу атак;
- пропуск не подпадающей под определение аномального поведения атаки. Данный случай более опасен, чем отнесение не являющегося атакой аномального поведения к классу атак[25].

Технология обнаружения аномалий ориентирована на выявление новых типов атак. Но ее недостатком является необходимость постоянного обучения. На данный момент эта технология не получила широкого распространения. Связано это с трудностями ее реализации на практике.

Обнаружение злоупотреблений заключается в описании атаки в виде сигнатуры и поиска данной сигнатуры в контролируемом пространстве. В качестве сигнатуры атаки может выступать характеризующие аномальную деятельность строка символов или шаблон действий. Данные сигнатуры хранятся в аналогичной используемой в антивирусных системах базе данных. Эта технология обнаружения атак очень похожа на технологию обнаружения вирусов, при этом система может обнаружить все известные атаки. Но системы данного типа не могут обнаруживать еще неизвестные новые виды атак.

Подход, реализованный в таких системах, достаточно прост и именно на нем основаны практически все предлагаемые сегодня на рынке системы обнаружения атак[26] [6, 7].

2.2.3. Классификация по способу сбора информации об атаке

Наиболее популярна классификация по способу сбора информации об атаке:

- обнаружение атак на уровне приложения;
- обнаружение атак на уровне сети;
- обнаружение атак на уровне хоста [27].

Система на уровне сети работает по принципу сниффера, осуществляя прослушивание трафика в сети и определение возможных действий злоумышленников. Такие системы анализируют сетевой трафик, используя, как правило, анализ «на лету» и сигнатуры атак. Метод анализа «на лету» заключается в мониторинге сетевого трафика в реальном или близком к реальному времени и использовании соответствующих алгоритмов обнаружения.

Системы на уровне хоста предназначены для мониторинга, детектирования и реагирования на действия злоумышленников на определенном хосте. Располагаясь на защищаемом хосте, они выявляют и проверяют направленные против него действия. Данные системы анализируют регистрационные журналы приложения или операционной системы[28].

Как правило, анализ журналов регистрации является дополнением к другим методам обнаружения атак, в частности к обнаружению атак «на лету». Использование данного метода позволяет проводить «разбор полетов» уже после того, как была зафиксирована атака, для того чтобы выработать эффективные меры предотвращения аналогичных атак в будущем.

Система на уровне приложений основана на поиске проблем в определенном приложении.

Каждый из этих типов систем обнаружения атак (на уровне приложения, на уровне хоста и на уровне сети) имеет собственные недостатки и достоинства. Гибридные IDS, которые представляют собой комбинацию различных типов систем, обычно включают в себя возможности нескольких категорий[29] [6, 7, 8].

2.2.4. Классификация по методу анализа информации

По методу анализа информации IDS делятся на поведенческие, такие как накопление статистики и обнаружение аномалий, сигнатурные, а также комбинированного типа или смешанные. Сигнатурные IDS генерируют сравнительно немного отчетов об ошибочном детектировании и выигрывают по скорости анализа входного потока, но бессильны перед еще неизвестными им уязвимостями — в этом случае как раз достаточно успешно выступают IDS с применением алгоритмов выявления статистических аномалий. Но зато последние дают ощутимое число ложных срабатываний в совершенно безобидных ситуациях повседневной работы[30].

Самой известной системой обнаружения вторжений на основе сигнатурного поиска безусловно является Snort. Данная IDS завоевала множество почитателей во многом благодаря открытому формату хранения баз, легкости их изменения и внесения собственных наборов правил. В Интернете существует некоммерческий проект Bleeding Edge Threats, который посвящен созданию соответствующих сигнатур для Snort и методам борьбы с сетевыми угрозами[31] [6, 7].

2.3. Компоненты и архитектура IDS

На основе анализа существующих решений можно привести перечень компонентов, из которых состоит типичная система обнаружения атак[32] [9].

2.3.1. Модуль слежения

Модуль слежения обеспечивает сбор данных из контролируемого пространства, такого как журнала регистрации или сетевой трафик. Разные производители дают этому модулю следующие названия: монитор, сенсор, зонд и другие подобные.

В зависимости от архитектуры построения системы обнаружения атак модуль слежения может быть физически отделен от других компонентов, то есть находиться на другом компьютере[33] [8].

2.3.2. Подсистема обнаружения атак

Подсистема обнаружения атак является основным модулем системы обнаружения атак, осуществляющим анализ информации, которая получается от модуля слежения. По результатам этого анализа данная подсистема может принимать решения относительно вариантов реагирования, сохранять сведения об атаке в хранилище данных, идентифицировать атаки и осуществлять другие подобные действия[34] [9].

