Кафедра Управления и Информационных Технологий

Специальность Прикладная информатика

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

к курсовому проекту

на тему: Способ и устройство обнаружения аномалий в сетях

Задание на курсовую работу

студенту группы

фамилия, имя, отчество полностью

Тема работы : Способ и устройство обнаружения аномалий в сетях

1. Исходные данные

Регламентирующие документы Гостехкомиссии РФ по обеспечению информационной безопасности

1.1 Руководящий документ «Программное обеспечение средств защиты информации классификация по уровню контроля отсутствия недекларированных возможностей».

1.2 РД «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации».

2 Содержание расчетно-пояснительной записки (перечень вопросов, подлежащих разработке)

## 2.1 Из истории обнаружения вторжений

## 2.2 Обзор технологий обнаружения вторжений

2.3 Проблемы сбора данных

2.4 Средства обнаружения атак

2.5 Парадигмы в обнаружении вторжений

2.6 Методы обнаружения

2.6.1 Обнаружение аномалий

2.6.2 Обнаружение злоупотреблений

2.7 Ответные действия: после вторжения

2.8 Эффективность системы

2.8 Производительность

2.8 Анализ в масштабе всей сети

2.8 Уведомления о взломе

1. Консультанты по работе (указанием относящихся к ним разделов работы)

Храмов В.В.

1. Срок сдачи студентом законченной работы
2. Дата выдачи задания

Руководитель профессор Храмов В.В. , к.т.н.

(подпись)

Задание принял к исполнению

Студент

(подпись)

Оглавление

Введение 6

Из истории обнаружения вторжений 7

Обзор технологий обнаружения вторжений 8

Проблемы сбора данных 9

Средства обнаружения атак 10

Парадигмы в обнаружении вторжений 12

Методы обнаружения 14

Обнаружение аномалий 14

Обнаружение злоупотреблений 15

Ответные действия: после вторжения 16

Эффективность системы 17

Производительность 18

Анализ в масштабе всей сети 19

Уведомления о взломе 20

Заключение 24

Список используемой литературы 26

## Введение

Даже с самой совершенной защитой компьютерные системы нельзя назвать абсолютно неуязвимыми. В настоящее время актуальное значение приобрела проблема обнаружения аномалий в работе сетевых устройств, являющихся как результатом сетевых атак хакеров, так и сбоев в работе аппаратуры и программного обеспечения.

Существующие системы, решающие эту проблему, имеют серьезные ограничения, связанные с принципами функционирования реализованных в них сигнатурных методов обнаружения:

- для любой новой аномалии (атаки) требуется создание новой сигнатуры;

- существуют методы, позволяющие хакерам «обходить» сигнатуры на основе разнообразных методов изменения атакующих воздействий.

Понятие "обнаружение аномалий" возникло сравнительно недавно и сразу привлекло внимание специалистов в области сетевой безопасности. В середине 2003 года на рынке средств защиты информации появились первые западные и отечественные системы обнаружения аномалий, а поставщики услуг сетевой безопасности начали активно предлагать соответствующие решения. Согласно прогнозам Gartner, 85% крупнейших международных компаний с вероятностью 0.8 воспользуются к 2007 году функциями современных систем обнаружения аномалий.

В разработанном Научно-техническим советом НАТО ранжированном списке из 11 важнейших технических задач на период 2002-2007 гг. три первые ориентированы на разработку аппаратных и аппаратно-программных систем обнаружения аномалий вычислительных процессов в современных и перспективных распределенных вычислительных системах на основе TCP/IP. Актуальность этой задачи объясняется тем, что согласно стратегическим отчетам НАТО существующие системы обнаружения вторжений (IDS) ежедневно обнаруживают в среднем 400-600 попыток несанкционированного автоматического вторжения. При этом эксперты подчеркивают: данное число составляет не более 14-17% от общего числа реально осуществляемых атак и воздействий нарушителей. По понятным причинам эти факты настораживают и вызывают определенное беспокойство у специалистов в области защиты информации.

