МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
Факультет прикладной математики и информатики
Кафедра информационных систем управления

МЕНЬКОВ АНДРЕЙ АЛЕКСАНДРОВИЧ

РАЗРАБОТКА МАТЕМАТИЧЕСКОГО И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ РЕШЕНИЯ ЗАДАЧИ ОБНАРУЖЕНИЯ АТАК НА КОМПЬЮТЕРНЫЕ СИСТЕМЫ

Отчёт по преддипломной практике
студента 5 курса 2 группы

Руководитель:
Образцов Владимир Алексеевич
доцент кафедры ИСУ,
кандидат физико-математических наук

МИНСК
БГУ
2013

АННОТАЦИЯ

Меньков А. А. Разработка математического и программного обеспечения для решения задачи обнаружения атак на компьютерные системы: Отчёт по преддипломной практике / Минск: БГУ, 2013. — 24 с.

АНАТАЦЫЯ

Менькоу А. А. Распрацоўка матэматычнага і праграмнага забеспячэння для вырашэння задачы выяўлення нападаў на кампутарныя сістэмы: Справаздача аб пераддыпломнай практыцы / Мінск: БДУ, 2013. — 24с.

ANNOTATION

Menkou A. A. Development of mathematical and software solutions for the problem of detection of attacks on computer systems: Pregraduation report / Minsk: BSU, 2013 — 24p.

РЕФЕРАТ

Отчёт по преддипломной практике, 24с.

Ключевые слова: КОМПЬЮТЕРНАЯ СЕТЬ, АТАКА, ОБНАРУЖЕНИЕ АТАК.

Объект исследования — атаки на компьютерные сети.

Цель работы — разработать обеспечение для обнаружения атак на компьютерные сети.

Методы исследования — методы прикладной математики и информатики, кластерный анализ.

Результат исследования — реализация модуля обнаружения аномалий в компьютерной сети как часть современной системы обнаружения атак.

Областью применения являются компьютерные сети с повышенным контролем безопасности информации, передаваемой по сети.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Компьютерные сети за несколько последних десятилетий из чисто технического решения превратились в глобальное явление, развитие которого оказывает влияние на большинство сфер экономической деятельности. Одним из первых количественную оценку значимости сетей дал Роберт Меткалф, участвовавший в создании Ethernet: по его оценке «значимость» сети во всех смыслах пропорциональна квадрату числа узлов в ней. То есть, зависимость от нормальной работы сетей растёт быстрее, чем сами сети. Обеспечение работоспособности сети и функционирующих в ней информационных систем зависит не только от надёжности аппаратуры, но и, зачастую, от способности сети противостоять целенаправленным воздействиям, которые направлены на нарушение её работы.

Создание информационных систем, гарантированно устойчивых к вредоносным воздействиям и компьютерным атакам, сопряжено с существенными затратами как времени, так и материальных ресурсов. Кроме того, существует известная обратная зависимость между удобством пользования системой и её защищённостью: чем совершеннее системы защиты, тем сложнее пользоваться основным функционалом информационной системы. В 80-е годы XX века, в рамках оборонных проектов США, предпринимались попытки создания распределенных информационных систем специального назначения (MMS – Military Messaging System), для которых формально доказывалась выполнимость основной теоремы безопасности – невыведение системы из безопасного состояния для любой последовательности действий взаимодействующих объектов. В этих системах использовалось специализированное программное обеспечение на всех уровнях, включая системный. Однако, на сегодняшний день подобные системы не получили развития, и для организации информационных систем используются операционные системы общего назначения, такие как ОС семейства Microsoft Windows, GNU/Linux, *BSD и различные клоны SysV UNIX (Solaris, HP-UX, etc).

Методы обнаружения атак в современных системах обнаружения атак (далее - СОА) недостаточно проработаны в части формальной модели атаки, и, следовательно, для них достаточно сложно строго оценить такие свойства как вычислительная сложность, корректность, завершимость. Принято разделять методы обнаружения атак на методы обнаружения аномалий и методы обнаружения злоупотреблений. Ко второму типу методов относятся большинство современных коммерческих систем (Cisco IPS, ISS RealSecure, NFR) — они используют сигнатурные (экспертные) методы обнаружения. Для таких систем основной проблемой является низкая, близкая к нулю, эффективность обнаружения неизвестных атак (адаптивность). Низкая адаптивность до сих пор остаётся проблемой, хотя такие достоинства как низкая вычислительная сложность и малая стоимость развёртывания определяют доминирование таких систем в данной области.

В данной работе реализуется попытка создать компонент для обнаружения аномалий в компьютерной системе на основе «сырых» сетевых данных, собранных с компьютеров в сети с реализацией как компьютерных атак, так и нормального поведения в сети, в течение 24 часов.

1 ОСНОВНЫЕ ПОНЯТИЯ ОБ АТАКАХ И ИХ ОБНАРУЖЕНИИ

Рассмотрим основные термины и определения, касающиеся области компьютерных систем и атак на них

Компьютерная атака — это целенаправленное несанкционированное воздействие на информацию, на ресурс автоматизированной информационной системы или получение несанкционированного доступа к ним с применением программных или программно-аппаратных средств (в соответствии с ГОСТ Р 51275-2006) [1].

Процесс функционирования компьютерной системы можно представить как последовательность событий, изменяющих состояние этой системы. С точки зрения информационной безопасности каждое событие можно представить как совокупность двух составляющих — действия и адресата. Если существуют потенциально возможные действия, которые могут нанести ущерб системе, значит, существует угроза нарушения информационной безопасности. Угрозы могут быть различны в зависимости от конкретных условий эксплуатации системы. Любая последовательность связанных между собой действий нарушителя, которые приводят к реализации угрозы путём использования уязвимостей этой информационной системы, является компьютерной атакой.

Любые несанкционированные системные или сетевые действия на одной из компьютеров в любой из подсетей, целью которых является нарушение политики безопасности, являются атакой на данную систему.

Существуют различные классификации атак. К основным факторам, которые влияют на клиссификацию атак, можно отнести:

- взаимное расположение атакующего и атакуемого объекта, то есть наличие или отсутствие у нарушителя физического доступа к атакуемой системе
- атакуемый ресурс — узел, сеть, линии связи, приложение, база данных и т.д.
- целевое воздействие на ресурс и уровень потенциального ущерба от атаки

Кроме того, многие атаки могут производиться не одним нарушителем, а множеством, что позволяет добавить ещё один фактор — распределённость атаки.