2.3.3. База знаний

База знаний в зависимости от методов, которые используются в системе обнаружения атак, может содержать сигнатуры атак, профили пользователей и вычислительной системы или подозрительные строки, которые характеризуют несанкционированную деятельность. База знаний может пополняться пользователем системы, производителем системы обнаружения атак или третьей стороной, к примеру, аутсорсинговой компанией, которая осуществляет поддержку этой системы[35] [7].

2.3.4. Хранилище данных

Хранилище данных обеспечивает хранение данных, которые собраны в процессе функционирования системы обнаружения атак[36] [6].

2.3.5. Графический интерфейс

Даже очень эффективное и мощное средство не будет использоваться в случае, когда у него отсутствует дружественный интерфейс. В зависимости от операционной системы, под управлением которой функционирует система обнаружения атак, графический интерфейс должен соответствовать стандартам де-факто для Windows и Unix[37] [8].

2.3.6. Подсистема реагирования

Подсистема реагирования осуществляет реагирование на обнаруженные атаки и иные контролируемые события[38] [7].

2.3.7. Подсистема управления компонентами

Подсистема управления компонентами предназначена для управления различными компонентами системы обнаружения атак. Под термином управления понимается возможность изменения политики безопасности для различных компонентов системы обнаружения атак, а также получение информации от этих компонентов. Управление может осуществляться как при помощи внутренних протоколов и интерфейсов, так и при помощи уже разработанных стандартов, например, SNMP [39] [9].

2.3.8. Архитектура систем обнаружения атак

Системы обнаружения атак строятся на основе двух архитектур: «агент-менеджер» и «автономный агент». Во втором случае на каждый защищаемый сегмент сети или узел устанавливаются агенты системы, не имеющие возможности обмена информацией между собой, а также не имеющие возможности управляться централизовано с единой консоли. Данных недостатков лишена архитектура «агент-менеджер». В ее случае в распределенной системе обнаружения атак dIDS, состоящей из множества расположенных в различных участках большой сети IDS, центральный анализирующий сервер и серверы сбора данных осуществляют централизованный анализ и сбор регистрируемых данных. Управление модулями dIDS осуществляется с центральной консоли управления. Для крупных организаций, где филиалы разнесены по разным территориям и даже городам, использование такой архитектуры имеет принципиальное значение[40].

Общая схема функционирования dIDS приведена на рисунке 1.