## Из истории обнаружения вторжений

Первоначально системные администраторы обнаруживали вторжения, сидя перед консолью и анализируя действия пользователей. Они могли заметить атаку, обратив, к примеру, внимание на то, что пользователь, который должен находиться в отпуске, вошел в систему, причем локально, либо необычайно активен принтер, который крайне редко используется. Когда-то достаточно эффективная, эта форма обнаружения вторжений была вместе с тем сугубо ориентированной на конкретные ситуации и не обладала масштабируемостью.

На следующем этапе для обнаружения вторжений стали использоваться журналы регистрации, которые системные администраторы просматривали в поисках признаков необычных или злонамеренных действий. В конце 70-х и в начале 80-х годов администраторы, как правило, печатали журналы регистрации на перфорированной бумаге, которая к концу рабочей недели представляла собой кипу высотой в полтора-два метра. Поиск по такому листингу, безусловно, занимал уйму времени. При огромном количестве информации и исключительно ручных методах анализа, администраторы зачастую использовали журналы регистрации в качестве доказательства нарушения защиты уже после того, как оно произошло. Надежда на то, что удастся обнаружить атаку в момент ее проведения, была крайне мала.

По мере того, как дисковая память становилась все дешевле, журналы регистрации стали создавать в электронном виде; появились программные средства для анализа собранных данных. Однако подобный анализ выполнялся очень медленно и зачастую требовал значительных вычислительных ресурсов, так что, как правило, программы обнаружения вторжений запускались в пакетном режиме, по ночам, когда с системой работало мало пользователей. Большинство нарушений защиты по-прежнему выявлялись уже постфактум.

В начале 90-х годов были разработаны системы обнаружения вторжений в оперативном режиме, которые просматривали записи в журнале регистрации сразу, как только они генерировались. Это позволило обнаруживать атаки и попытки атак в момент их проведения, что, в свою очередь, дало возможность немедленно принимать ответные меры, а, в некоторых случаях, даже предупреждать атаки.

Самые последние проекты, посвященные обнаружению вторжений, сосредоточиваются вокруг создания инструментов, которые могут эффективно развертываться в крупных сетях. Эта задача отнюдь не проста, учитывая все большее внимание, уделяемое вопросам безопасности, бесчисленное количество новых методов организации атак и непрерывные изменения в окружающей вычислительной среде.

## Обзор технологий обнаружения вторжений

Цель обнаружения вторжений, на первый взгляд, очень проста: выявить проникновение в информационную систему. Однако это весьма сложная задача. На самом деле, системы обнаружения вторжений никаких вторжений вообще не обнаруживают — они только выявляют признаки вторжений либо во время таких атак, либо постфактум.

Такие свидетельства иногда называют «проявлениями» атаки. Если никаких проявлений нет, если о таких проявлениях нет необходимой информации, либо если информация есть, но не внушает доверия, система не в состоянии обнаружить вторжение.

Например, предположим, что система мониторинга дома анализирует данные, полученные с камеры слежения, которая показывает человека, пытающегося открыть дверь. Видеоданные камеры — проявление происходящего вторжения. Если объектив камеры запачкан или не в фокусе, система не сможет определить, что это за человек — грабитель или хозяин дома.

## Проблемы сбора данных

Для точного обнаружения вторжений необходимы надежные и исчерпывающие данные о происходящем в защищаемой системе. Сбор надежных данных — вопрос сложный сам по себе. Большинство операционных систем содержит определенные виды аудита, которые позволяют создавать различные журналы регистрации операций для разных пользователей. Эти журналы можно ограничить только событиями, связанными с безопасностью (например, неудачные попытки входа в систему); кроме того, они могут предоставлять полный отчет по каждому системному вызову, инициированному каждым процессом. Маршрутизаторы и межсетевые экраны также ведут журналы регистрации событий для сетевой деятельности. Эти журналы могут содержать простую информацию, такую как открытие и закрытие сетевых соединений, или полную запись о каждом пакете, появляющемуся в сети.