В зависимости от наличия физического доступа к системе выделяют [2]:

- локальные атаки — попытки получения доступа к информации или к управлению при наличии непосредственного доступа к системе
- удалённые атаки — попытки получения доступа к информации или управлению без непосредственного доступа к системе, а через каналы связи другой системы
- атаки на каналы связи — попытки получения доступа к информации или управлению системами в процессе передачи данных по каналам связи между системами
- атаки с отслеживанием побочных электромагнитных излучений ЭВМ — реализуются с применением средств спецтехники

В зависимости от цели атаки выделяют:

- «удалённое проникновение», «Remote-To-Local», «R2L» — целью является получение управления удалённой системой (относится к удалённым атакам)

- «локальное проникновение», «User-To-Root», «U2R», в том числе взлом паролей — целью является получение управления на локальной системе, превышающего полномочия данного субъекта (относится к локальным атакам)

- «удалённый отказ в обслуживании», «remote Denial of service», «DoS» — целью является нарушение функционирования системы или перегрузка компьютера, на котором она реализуется (относится к локальным атакам)

- сетевое сканирование, сканирование уязвимостей, «Probing» - целью является получение информации о топологии вычислительное сети и уязвимых сервисах, доступных для атаки (относятся к удалённым атакам или атакам на каналы связи). Выделяется в отдельных класс, несмотря на то, что является по сути сбором исходных данных для последующей реализации других атак: так как информация о внутренней организации сети является конфиденциальной, получение информации о ней посторонним субъектом уже само по себе является атакой

- перехват сетевого траффика — «прослушивание» траффика с целью поиска идентификаторов и паролей пользователей, другой конфиденциальное инофрмации (относится к атакам на каналы связи). Стоит отметить, что практически все средства защиты информации используют перехват траффика в собственных целях, поэтому нужно различать — кто и с какой целью «прослушивает» сеть

Сетевая атака — это компьютерная атака с использованием протоколов межсетевого взаимодействия (в соответствии с ГОСТ Р 51275-2006) [1].

Согласно приведенным выше классификациям, к сетевым атакам в первую очередь стоит отнести удалённые атаки и атаки на каналы связи. Однако, некоторые локальные атаки также могут производиться с использованием сетевых средств системы.

Сетевые атаки могут производиться на любом из уровней эталонной модели взаимодействия открытым систем OSI. Атаки на физическом и канальном уровнях из-за специфики можно не рассматривать при создании методов обнаружения сетевых атак. Противодействие данным атакам должно производиться при помощь оборудования, функционирующего на этих уровнях. Обнаружение атак на остальных пяти уровнях модели — начиная с сетевого и заканчивая прикладным — это и есть задача системы обнаружения атак.

Система обнаружения атак, или ***система обнаружения вторжений*** — это система, осуществляющая сбор информации с множества системных и сетевых источников, анализирующая полученную информацию на предмет признаков вторжений (атак) [3]. Соответствует английскому термину *Intrusion Detection System*.

СОА отличаются от других средств обеспечения сетевой безопасности, например, межсетевых экранов или антивирусного ПО. Занимаясь анализом поведения субъекта системы либо анализом сетевого трафика, СОА может обнаружить признаки атаки, производимой при помощь легальных для данной системы средств — соединений через открытые порты, незараженных вирусами программ, и даже аномального поведения пользователя, не похожего на его обычное поведение в информационной системе. Поэтому СОА являются необходимым элементов обеспечения безопасности компьютерной системы.

Практически любую компьютерную атаку можно обнаружить «постфактум» путём анализа экспертом журналов регистрации событий безопасности — ОС, СУБД, прикладных программ и т.д. Тем самым снижаются затраты на развёртывание и обеспечение функционирования инфраструктуры обнаружения атак. Однако, временные затраты на осуществление данного процесса возрастут многократно, что в итоге не позволит оперативно реагировать на нарушения политики безопасности и тем более предотвращать их. С этой целью и создаются специализированные средства обнаружения атак.

Можно определить главные задачи системы защиты информации.

1. Система должна качественно выполнять возложенные на неё функции — обнаруживать и распознавать как известные, так и неизвестные атаки, а также сообщать об этом надлежащим образом

2. Снижение нагрузки на персонал за счёт автоматического контроля действий в информационной системе. Персонал оставляет за собой ответственность за управлением функционированием системы защиты информации и выполняет мероприятия по реагированию на обнаруженные атаки

2 ПОСТАНОВКА ЗАДАЧИ

Традиционно, наиболее используемыми методами для автоматического обнаружения атак являются сигнатурные методы. Эти методы выделяют ключевые признаки из сетевого трафика, и обнаружение происходит путём сравнения этих признаков согласно списка сигнатур атак, предоставляемых экспертами. Очевидно, такие методы не имеют возможности обнаружения новых типов атак, потому что для этого необходимо наличие соответствующего этой атаке сигнатурного правила. База данных, содержащие такие правила, должна поддерживаться вручную и обновляться по мере появление новых известных атак. Другие подходы используют data mining и алгоритмы машинного обучения для обучения на помеченных сетевых данных (т.е. на экзэмплярах сетевой активности, помеченных метками «атака» или «не атака»).

Подход, использующий обнаружение аномалий, обычно оперирует над моделью «нормальных» данных и в последующем пытается обнаружить отклонения от «нормальной» модели исследуемых данных. Алгоритмы обнаружения аномалий имеют преимущество в том, что могут обнаруживать новый типы атак, т.к. новые атаки, по предположению, будут отклоняться от нормального сетевого поведения. Традиционно алгоритмы обнаружения аномалий требуют наличия абсолютно чистых сетевых данных, на базе которых происходит обучение их модели. Если же окажется, что данные содержат какие-то атаки, алгоритм может не распознать эти типы атак, посчитав их нормальными.

Чаще всего таких данных не существует, как и не всегда просто найти заранее помеченные данные, для которых известно где производилась атака, а где нет. В общем случае приходится иметь дело с огромными объёмами сетевых данных, в связи с чем становится сложно реализуемой возможность ручной классификации этих данных. Можно сгенерировать помеченные данные, имитируя атаки, но в таком случае у нас будут данные только для заранее известных типов атак. И мы столкнёмся с тем же недостатком обнаружения, которым обладают сигнатурные методы — невозможность обнаружения новых типов атак. Более, если и предположить возможность ручной классификации данных, всё равно мы ограничены возможностью обнаружения только заданных типов атак, тем самым сокращая возможности системы. Генерация абсолютно чистых от атак данных сложно реализуема на практике. При сборе «сырых» данных из сети, нельзя гарантировать, что во время сбора не было произведено каких-либо атак в сети.

В этой работе будет сделана попытка реализовать новый тип алгоритма обнаружения атак с целью избежать сложностей и недостатков представленных выше подходов. На вход алгоритму поступают заранее неизвестные сетевые данные и в них производится поиск на наличие атак. О данных делается 2 предположения, которые лежат в основе возможности реализации и корректности такого алгоритма. Первое предположение состоит в том, что число нормальных данных намного больше данных с атаками. Второе предположение — атаки качественно отличаются от нормальных данных. Основная идея состоит в том, что благодаря редкости и качественному отличию атак, на фоне всех данных они будут представлять своего рода выбросы. На основании чего и будут обнаружены.