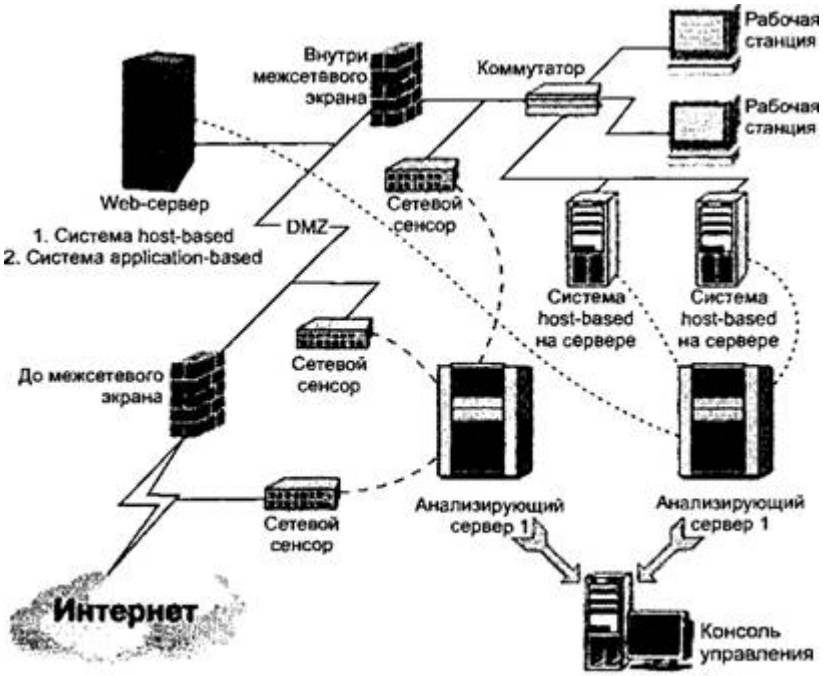

Рис. 14.5. Общая схема функционирования распределенной dIDS

Рис. 1. Общая схема функционирования распределенной dIDS

Даная система позволяет усилить защищенность корпоративной подсети благодаря централизации информации об атаке от различных IDS. Распределенная система обнаружения атак dIDS состоит из следующих подсистем: анализирующих серверов, консоли управления, серверов сбора информации об атаке, агентов сети. Центральный анализирующий сервер обычно состоит из Web-сервера и базы данных, что позволяет сохранять информацию об атаках и манипулировать данными с помощью удобного Web-интерфейса. Агент сети является одним из наиболее важных компонентов dIDS. Он представляет собой небольшую программу, целью которой является информирование об атаке на центральный анализирующий сервер. Сервер сбора информации об атаке является частью системы dIDS, которая логически базируется на центральном анализирующем сервере. Сервер определяет параметры, по которым группируются полученные от агентов сети данные. Группировка данных может осуществляться по следующим параметрам:

- порту получателя;
- IP-адресу атакующего;
- дате, времени;
- номеру агента;
- типу атаки;
- протоколу[41] [6, 9].

2.4. Методы реагирования

Атака не только должна быть обнаружена, но и необходимо своевременно и правильно среагировать на нее. В существующих системах применяется широкий спектр методов реагирования, которые можно разделить на три категории:

- сохранение;
- уведомление;
- активное реагирование.

Применение той или иной реакции зависит от многих факторов[42] [10].

2.4.1. Уведомление

Самым широко распространенным и простым методом уведомления является отправление администратору безопасности сообщений об атаке на консоль системы обнаружения атак. Данная консоль может быть установлена не у каждого сотрудника, который в организации отвечает за безопасность, кроме того, данных сотрудников могут интересовать не все события безопасности, по этой причине необходимо применение иных механизмов уведомления. Данными механизмами могут быть отправление сообщений на пейджер, по электронной почте, по телефону или факсу[43].

К категории уведомлений относят также посылку управляющих последовательностей к другим системам, к примеру, к МЭ или к системам сетевого управления[44] [7, 10].

2.4.2. Сохранение

К категории сохранения относятся два варианта реагирования:

- воспроизведение атаки в реальном масштабе времени;
- регистрация события в базе данных[45].

Второй вариант широко распространен и в других системах защиты. Для реализации первого варианта бывает необходимо пропускать атакующего в сеть компании для фиксации его действий. Данный метод позволяет администратору

безопасности в будущем воспроизводить с заданной скоростью или в реальном масштабе времени все действия, которые осуществлены атакующим, анализировать успешные атаки и предотвращать их в дальнейшем, а также использовать собранные данные в процессе разбирательства[46] [8, 9].

2.4.3. Активное реагирование

К данной категории относятся следующие варианты реагирования:

- завершение сессии с атакующим узлом;
- блокировка работы атакующего;
- управлением сетевым оборудованием и средствами защиты[47].

IDS могут предложить такие конкретные варианты реагирования: автоматическое завершение сессии с атакующим узлом, блокировка учетной записи атакующего пользователя, реконфигурация МЭ и маршрутизаторов и другие подобные. Данная категория механизмов реагирования, достаточно эффективна с одной стороны, но требует аккуратного использования с другой стороны, так как неправильное применение может привести к нарушению работоспособности всей корпоративной информационной системы[48] [6, 10].

Заключение

Большинство рассмотренных недостатков современного обнаружения атак являются недостатками, с которыми может столкнуться пользователь в реальных компьютерных сетях. Большая часть замечаний о степени эффективности и недостатках разрабатываемых средств и методов происходит из практики использования систем обнаружения атак в реальных корпоративных интрасетях.

Существующие подходы к решению задач обнаружения вторжений зачастую отличаются не только реализацией методов обнаружения, но и своей архитектурой, типами обнаружения вторжений и уровнем детализации. Разумеется, у каждой системы есть свои недостатки и достоинства. Но, несмотря на постоянное развитие применяемых при разработке технологий обнаружения атак, о легкости развертывания, модификации и эксплуатации систем обнаружения вторжений придется забыть, все существующие разработки имеют тенденцию лишь к усложнению. Технологии взлома постоянно совершенствуются,

атаки распространяются с очень большой скоростью и становятся комбинированными, поэтому к современному обнаружению атак выдвигаются все более сильные и жесткие требования.

Если рассматривать методы обнаружения атак, то, очевидно, что они должны быть реализованы системами, включающими в себя множество модулей, которые реализуют различные подходы — с учетом различных типовых сегментов защищаемых сетей.