Объем информации, которую собирает система, — это компромисс между накладными расходами и эффективностью. Система, которая записывает каждое действие во всех подробностях, может серьезно потерять в своей производительности и потребовать чересчур большого дискового пространства. Например, на сбор полной регистрационной информации о сетевых пакетах в канале Fast Ethernet ежедневно могут потребоваться сотни гигабайт дисковой памяти.

Сбор информации — дело дорогостоящее, а сбор нужной информации — крайне важное. Вопрос о том, какую информацию следует регистрировать и где ее следует накапливать, остается открытым. Например, установка в системе охраны дома монитора для контроля уровня загрязнения воды обойдется недешево, но никоим образом не позволит предотвратить проникновение в дом грабителей. С другой стороны, если модель потенциальных угроз дому предполагает атаки террористов, то контроль загрязнения воды, возможно, оправдан.

## Средства обнаружения атак

Классификация средств обеспечения секретности информации по уровням модели ISO/OSI в стандарте ISO 7498:

-  Физический уровень. Средства, предоставляемые на этом уровне, ограничиваются конфиденциальностью для соединений и конфиденциальностью для потока данных, согласно ISO 7498-2.Конфиденциальность на этом уровне обеспечивается обычно с помощью шифрования бит. Эти средства могут быть реализованы как почти прозрачные, то есть без появления дополнительных данных (кроме установления соединения).

Целостность и аутентификация обычно невозможны здесь из-за того, что интерфейс на уровне бит этого уровня не имеет возможностей для передачи дополнительных данных, требуемых при реализации этих средств. Тем не менее, использование соответствующих технологий шифрования на этом уровне может обеспечить предоставление этих средств на более высоких уровнях.

- Канальный уровень. Согласно ISO 7498-2, средствами, предоставляемыми на канальном уровне, являются конфиденциальность для соединений и конфиденциальность для дейтаграмм.

- Сетевой уровень. Средства секретности сетевого уровня могут предоставляться между конечными системами в сети, независимо от используемых коммутаторов (например, коммутаторов пакетов Х.25). ISO 7498-2 отмечает применимость нескольких средств секретности для этого уровня: конфиденциальность для соединений, конфиденциальность для дейтаграмм, конфиденциальность потока данных, целостность (для соединений без восстановления и для дейтаграмм), аутентификацию источника данных и взаимодействующих сущностей, а также управление доступом.

- Транспортный уровень. Для транспортного уровня ISO 7498-2 определяет следующие средства секретности: конфиденциальность (для соединений или дейтаграмм), целостность (любая, кроме отдельных полей), аутентификация источника данных и взаимодействующих сущностей, и управление доступом. Существует лишь одно отличие между средствами секретности, предоставляемыми для дейтаграммного взаимодействия на транспортном уровне и средствами, предлагаемыми над сетевым уровнем. Оно заключается в способности обеспечить защиту в промежуточных системах (используя механизмы сетевого уровня), а не только в конечных системах (используя механизмы транспортного уровня).

- Сеансовый уровень. ISO 7498-2 не позволяет предоставлять средства на сеансовом уровне. Этот уровень мало, что дает в смысле средств взаимодействия по сравнению с транспортным или прикладным уровнем. Основываясь на принципе, что не стоит предоставлять средства секретности, не соответствующие базовым средствам взаимодействия на данном уровне, можно возражать против предоставления средств секретности на сеансовом уровне. Кроме того, можно утверждать, что средства секретности лучше предоставлять на транспортном, представительном или прикладном уровнях.

- Представительный уровень. Так как этот уровень используется для преобразования данных между обычным и сетевым представлениями, то выгодно шифровать данные на этом уровне, а не на прикладном. Если приложение выполняет шифрование, оно предохраняет представительный уровень от реализации этой функции. Это аргумент против реализации шифрования на прикладном уровне для приложений, которые взаимодействуют напрямую (а не через посредников). Альтернативой этому является дублирование возможностей представительного уровня в приложениях. В стеке TCP/IP, из-за того, что функции представления включены в состав приложений, а не выделены в отдельный уровень, этот конфликт преодолен.