3 ОБЗОР МЕТОДОВ И СИСТЕМ ОБНАРУЖЕНИЯ КОМПЬЮТЕРНЫХ АТАК

В данном разделе приведен обзор основных методов обнаружения компьютерных атак, используемых в современных СОА, а также нескольких некоммерческих СОА. Целью обзора является исследовать эффективность доступных в настоящее время СОА и определить основные недостатки используемых в них методов обнаружения атак. Основная сложность составления подобного обзора заключается в том, что множество доступных реализаций СОА представлено, в основном, коммерческими системами (такими как Cisco IPS, Juniper NetScreen, ISS RealSecure, NFR и т.д.), для которых отсутствует открытая информация о программной архитектуре и используемым формальным методам обнаружения атак. Доступная информация по подобным системам носит маркетинговый характер, что затрудняет проведение сравнительного анализа по публикациям в литературе. По этой причине множество рассматриваемых в обзоре систем будет ограничено СОА с открытым исходным кодом, доступным публично. В результате обзора будет показано, что:

1. Большинство современных СОА используют на базовом уровне ту или иную реализацию сигнатурного метода обнаружения (pattern matching, сравнение шаблонов). Реализации отличаются друг от друга уровнем рассмотрения системы, алфавитом сигнатур и используемым «движком» — от простого поиска подстрок до полноценной реализации регулярных выражений над заданным алфавитом.

2. Множество существующих методов обнаружения атак много шире, но их использование в системах имеет принципиальные ограничения, связанные с требованиями верифицируемости, устойчивости и воспроизводимости результата, а также большим числом ошибок второго рода (ложных срабатываний). Использование таких методов ограничено экспериментальными академическими разработками.

3. Доступные реализации СОА неустойчивы к модификациям атак и не могут автоматически адаптироваться к появлению новых атак. При этом использование методов обнаружения аномалий (например, в препроцессорах СОА Snort) ограничено по причинам, перечисленным в п.2.

3.1 Критерии сравнения

В обзоре используются две группы критериев: первая группа характеризует собственно методы обнаружения атак и специфичные для них качественные и количественные показатели эффективности, в то время как вторая группа критериев характеризует реализации этих методов в системах обнаружения атак.

3.1.1 Критерии сравнения методов обнаружения атак

Для сравнительного анализа методов обнаружения атак выбраны следующие критерии:

Уровень наблюдения за системой: Данный критерий определяет уровень абстракции анализируемых событий в защищаемой системе и определяет границы применимости метода для обнаружения атак в сетях. В рамках данного обзора рассматриваются следующие уровни:

- HIDS — наблюдение на уровне операционной системы отдельного узла сети
- NIDS — наблюдение на уровне сетевого взаимодействия объектов на узлах сети

- AIDS — наблюдение на уровне отдельных приложений узла сети
- Hybrid — комбинация наблюдателей разных уровней

Верифицируемость метода: Данный критерий позволяет оценить, может ли человек (например, квалифицированный оператор СОА или эксперт) воспроизвести последовательность шагов по принятию решения о наличии атаки, сопоставляя входные и выходные данные СОА. Например, сигнатурные методы будем считать верифицируемыми, а кластерные – нет. Верифицируемость позволяет провести экспертную оценку корректности метода и его реализации в произвольный момент времени, в том числе в процессе эксплуатации системы обнаружения на его основе. Свойство верифицируемости метода важно при эксплуатации системы обнаружения атак в реальной обстановке в качестве средства сбора доказательной базы об атаках.

Возможные значения: высокая (+), низкая (-).

Адаптивность метода: Оценка устойчивости метода к малым изменениям реализации атаки, которые не изменяют результат атаки. Адаптивность является единственным существенным преимуществом «альтернативных» методов обнаружения атак перед «сигнатурными». Отсутствие адаптивности не позволяет системе защиты оперативно реагировать на неизвестные атаки и требует организации системы регулярного обновления баз известных атак, по аналогии с антивирусными системами. Возможные значения: высокая (+), низкая (-).

Устойчивость: Данный критерий характеризует независимость выхода метода от защищаемой системы — для одного и того же входа метод должен давать один и тот же выход, независимо от защищаемой системы. Проблема устойчивости особенно остро стоит для статистических методов, анализирующих абсолютные значения параметров производительности и загруженности ресурсов сети и узлов, которые могут существенно отличаться на различных узлах и в различных сетях. Обученный в одной сети распознаватель может быть устойчивым в пределах данной сети и неустойчивым во всех остальных сетях. Такую устойчивость будем называть локальной. Так как процедура обучения обычно является «дорогой» — требует использования большого количества ресурсов и времени — число процедур обучения желательно минимизировать. Методы обнаружения атак, анализирующие семантику ввода, более устойчивы, чем статистические. Возможные значения: глобальная (+), локальная (-).

Вычислительная сложность: Теоретическая оценка сложности метода на основе информации из публикаций. В обзоре рассматривается только сложность метода в режиме обнаружения, без учёта возможных предварительных этапов настройки и обучения. Данный критерий является ключевым для задачи обнаружения атак в сетях и имеет гораздо большее значение, нежели сложность по памяти из-за опережающего роста пропускной способности каналов передачи данных и удешевления машинной памяти.

- Сублинейная — константа, логарифм
- Линейная
- Квадратичная и т.д.

В обзоре не рассмотрены такие важные критерии как полнота и точность метода, т.к. эти характеристики редко приводятся в публикациях.

3.1.2 Критерии сравнения систем обнаружения атак

Для сравнительного анализа СОА были выбраны следующие критерии:

Класс обнаруживаемых атак. Данный критерий определяет, какие классы атак способна обнаружить рассматриваемая система. Это один из ключевых критериев. В связи с тем, что

на сегодняшний день ни одна система не способна обнаружить атаки всех классов, для более полного покрытия всего спектра атак необходимо комбинировать различные СОА. Здесь мы используем классификацию атак, основанную на разделении ресурсов защищаемой системы по типам.

Класс атаки – это четверка **<L,R,A,D>**, где L — расположение атакующего объекта, R — атакуемый ресурс, A — целевое воздействие на ресурс, D — признак распределенного характера атаки.

L: расположение атакующего объекта. Оно может быть либо внутренним по отношению к защищаемой системе **(li)**, либо внешним **(le)**.

R: атакуемый ресурс. Ресурсы разделяются по расположению и по типу.

- По расположению: узловые **(rl)**, сетевые **(rn)**.
- По типу: пользовательские ресурсы **(ru)**, системные ресурсы **(rs)**, ресурсы СУБД **(rd)**, вычислительные ресурсы **(rc)**, ресурсы защиты **(rp)**.

A: целевое воздействие на ресурс: сбор информации **(as)**, получение прав пользователя ресурса **(au)**, получение прав администратора ресурса **(ar)**, нарушение целостности ресурса **(ai)**, нарушение работоспособности ресурса **(ad)**.

D: признак распределенного характера атаки: распределенные **(dd)**, нераспределенные **(dn)**.