Таким образом, особенности и требования современных компьютерных сетей, такие как повышение надежности сетей, иерархическая структура сетей, повышение мобильности, различные требования к безопасности — все это накладывает отпечаток на подходы и технологии, которые должны быть уже сегодня реализованы в системах обнаружения атак.

Подход к обнаружению сетевых вторжений и выявлению признаков компьютерных атак на информационные системы полон уязвимостей и недостатков, которые позволяют злонамеренным воздействиям успешно преодолевать системы защиты информации. Переход к выявлению предпосылок возникновения угроз информационной безопасности от поиска сигнатур атак должен способствовать тому, чтобы в корне изменить данную ситуацию, сократив дистанцию отставания в развитии систем защиты от систем их преодоления.

Также такой переход должен способствовать повышению эффективности управления информационной безопасностью и, наконец, более конкретным примерам применения руководящих и нормативных документов уже ставших стандартами.

Список используемой литературы

1. Mell P. Computer Attacks: What They Are and How to Defend Against Them / P. Mell. – NIST:Computer Security Division. 1999.
2. IBM Internet Security Systems [Электронный ресурс] – Режим доступа: [http://www.iss.net] (дата обращения: 20.01.2017).
3. Nessus [Электронный ресурс] – Режим доступа: [http://www.tenable.com/products/nessus] (дата обращения: 20.01.2017).
4. Милославская Н.Г., Толстой А.И. Интрасети: обнаружение вторжений / Н.Г. Милославская, А.И. Толстой. – М.:ЮНИТИ-ДАНА, 2001. – 592 с.

5. Боршевников А. Е. Сетевые атаки. Виды. Способы борьбы / А. Е. Боршевников // Современные тенденции технических наук: материалы междунар. науч. конф. — Уфа, 2011. — С. 8-13.
6. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей / В. Ф. Шаньгин. – М.:ДМК Пресс, 2014. – 702 с.
7. Snort [Электронный ресурс] – Режим доступа: [https://www.snort.org] (дата обращения: 21.01.2017).
8. Bleeding Edge Threats [Электронный ресурс] – Режим доступа: [http://www.bleedingthreats.net] (дата обращения: 21.01.2017).
9. Одом У. Компьютерные сети. Первый шаг / У. Одом. — СПб.:Вильямс, 2006. — 432 с.
10. Таненбаум Э. Компьютерные сети / Э. Таненбаум, Д. Уэзеролл. — СПб.:Питер, 2012. — 960 с.

1. Mell P. Computer Attacks: What They Are and How to Defend Against Them / P. Mell. – NIST:Computer Security Division. ↑

2. Mell P. Computer Attacks: What They Are and How to Defend Against Them / P. Mell. – NIST:Computer Security Division. ↑

3. Mell P. Computer Attacks: What They Are and How to Defend Against Them / P. Mell. – NIST:Computer Security Division ↑

4. IBM Internet Security Systems [Электронный ресурс] – Режим до-ступа: [http://www.iss.net] ↑

5. IBM Internet Security Systems [Электронный ресурс] – Режим до-ступа: [http://www.iss.net] ↑

6. Mell P. Computer Attacks: What They Are and How to Defend Against Them / P. Mell. – NIST:Computer Security Division. ↑

7. Nessus [Электронный ресурс] – Режим доступа: [http://www.tenable.com/products/nessus] ↑

8. IBM Internet Security Systems [Электронный ресурс] – Режим до-ступа: [http://www.iss.net] ↑

9. Nessus [Электронный ресурс] – Режим доступа: [http://www.tenable.com/products/nessus] ↑

10. Mell P. Computer Attacks: What They Are and How to Defend Against Them / P. Mell. – NIST:Computer Security Division. ↑

11. Милославская Н.Г., Толстой А.И. Интрасети: обнаружение вторжений / Н.Г. Милославская, А.И. Толстой. – М.:ЮНИТИ-ДАНА, 2001. – 592 с. ↑

12. IBM Internet Security Systems [Электронный ресурс] – Режим до-ступа: [http://www.iss.net] ↑

13. Боршевников А. Е. Сетевые атаки. Виды. Способы борьбы / А. Е. Боршевников // Современные тенденции технических наук: материалы междунар. науч. конф. — Уфа, 2011. — С. 8-13. ↑

14. Боршевников А. Е. Сетевые атаки. Виды. Способы борьбы / А. Е. Боршевников // Современные тенденции технических наук: материалы междунар. науч. конф. — Уфа, 2011. — С. 8-13. ↑