- Прикладной уровень. ISO 7498-2 утверждает, что все секретные средства могут быть предоставлены на прикладном уровне, а контроль за участниками взаимодействия может быть предоставлен только на этом уровне. Фактически, приложения, такие, как средства электронной почты и справочника, могут быть засекречены только с помощью секретности прикладного уровня.

## Парадигмы в обнаружении вторжений

Исследователи работают над системами обнаружения вторжений уже длительное время, но так и не достигли того, что можно было бы назвать "настоящим прорывом". Обычно, направление исследований сфокусировано на направлении, которое называется "обнаружение аномального поведения" (Anomaly Detection Intrusion Detection Systems, AD-IDS). В принципе, AD-IDS "изучает" то, что составляет "нормальный" сетевой трафик; на его основе разрабатываются наборы моделей, которые обновляются с течением времени. Затем эти модели применяются для нового трафика, и трафик, который не соответствует шаблону "нормального" трафика, отмечается как подозрительный (аномальный). AD-IDS являются привлекательными по своей концепции, но они требуют предварительного обучения. Однако реальность такова, что очень трудно классифицировать "нормальный" трафик. И это грустно. Поскольку сети со временем становятся достаточно крупными, число приложений, установленных в них, становится настолько большим и они настолько сложны, что сеть выглядит хаотичной. Хакер может анализировать и генерировать трафик для того, чтобы получить шаблон "нормального" трафика. Так что, рано или поздно, атака будет выглядеть как "нормальный" трафик и сможет пройти для IDS незамеченной. Если IDS является консервативной относительно составных частей атаки, она будет иметь тенденцию генерировать большое количество "false positives" - ложных предупреждений об опасности. Рано или поздно сообщения системы обнаружения атак начнут игнорировать.

По-прежнему в области аномального обнаружения проводятся обширные исследования. Обещается появление новых средств, включая объединение анализа защиты с методами визуализации и анализа данных. Однако по прошествии времени, кажется, что AD-IDS не являются той "серебряной пулей", которая может решить проблему. Поэтому многие коммерческие фирмы реализуют более простые и легкие в эксплуатации формы IDS, называемые "системами обнаружения злоупотреблений" (Misuse Detection Intrusion Detection Systems, MD-IDS).

MD-IDS сильно напоминают антивирусные системы, подключенные к сети. Обычно они содержат набор сигнатур, которые описывают типы соединений и трафика, которые указывают на то, что развертывается конкретная атака. Другие типы MD-IDS основаны на информации от хостов, например, из журналов регистрации операционной системы, для обнаружения событий, свидетельствующих о подозрительной деятельности.

Преимущества MD-IDS заметны сразу: быстрота, отсутствие "false positives". Слабая сторона MD-IDS заключается в том, что также как и сканеры вирусов, они не могут обнаружить того, о чем они не знают. К сожалению, атака, о которой не знают системные администраторы, это именно то, что они очень сильно хотели бы обнаружить. Для того чтобы поддерживать MD-IDS в рабочем состоянии, вам необходимо будет проводить постоянные обновления ее базы данных сигнатур за счет какого-нибудь поставщика, который содержит и платит стабильную зарплату прирученным хакерам. Но даже в этом случае можно по-прежнему оставаться уязвимым к атакам, которых пока еще никто не видел. Кроме того, как это ни прискорбно, хакер довольно легко скрывает следы атаки, дурача MD-IDS путем использования трюков вроде вставки пробела в поток данных, тем самым, изменяя сигнатуру атаки.

## Методы обнаружения

Контроль системы не имеет никакого смысла без последующего анализа полученной информации. Крайне важная характеристика системы обнаружения вторжений, — то, как она анализирует накопленные ею данные.

Существует две основные категории методов обнаружения вторжений: обнаружение аномалий и обнаружение злоупотреблений.

## Обнаружение аномалий

Обнаружение аномалий использует модели предполагаемого поведения пользователей и приложений, интерпретируя отклонение от «нормального» поведения как потенциальное нарушение защиты.