Следующий критерий характеризует источники и способы сбора информации о поведении объектов и состоянии ресурсов:

Уровень наблюдения за системой. Определяет, на каком уровне защищаемой системы собирают данные для обнаружения атаки. Различаются узловые и сетевые источники. В пределах узловых источников разделяются уровни ядра и приложения. От уровня наблюдения за системой зависит скорость сбора информации, влияние системы на собираемую информацию, вероятность получения искаженной информации. Следует отметить, что использование метода обнаружения, позволяющего анализировать поведение на всех уровнях абстракции, не означает, что эта возможность реализована в конкретной системе. Зачастую реализация обладает меньшими возможностями, чем теоретические возможности используемого ею метода.

- HIDS — наблюдение на уровне операционной системы отдельного узла сети
- NIDS — наблюдение на уровне сетевого взаимодействия объектов на узлах сети
- AIDS — наблюдение на уровне отдельных приложений узла сети
- Hybrid — комбинация наблюдателей разных уровней

Следующий критерий определяет эффективность обнаружения атаки на основе анализа полученной информации.

Используемый метод обнаружения. Метод обнаружения также является ключевым критерием сравнения. Существует два класса методов: *методы обнаружения аномалий* и *методы обнаружения злоупотреблений*. В приведенном ниже списке перечислены не отдельные методы, но, в основном, семейства методов, объединённых некоторым единым подходом или теоретической моделью.

- Обнаружение злоупотреблений
  - Анализ систем состояний

  - Графы атак
  - Нейронные сети
  - Иммунные сети
  - SVM
  - Экспертные системы
  - Методы, основанные на спецификациях
  - MARS – Multivariate Adaptive Regression Splines
  - Сигнатурные методы

- Обнаружение аномалий

  - Статистический анализ
  - Кластерный анализ (data mining)
  - Нейронные сети
  - Иммунные сети
  - Экспертные системы
  - Поведенческая биометрия
  - SVM
  - Анализ систем состояний

Адаптивность к неизвестным атакам. Определяет способность используемого метода обнаруживать ранее неизвестные атаки.
Следующие критерии определяют такие архитектурные особенности СОА как управление и распределенность.

Масштабируемость. Определяет возможность добавления новых анализируемых ресурсов сети, новых узлов и каналов передачи данных, в том числе возможность управления единой распределенной системой обнаружения атак. Управление может быть централизованное и/или распределенное. Дополнительно может присутствовать возможность удаленного управления СОА. Сюда включаются задачи установки, настройки и администрирования системы. При полностью распределенном управлении необходимо управлять всеми компонентами СОА в отдельности. При полностью централизованном управлении все компоненты СОА могут управляться с одного узла. Оптимальной представляется организация управления по централизованной схеме, в которой может быть несколько центров, и они могут динамически меняться.

Открытость. Определяет насколько система является открытой для интеграции в нее других методов обнаружения атак, компонентов сторонних разработчиков и сопряжения ее с другими системами защиты информации. Это могут быть программные интерфейсы для встраивания дополнительных модулей и/или реализация стандартов взаимодействия сетевых компонентов.

Формирование ответной реакции на атаку. Определяет наличие в системе встроенных механизмов ответной реакции на атаку, кроме самого факта ее регистрации. Примерами реакции могут быть разрыв соединения с атакующим объектом, блокировка его на межсетевом экране, отслеживание пути проникновения атакующего объекта в защищаемую систему и т.д.

Защищенность. Определяет степень защищенности СОА от атак на ее компоненты, включая защиту передаваемой информации, устойчивость к частичному выходу компонентов из

строя или их компрометации. Затрагиваются такие вопросы, как наличие уязвимостей в компонентах СОА, защищенность каналов передачи данных между ними, а также авторизация компонентов внутри СОА.

Таким образом, некая «идеальная» система обнаружения атак обладает следующими свойствами:

- покрывает все классы атак (система полна)
- позволяет анализировать поведение защищаемой РИС на всех уровнях: сетевом, узловом и уровне отдельных приложений
- адаптивна к неизвестным атакам (использует адаптивный метод обнаружения атак)
- масштабируется для РИС различных классов: от небольших локальных сетей класса «домашний офис» до крупных многосегментных и коммутированных корпоративных сетей, обеспечивая возможность централизованного управления всеми компонентами СОА
- является открытой
- имеет встроенные механизмы реагирования на атаки
- является защищённой от атак на компоненты СОА, в том числе от перехвата управления или атаки «отказ в обслуживании».

3.2 Методы обнаружения атак

Все методы обнаружения атак можно разделить на два класса: методы обнаружения аномалий и методы обнаружения злоупотреблений. Методы первого класса базируются на наличии готового описания нормального поведения наблюдаемых объектов РИС, и любое отклонение от нормального поведения считается аномальным (нарушением). Методы обнаружения злоупотреблений основаны на описании известных нарушений или атак: если наблюдаемое поведение некоторого объекта РИС совпадает с описанием известной атаки, поведение объекта считается атакой.

3.2.1 Методы обнаружения злоупотреблений

Анализ систем состояний: В данной группе методов функционирование защищаемой системы представляется через множество состояний и множество переходов между ними, т.е. в виде ориентированного графа (как правило, бесконечного). Суть метода обнаружения атак заключается в том, что часть путей в таком графе помечаются как недопустимые; конечное состояние каждого такого пути считается опасным для защищаемой системы. Процесс обнаружения атаки представляет собой построение части графа состояний системы и наблюдаемых переходов между ними, и поиск в полученном графе известных недопустимых путей. Обнаружение последовательности переходов, приводящей в опасное состояние, означает успешное обнаружение атаки. В соответствии с введёнными критериями, данный метод является гибридным с точки зрения уровня наблюдения за системой, верифицируемым, устойчивым, имеет низкую вычислительную сложность (линейную относительно длины трассы наблюдаемых переходов и числа состояний), но не является адаптивным.

Графы сценариев атак: На вход системе верификации подаётся конечная модель защищаемой системы и некоторое формальное свойство корректности, которое выполняется только для разрешённого поведения системы. Данное свойство корректности делит всё

множество поведений на два класса — допустимого поведения, для которого свойство выполняется, и недопустимого, для которого оно не выполняется. Отличие данного метода от обычных систем верификации заключается в том, что их задача, обычно, найти один контрпример из множества недопустимого поведения, а в предложенном методе строится полный набор таких примеров для конкретной защищаемой системы, что даёт на выходе описание возможных путей атаки. Из-за высокой вычислительной сложности (NP) данный метод может быть использован для поиска уязвимостей проектирования систем и других сложных для обнаружения уязвимостей, но для задачи обнаружения атак в реальном времени он неприменим. По остальным критериям метод является гибридным, верифицируемым, устойчивым и адаптивным.