15. Милославская Н.Г., Толстой А.И. Интрасети: обнаружение вторжений / Н.Г. Милославская, А.И. Толстой. – М.:ЮНИТИ-ДАНА, 2001. – 592 с. ↑

16. Боршевников А. Е. Сетевые атаки. Виды. Способы борьбы / А. Е. Боршевников // Современные тенденции технических наук: материалы междунар. науч. конф. — Уфа, 2011. — С. 8-13. ↑

17. Боршевников А. Е. Сетевые атаки. Виды. Способы борьбы / А. Е. Боршевников // Современные тенденции технических наук: материалы междунар. науч. конф. — Уфа, 2011. — С. 8-13. ↑

18. Nessus [Электронный ресурс] – Режим доступа: [http://www.tenable.com/products/nessus] ↑

19. Mell P. Computer Attacks: What They Are and How to Defend Against Them / P. Mell. – NIST:Computer Security Division. ↑

20. Боршевников А. Е. Сетевые атаки. Виды. Способы борьбы / А. Е. Боршевников // Современные тенденции технических наук: материалы междунар. науч. конф. — Уфа, 2011. — С. 8-13. ↑

21. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей / В. Ф. Шаньгин. – М.:ДМК Пресс, 2014. – 702 с. ↑

22. Snort [Электронный ресурс] – Режим доступа: [https://www.snort.org] ↑

23. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей / В. Ф. Шаньгин. – М.:ДМК Пресс, 2014. – 702 с. ↑

24. Snort [Электронный ресурс] – Режим доступа: [https://www.snort.org] ↑

25. Snort [Электронный ресурс] – Режим доступа: [https://www.snort.org] ↑

26. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей / В. Ф. Шаньгин. – М.:ДМК Пресс, 2014. – 702 с. ↑

27. Bleeding Edge Threats [Электронный ресурс] – Режим доступа: [http://www.bleedingthreats.net] ↑

28. Snort [Электронный ресурс] – Режим доступа: [https://www.snort.org] ↑

29. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей / В. Ф. Шаньгин. – М.:ДМК Пресс, 2014. – 702 с. ↑

30. Snort [Электронный ресурс] – Режим доступа: [https://www.snort.org] ↑

31. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей / В. Ф. Шаньгин. – М.:ДМК Пресс, 2014. – 702 с. ↑

32. Одом У. Компьютерные сети. Первый шаг / У. Одом. — СПб.:Вильямс, 2006. — 432 с. ↑

33. Bleeding Edge Threats [Электронный ресурс] – Режим доступа: [http://www.bleedingthreats.net] ↑

34. Одом У. Компьютерные сети. Первый шаг / У. Одом. — СПб.:Вильямс, 2006. — 432 с. ↑

35. Snort [Электронный ресурс] – Режим доступа: [https://www.snort.org] ↑

36. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей / В. Ф. Шаньгин. – М.:ДМК Пресс, 2014. – 702 с. ↑

37. Bleeding Edge Threats [Электронный ресурс] – Режим доступа: [http://www.bleedingthreats.net] ↑

38. Snort [Электронный ресурс] – Режим доступа: [https://www.snort.org] ↑

39. Одом У. Компьютерные сети. Первый шаг / У. Одом. — СПб.:Вильямс, 2006. — 432 с. ↑

40. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей / В. Ф. Шаньгин. – М.:ДМК Пресс, 2014. – 702 с. ↑

41. Одом У. Компьютерные сети. Первый шаг / У. Одом. — СПб.:Вильямс, 2006. — 432 с. ↑

42. Таненбаум Э. Компьютерные сети / Э. Таненбаум, Д. Уэзеролл. — СПб.:Питер, 2012. — 960 с. ↑

43. Snort [Электронный ресурс] – Режим доступа: [https://www.snort.org] ↑

44. Таненбаум Э. Компьютерные сети / Э. Таненбаум, Д. Уэзеролл. — СПб.:Питер, 2012. — 960 с. ↑

45. Одом У. Компьютерные сети. Первый шаг / У. Одом. — СПб.:Вильямс, 2006. — 432 с. ↑

46. Bleeding Edge Threats [Электронный ресурс] – Режим доступа: [http://www.bleedingthreats.net] ↑

47. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей / В. Ф. Шаньгин. – М.:ДМК Пресс, 2014. – 702 с. ↑

48. Таненбаум Э. Компьютерные сети / Э. Таненбаум, Д. Уэзеролл. — СПб.:Питер, 2012. — 960 с. ↑