Нейронные сети: Так как задачу обнаружения атак можно рассматривать как задачу распознавания образов (или задачу классификации), то для её решения также применяются нейронные сети. Для этого функционирование защищаемой системы и взаимодействующих с ней внешних объектов представляется в виде траекторий в некотором числовом пространстве признаков. В качестве метода обнаружения злоупотреблений, нейронные сети обучаются на примерах атак каждого класса и, в дальнейшем, используются для распознавания принадлежности наблюдаемого поведения одному из классов атак. Основная сложность в использовании нейросетей заключается в корректном построении такого пространства признаков, которое позволило бы разделить классы атак между собой и отделить их от нормального поведения. Кроме того, для классических нейронных сетей характерно долгое обучение, при этом время обучения зависит от размера обучающей выборки. В соответствии с введёнными критериями, нейронные сети используются на сетевом и узловом уровнях, являются адаптивными, имеют сравнительно низкую вычислительную сложность. При этом они не являются верифицируемыми и устойчивы, как правило, только в пределах той сети, в которой они обучались, что существенно ограничивает применимость метода (только локальная устойчивость).

Иммунные сети: Также как и нейронные сети, иммунные сети являются механизмом классификации и строятся по аналогии с иммунной системой живого организма. Основное достоинство иммунных сетей заключатся в возможности получения «антител» к неизвестным атакам. В одной работе (РАБОТА) была предложена модель формального пептида, для которой заявлена возможность использования в системах обнаружения атак. Однако, позже было показано, что использование данного метода требует решения системы дифференциальных уравнений в режиме обнаружения, что даёт вычислительную сложность порядка $O(n^3)$ при использовании метода Рунге-Кутта. В соответствии с введёнными критериями, данная группа методов применима для сетевого и узлового уровней, не верифицируема, адаптивна, устойчива только локально, имеет высокую вычислительную сложность.

Support vector machines (SVM): SVM – это метод представления и распознания шаблонов, который позволяет формировать шаблоны в результате обучения. Данный метод требует небольшого количества данных для обучения и позволяет обрабатывать векторы признаков большой размерности, что полезно для повышения точности систем обнаружения атак и снижения временных затрат на обучение и переобучение. Метод применим как для обнаружения злоупотреблений, так и для обнаружения аномалий. SVM имеет такие же достоинства и недостатки для решения нашей задачи, как и нейронные сети, т.е. является адаптивным, но неверифицируемым.

Экспертные системы: Использование экспертных систем для обнаружения атак основано на описании функционирования системы в виде множества фактов и правил вывода, в том числе для атак. На вход экспертная система получает данные о наблюдаемых событиях в системе в виде фактов. На основании фактов и правил вывода система делает вывод о наличии или отсутствии атаки. Данная группа методов удовлетворяет практически всем критериям (верифицируема, адаптивна, устойчива), но в общем случае имеет очень большую

вычислительную сложность, так как для нее может наблюдаться явление «комбинаторного взрыва» и полного перебора большого числа альтернатив.

Методы, основанные на спецификациях: В основе данного метода лежит описание ограничений на запрещенное поведение объектов в защищаемой системе в виде спецификаций атак. В спецификацию может входить: ограничения на загрузку ресурсов, на список запрещенных операций и их последовательностей, на время суток, в течение которого применимы те или иные ограничения. Соответствие поведения спецификации считается атакой. Спецификации используются для сетевого уровня, является верифицируемым, локально устойчивым и имеет низкую вычислительную сложность. Данный подход близок к классу методов обнаружения аномалий. Основные недостатки — низкая адаптивность и сложность разработки спецификаций.

Multivariate Adaptive Regression Splines (MARS): Один из методов аппроксимации функций, основанный на сплайнах. Аналогично нейронным сетям и кластерному анализу MARS оперирует в многомерном пространстве признаков. Поведение сетевых объектов отображается в последовательности векторов данного пространства. Задача процедуры MARS заключается в построении оптимальной аппроксимации поведения по заданной истории в виде обучающего множества векторов, при этом в качестве аппроксимирующей функции используются сплайны с переменным числом вершин. В ходе «обучения», с помощью переборного процесса, выбирается оптимальное число вершин для заданной выборки. Построенный сплайн является «шаблоном» атаки. В режиме распознавания наблюдаемое поведение отображается в параметрическое пространство и сравнивается с аппроксимирующей функцией. Достоинства и недостатки данного метода аналогичны SVM и нейронным сетям.

Сигнатурные методы: Наиболее часто используемая группа методов, суть которых заключается в составлении некоторого алфавита из наблюдаемых в системе событий и описании множества сигнатур атак в виде регулярных выражений (в общем случае) в построенном алфавите. Как правило, сигнатурные методы работают на самом низком уровне абстракции и анализируют непосредственно передаваемые по сети данные, параметры системных вызовов и записи файлов журналов. В наиболее развитом виде представляет собой реализацию регулярных выражений над различными трассами (сетевой трафик, системные вызовы, записи журналов приложений и т.п.). Сигнатурные методы примечательны тем, что для них хорошо применимы аппаратные ускорители, но при этом метод не является адаптивным. По остальным критериям данная группа методов является гибридной, глобально устойчивой, верифицируемой.

3.2.2 Методы обнаружения аномалий

Статистический анализ: Данная группа методов основана на построении статистического профиля поведения системы в течение некоторого периода «обучения», при котором поведение системы считается нормальным. Для каждого параметра функционирования системы строится интервал допустимых значений, с использованием некоторого известного закона распределения. Далее, в режиме обнаружения, система оценивает отклонения наблюдаемых значений от значений, полученных во время обучения. Если отклонения превышают некоторые заданные значения, то фиксируется факт аномалии (атаки). Для статистического анализа характерен высокий уровень ложных срабатываний при использовании в локальных сетях, где поведение объектов не имеет гладкого, усреднённого характера. Кроме того, данный метод устойчив только в пределах конкретной системы, то есть построенные статистические профили нельзя использовать на других аналогичных системах.

Кластерный анализ: Суть данной группы методов состоит в разбиении множества наблюдаемых векторов-свойств системы на кластеры, среди которых выделяют кластеры нормального поведения. В каждом конкретном методе кластерного анализа используется своя

метрика, которая позволяет оценивать принадлежность наблюдаемого вектора свойств системы одному из кластеров или выход за границы известных кластеров. Кластерный анализ является адаптивным, но не верифицируемым и устойчивым в пределах конкретной системы, в которой собирались данные для построения кластеров.

Нейронные сети: Нейронные сети для обнаружения аномалий обучаются в течение некоторого периода времени, когда всё наблюдаемое поведение считается нормальным. После обучения нейронная сеть запускается в режиме распознавания. В ситуации, когда во входном потоке не удается распознать нормальное поведение, фиксируется факт атаки. В случае использования репрезентативной обучающей выборки нейронные сети дают хорошую устойчивость в пределах заданной системы; но составление подобной выборки является серьёзной и сложной задачей. Классические нейронные сети имеют высокую вычислительную сложность обучения, что затрудняет их применение на больших потоках данных.

Иммунные сети: Обнаружение аномалий является одним из возможных приложений иммунных методов. Так как количество примеров нормального поведения обычно на порядки превышает число примеров атак, использование иммунных сетей для обнаружения анормалий имеет большую вычислительную сложность.

Экспертные системы: Информация о нормальном поведении представляется в подобных системах в виде правил, а наблюдаемое поведение в виде фактов. На основании фактов и правил принимается решение о соответствии наблюдаемого поведения «нормальному», либо о наличии аномалии. Главный недостаток подобных систем — высокая вычислительная сложность (в общем случае). В том числе при обнаружении аномалий.

Поведенческая биометрия: Включает в себя методы, не требующие специального оборудования (сканеров сетчатки, отпечатков пальцев), т.е. методы обнаружения атак, основанные на наблюдения клавиатурного почерка и использования мыши. В основе методов лежит гипотеза о различии «почерка» работы с интерфейсами ввода-вывода для различных пользователей. На базе построенного профиля нормального поведения для данного пользователя обнаруживаются отклонения от этого профиля, вызванные попытками других лиц работать с клавиатурой или другими физическими устройствами ввода. Поведенческая биометрия имеет строго локальную устойчивость (в пределах одной сети) и слабо верифицируема.

Support vector machines (SVM): SVM применим как для обнаружения злоупотреблений, так и для обнаружения аномалий, при этом метод имеет достоинства и недостатки, аналогичные нейронным сетям

3.2.3 Результаты сравнительного анализа

Таким образом, анализ публикаций показывает, что для большинства методов обнаружения аномалий характерна слабая верифицируемость и слабая глобальная устойчивость (либо её отсутствие). Основное достоинство методов обнаружения аномалий заключается в их адаптивности и способности обнаруживать ранее неизвестные атаки. Среди глобально устойчивых и верифицируемых методов, имеющих при этом низкую вычислительную сложность, можно отметить метод анализа системы переходов и простой сигнатурный метод. Ни один из рассмотренных методов не обладает одновременно адаптивностью, устойчивостью и верифицируемостью, имея при этом приемлемую вычислительную сложность.

3.3 Современные открытые системы обнаружения атак

В данном разделе рассмотрены доступные на сегодняшний день системы обнаружения атак с открытым исходным кодом.

Таблица 1 – Результаты сравнения методов обнаружения атак

Критерий / Метод	Уровень наблюдения	Аномалии / Злоупотр.	Вериф	Адапт	Устойч	Выч. сложность
Системы переходов	Hybrid	-/+	+	-	+	$O(n)$
Графы атак	Hybrid	-/+	+	+	+	NP
Нейронные сети	NIDS, HIDS	+/+	-	+	-	$O(n)$ и выше
Имунные сети	NIDS, HIDS	+/+	-	+	-	$O(n)$ и выше
SVM	NIDS, HIDS	+/+	-	+	-	$ln(n)$
Экспертные системы	NIDS, HIDS	+/+	+	+	+	NP
Спецификации	NIDS	-/+	+	-	-	$ln(n)$
MARS	NIDS, HIDS	-/+	-	+	-	$O(n)$ и выше
Сигнатурные методы	Hybrid	-/+	+	-	+	$ln(n)$
Статистические методы	NIDS, HIDS	+/-	-	+	-	$O(n)$ и выше
Кластерный анализ	Hybrid	+/+	-	+	-	$O(n)$ и выше
Поведенческая биометрия	HIDS	+/-	-	+	-	$O(n)$ и выше

3.3.1 Исследованные системы обнаружения атак

Всего рассмотрено 5 систем обнаружения атак. В таблице 2 приведена краткая информация по каждой из них.

Таблица 2 – Открытые системы обнаружения компьютерных атак

Название	Производитель	Ссылки
Bro	University of California, Lawrence Berkeley National Laboratory	http://bro-ids.org/
OSSEC	Daniel B. Sid, OSSEC.net	http://www.ossec.net/
STAT	University of California at Santa Barbara	http://www.cs.ucsb.edu/seclab/index.html
Prelude	Yoann Vandoorselaere, Laurent Oudot	http://www.prelude-ids.org/
Snort	Martin Roesch	http://www.snort.org/

Часть рассмотренных систем (Bro, NetSTAT) разработаны в университетах и базируются на исследованиях в области обнаружения атак, проведенных в этих университетах.

3.3.2 Результаты сравнительного анализа

В данном разделе приводятся результаты сравнения рассмотренных СОА. Системы сравниваются отдельно по каждому из вышеуказанных критериев. Сводная таблица сравнения СОА по всем критериям дана в конце раздела. Все рассмотренные системы используют в качестве основного метода обнаружения атак сигнатурный метод (сравнение строк, шаблонов).

Система Bro [5] использует регулярные выражения над трассами, которые формируются сетевыми протоколами. Набор регулярных выражений создаётся экспертами. Кроме того, в состав системы входит транслятор сигнатур из формата системы Snort в сценарии Bro (хотя в настоящее время этот транслятор поддерживает не все конструкции языка Snort).

Система OSSEC [6] является монолитной – в сенсоры и анализаторы «зашиты» знания разработчиков системы обнаружения атак о том, какие последовательности сообщений в журналах могут быть признаками атаки. Такая архитектура системы является трудно расширяемой с точки зрения базы знаний об атаках.

Система NetSTAT [7] использует язык описания сценариев атак STATL, особенностью которого является возможность описания сценария атаки в виде последовательности действий над атакуемым ресурсом. Таким образом, эта система использует метод обнаружения, близкий к методу анализа переходов состояний.

Система Prelude [8] использует различные анализирующие компоненты для сетевых данных и журналов регистрации. Для анализа сетевых данных можно использовать систему Snort. Также используется набор специализированных модулей для обнаружения специфических атак, таких как сканирование портов, некорректные ARP- пакеты и т.п. Специальные модули производят дефрагментацию IP, сборку TCP-потока, декодирование HTTP-запросов.

Система Snort [9] использует базу сигнатур известных атак. В ней также используется набор специализированных модулей для обнаружения специфических атак, таких как сканирование портов или отправка большого числа фрагментированных пакетов. Специальные модули производят дефрагментацию IP, декодирование HTTP-запросов. Сторонние разработчики часто реализуют другие методы обнаружения атак в виде модулей (препроцессоров) Snort. Но в основную версию системы они не входят.

Класс обнаруживаемых атак

Все исследованные системы могут обнаруживать атаки нескольких классов. Поэтому для улучшения читаемости и сокращения объема текста вводятся понятия объединения, пересечения и вложения классов атак. Для обозначения объединения и пересечения классов атак будем использовать символы $\cup$ и $\cap$ соответственно.

Системы, рассмотренные в данной работе, предназначены для обнаружения атак разных классов. Часть систем ориентирована на обнаружения узловых атак, и использует для анализа такие источники как журналы регистрации приложений, ОС, журналы систем аудита (OSSEC). Другие системы обнаруживают только внешние (сетевые) атаки и используют для анализа информацию, получаемую из каналов передачи данных в сети (Bro, Snort). Остальные системы являются гибридными и обнаруживают как локальные, так и внешние атаки (STAT, Prelude).

Система Bro является сетевой системой обнаружения атак. Она представляет собой набор модулей декомпозиции данных различных сетевых протоколов (от сетевого до прикладного уровня) и набор сигнатур над событиями соответствующих протоколов. Сигнатуры Bro фактически представляют собой регулярные выражения в алфавитах протоколов.

Данная система обнаруживет атаки следующих классов (L,R,A,D):

- L=$\{\mathbf{li} \cup \mathbf{le}\}$ (внутренние и внешние атаки)
- R=$\{\mathbf{rn}\} \cap \{\mathbf{ru} \cup \mathbf{rs}\}$ (атаки на сетевые пользовательские ресурсы и системные ресурсы)
- A=$\{\mathbf{as} \cup \mathbf{au} \cup \mathbf{ar} \cup \mathbf{ad}\}$ (сбор информации о системе, попытки получения прав пользователя, попытки получения прав администратора и нарушение работоспособности ресурса)
- D=$\{\mathbf{dn} \cup \mathbf{dd}\}$ (нераспределенные и распределенные)

Система OSSEC, единственная из рассмотренных в данной работе, является изначально ориентированной на обнаружение атак уровня системы (узловых). Она наиболее «молодая» из рассмотренных систем; её последняя версия предназначена, в частности, для анализа журналов регистрации UNIX, типовых приложений (ftpd, apache, mail, etc), а также журналов межсетевых экранов и сетевых СОА. OSSEC включает в себя набор анализаторов для различных источников данных, контроль целостности файловой системы, сигнатуры известных троянских закладок (rootkits) и пр.

Обнаруживаются атаки следующих классов:

- L={**li**} (атакующие объекты находятся внутри системы)
- R={**rl**} ∩ {**ru** ∪ **rs**} (узловые пользовательские и системные ресурсы)
- A={**au** ∪ **ar** ∪ **ai**} (попытки получения прав пользователя, попытки получения прав администратора, нарушение целостности ресурса)
- D={**dn** ∪ **dd**} (нераспределенные и распределенные)

Система STAT является экспериментальной университетской разработкой, и наиболее «старой» из рассматриваемых систем — первые публикации по STAT датируются 1992 годом. Система включает в себя набор компонентов обнаружения атак различных уровней — сетевой (NetSTAT), узловой (USTAT, WinSTAT), приложений (WebSTAT), т.е. является классической гибридной системой.

СОА обнаруживает атаки следующих классов:

- L={**li** ∪ **le**} (внутренние и внешние атаки)
- R={**rl** ∪ **rn**} ∩ {**ru** ∪ **rs**} (атаки на узловые или сетевые пользовательские ресурсы и системные ресурсы);
- A={**as** ∪ **au** ∪ **ar** ∪ **ad**} (сбор информации о системе, попытки получения прав пользователя, попытки получения прав администратора и нарушение работоспособности ресурса)
- D={**dn**} (нераспределенные)

Система Prelude, как и NetSTAT, является гибридной, т.е. способна обнаружить атаки как на уровне системы, так и на уровне сети. Данная система изначально разрабатывалась в качестве самостоятельной СОА, но в настоящее время является высокоуровневой надстройкой над открытыми СОА и системами контроля целостности (AIDE, Osiris и т.п.). Узловая часть Prelude имеет достаточно широкий набор описаний атак и, в качестве источника информации, использует различные журналы регистрации:

- журналы регистрации межсетевого экрана IPFW
- журналы регистрации NetFilter ОС Linux
- журналы регистрации маршрутизаторов Cisco and Zyxel
- журналы регистрации GRSecurity
- журналы регистрации типовых сервисов ОС UNIX и другие

СОА обнаруживает атаки следующих классов:

- L={**li** ∪ **le**} (внутренние и внешние атаки)
- R={**rl** ∪ **rn**} ∪ {**ru** ∪ **rs** ∪ **rp**} (атаки на локальные или сетевые пользовательские ресурсы, системные ресурсы и ресурсы защиты)
- A={**as** ∪ **au** ∪ **ar** ∪ **ad**} (сбор информации о системе, попытки получения прав пользователя, попытки получения прав администратора и нарушение работоспособности ресурса)
- D={**dn**} (нераспределенные)

Система Snort это наиболее популярная на сегодняшний день некоммерческая СОА. Она активно и динамично развивается, обновления базы известных атак происходят с частотой, сравнимой с коммерческими аналогами (обычно обновления Snort опережают коммерческие). Snort является чисто сетевой СОА и, кроме основной базы описаний атак, имеет набор подключаемых модулей для обнаружения специфических атак или реализующих альтернативные методы обнаружения.

Система способна обнаружить атаки следующих классов:

- L="внутренние" ∪ "внешние"
- R={**rl** ∪ **rn**} ∩ {**ru** ∪ **rs** ∪ **rp**} (атаки на локальные или сетевые пользовательские ресурсы, системные ресурсы и ресурсы защиты);
- A={**as** ∪ **au** ∪ **ar** ∪ **ad**} (сбор информации о системе, попытки получения прав пользователя, попытки получения прав администратора и нарушение работоспособности ресурса);
- D={**dn** ∪ **dd**} (нераспределенные и распределенные).

Таким образом, ни одна из рассмотренных систем не покрывает всё множество классов атак. Следует также отметить, что эти системы используют неадаптивные методы обнаружения атак.

Уровень наблюдения за системой

Все рассмотренные выше системы работают с данными приложений и операционной системы на узловом уровне, а так же с сетевыми данными. То есть анализируемая информация получается из вторичных источников, таких как журналы регистрации приложений, ОС, либо из сетевого канала передачи данных. Система OSSEC работает исключительно с журналами регистрации приложений и операционной системы. Системы Bro, Snort анализируют только сетевые данные. Системы NetSTAT и Prelude анализируют как данные из локальных системных источников, так и сетевые данные. Из рассмотренных систем ни одна не покрывает все уровни наблюдения, и анализируемая каждой системой информация неполна с точки зрения возможности обнаружения атак всех классов. Для обнаружения атак всех классов необходимо анализировать информацию на всех трёх уровнях одновременно.

Адаптивность к неизвестным атакам

На данный момент эта возможность в рассмотренных СОА отсутствует. Возможно использование экспериментального модуля статистического анализа системы Snort, но его эффективность не изучена. За счет контроля целостности ресурсов узла в системе OSSEC присутствует условная адаптивность. Тем не менее, следует признать, что контроль целостности

решает не задачу обнаружения атак, а лишь задачу обнаружения их последствий. Таким образом, адаптивность к неизвестным атакам в рассмотренных СОА, в целом, отсутствует.

Масштабируемость

Система Bro является нераспределённой и управляется централизованно на том узле, где она установлена, с помощью файлов конфигурации. При увеличении числа защищаемых узлов и каналов связи необходимо устанавливать дополнительные независимые экземпляры системы Bro, что означает фактическую немасштабируемость.

Система OSSEC является распределённой и управляется либо распределенно на узлах, где установлены агенты (при помощи файлов конфигурации), либо централизованно с помощью специализированной утилиты администрирования с центрального сервера OSSEC. Система является хорошо масштабируемой.

Система NetSTAT также является распределённой и управляется распределенно через файлы конфигурации на всех узлах, где расположены компоненты системы. Индивидуальное управление компонентов системы делает процесс управления и настройки сложным и длительным, причём с ростом числа компонентов сложность настройки и внесения изменений в конфигурацию усложняется.

Система Prelude является распределённой и управляется централизованно при помощи управляющей консоли. Компоненты системы сами предоставляют управляющей консоли те параметры их функционирования, которые могут изменяться. Управление производится по защищенному каналу (SSL). Также управление может осуществляться через локальные конфигурационные файлы на тех узлах, где установлены компоненты СОА. Данная система является хорошо масштабируемой.

Система Snort управляется централизованно через файлы конфигурации, консольные команды и сигналы UNIX. Сама по себе система не является масштабируемой, но в случае использования Snort в качестве сенсора системы Prelude этот недостаток устаняется.

Открытость

Три из рассматриваемых систем, за исключением Bro и OSSEC, имеют открытый интерфейс для добавления новых анализирующих модулей, а также используют стандартный для систем обнаружения атак формат обмена сообщениями (IDMEF).

Система Bro позволяет пользователю и сторонним разработчикам расширять набор сигнатур.

NetSTAT имеет открытый интерфейс для добавления новых агентов и фильтров.

Prelude имеет открытый интерфейс для добавления новых модулей анализа и реагирования, а так же ведения журналов регистрации. Обмен сообщениями между компонентами системы происходит по стандарту IDMEF (Intrusion Detection Message Exchange Format), оптимизированному для высокоскоростной обработки.

Snort имеет открытый интерфейс для добавления новых модулей анализа; имеется модуль, реализующий протокол SNMPv2.

По совокупности используемых стандартных интерфейсов, системы Prelude и Snort лучше остальных позволяют наращивать функциональность по обнаружению атак.

Формирование ответной реакции на атаку

Встроенную возможность реагирования на атаку имеют все рассматриваемые системы. В системе NetSTAT это реализовано лишь в тестовом варианте. Система Prelude имеет набор агентов ответной реакции, которые могут блокировать атакующего при помощи межсетевого экрана. Ведутся работы по агентам, способным либо полностью изолировать атакующего, либо уменьшить пропускную способность его канала. Система Snort имеет встроенную ограниченную возможность реагирования на атаку путем отправки TCP-пакетов, разрывающих

соединение (с установленным флагом RST), а также ICMP-пакетов, сообщающих атакующему узлу о недоступности узла, сети или сервиса. Аналогичная функциональность по реагированию доступна в системе Bro. Система OSSEC позволяет использовать произвольные команды для реагирования — для этого необходимо статически задать соответствие между событием, командой и параметрами её вызова.

Защищенность

Все системы, которые пересылают какие-либо данные, используют для этого защищенные каналы.

STAT и Prelude используют библиотеку OpenSSL для шифрования канала между компонентами.

Snort реализует протокол SNMPv2, в котором присутствуют функции шифрования паролей при передаче данных.

СОА Prelude имеет дополнительные механизмы, обеспечивающие безопасность ее компонентов. В системе используется специализированная библиотека, которая делает безопасными такие библиотечные функции алгоритмического языка С как printf, strcpy, которые не проверяют размер передаваемых им данных. Библиотека предотвращает классические ошибки выхода за границы массивов и переполнения буферов. Дополнительные модули анализа сетевых данных делают систему устойчивой к некорректным сетевым пакетам на разных уровнях стека и выходу ее компонентов из строя. Такие атаки, как отправка пакетов с неправильными контрольными суммами, обнуленными флагами TCP, ресинхронизация сессий, случайная отправка и «обрезание» сегментов системой игнорируются.

Из рассмотренных систем вопрос безопасности наиболее проработан в системе Prelude.

ЗАКЛЮЧЕНИЕ

За время прохождения преддипломной практики выполнено:

- изучен предмет компьютерной атаки, их основные типы и угрозы, которые они могут представлять
- рассмотрены и проанализированы существующие на данный момент методы обнаружения компьютерных атак, их реализации в современных системах обнаружения атак
- выявлены достоинства и недостатки существующих методов
- найдены и получены актуальные тестовые данные о поведении в компьютерной сети за 2012 год [10]
- предложена модификация существующих методов обнаружения аномалий (снято ограничение на необходимость иметь на входе алгоритма кластеризованные по типам данные)
- рассмотрены основные алгоритмы кластерного анализа

В итоге можно сделать вывод, что была проделана работа по изучению теоретической основы, на которой базируется любая система обнаружения атак, изучены основные подходы к решению проблемы обнаружения атак и предложен вариант модификации одного из методов обнаружения аномалий с использованием инструмента кластерного анализа. Дальнейшая работа предполагает реализацию предложенного алгоритма и внедрение его как составной части комплексной системы обнаружения атак Snort.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

[1] Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения: ГОСТ Р 51275-2006. — Введ. — М. Стандартинформ, 2007. — 7 с.

[2] Губенков, А. А. Информационная безопасность / А. А. Губенков, В. Б. Байбурин. — М.: Новый издательский дом, 2005. — 128 с.

[3] Bace, R. An Introduction to Intrusion Detection & Assessment: For System and Network Security Management / R. Bace // ICSA White Paper. — 1998. — 38 p.

[4] Northcutt, S. Network Intrusion Detection. / S. Northcutt, J. Novak. — New Riders Publishing, 2002. — 346 p.

[5] Bro Intrusion Detection System [Electronic resource] — Mode of access: http://www.bro-ids.org/. — Date of access: 15.01.2013.

[6] OSSEC — an Open Source Host-based Intrusion Detection System [Electronic resource] — Mode of access: http://www.ossec.net/. — Date of access: 15.01.2013.

[7] Vigna, G. NetSTAT: A Network-based Intrusion Detection System. / G. Vigna, R. A. Kemmerer — Journal of Computer Security, 1999. — 79 p.

[8] Prelude SIEM [Electronic resource] — Mode of access: https://www.prelude-ids.org/. — Date of access: 18.01.2013.

[9] Snort network intrusion prevention and detection system [Electronic resource] — Mode of access: http://www.snort.org/. — Date of access: 20.01.2013.

[10] UNB ISCX Intrusion Detection Evaluation DataSet — Information Security Center of eXcellence [Electronic resource] — Mode of access: http://www.iscx.ca/dataset. — Date of access: 25.11.2012.