Основной постулат обнаружения аномалий состоит в том, что атаки отличаются от нормального поведения. Скажем, определенную повседневную активность пользователей (ее тип и объем) можно смоделировать достаточно точно. Допустим, конкретный пользователь обычно регистрируется в системе около десяти часов утра, читает электронную почту, выполняет транзакции баз данных, уходит на обед около часа дня, допускает незначительное количество ошибок при доступе к файлам и так далее. Если система отмечает, что тот же самый пользователь зарегистрировался в системе в три часа ночи, начал использовать средства компиляции и отладки и делает большое количество ошибок при доступе к файлам, она пометит эту деятельность как подозрительную.

Главное преимущество систем обнаружения аномалий заключается в том, что они могут выявлять ранее неизвестные атаки. Определив, что такое «нормальное» поведение, можно обнаружить любое нарушение, вне зависимости от того, предусмотрено оно моделью потенциальных угроз или нет. В реальных системах, однако преимущество обнаружения ранее неизвестных атак сводится на нет большим количеством ложных тревог. К тому же, системы обнаружения аномалий трудно настроить корректным образом, если им приходится работать в средах, для которых характерна значительная изменчивость.

## Обнаружение злоупотреблений

Системы обнаружения злоупотреблений, по существу, определяют, что идет не так, как должно. Они содержат описания атак («сигнатуры») и ищут соответствие этим описаниям в проверяемом потоке данных, с целью обнаружить проявление известной атаки. Одна из таких атак, к примеру, возникает, если кто-то создает символьную ссылку на файл паролей ОС Unix и выполняет привилегированное приложение, которое обращается по этой символьной ссылке. В данном примере атака основана на отсутствии проверки при доступе к файлу.

Основное преимущество систем обнаружения злоупотреблений состоит в том, что они сосредотачиваются на анализе проверяемых данных и обычно порождают очень мало ложных тревог.

Главный недостаток систем обнаружения злоупотреблений связан с тем, что они могут определять только известные атаки, для которых существуют определенная сигнатура. По мере обнаружения новых атак разработчики должны строить соответствующие им модели, добавляя их к базе сигнатур.

## Ответные действия: после вторжения

Ответные действия системы вторжений — это ее реакция на обнаруженную проблему. Ответные шаги могут осуществляться в разной форме; самая распространенная среди них — генерация предупреждения, которая описывает обнаруженное вторжение. Существуют также более активные ответные действия, такие как отправка сообщения на пейджер системного администратора, включение сирены или даже организация контратаки.

Контратака может включать в себя изменение конфигурации маршрутизатора с тем, чтобы блокировать адрес атакующего или даже организовать ответное нападение на подозреваемого. Активные ответные действия — весьма рискованная мера, поскольку они могут обрушиться на совершенно неповинных людей. Скажем, хакер может атаковать сеть с помощью фальсифицированного трафика, как будто бы направляемого с определенного адреса, но на самом деле генерируемого в некотором другом месте. Если система обнаружения вторжений выявит атаку и изменит конфигурацию сетевых маршрутизаторов, для того чтобы блокировать трафик, получаемый с данного адреса, по существу, это будет означать организацию атаки типа «отказ в обслуживании» (denial of service — DoS) против того сайта, за который выдает себя хакер.

## Открытые вопросы

Хотя за последние годы технология обнаружения вторжений развивалась очень быстро, многие важные вопросы до сих пор остаются открытыми. Во-первых, системы обнаружения должны стать более эффективными, научившись выявлять широкий диапазон атак с минимальным количеством ложных тревог. Во-вторых, методы обнаружения вторжений должны развиваться с учетом роста размера, скорости и динамизма современных сетей. Наконец, необходимы методы анализа, которые поддерживают идентификацию атак, направленных против сетей в целом.

## Эффективность системы

Основная задача увеличения эффективности состоит в разработке системы, которая способна определять почти 100% атак с минимальным количеством ложных тревог. Пока мы далеки от достижения этой цели.

Современные системы обнаружения вторжений, в основном, базируются на методах выявления злоупотреблений. Свободно распространяемая система Snort и коммерческое решение ISS RealSecure — вот два продукта, которые используют сигнатуры для анализа сетевого трафика. Поскольку они моделируют только известные атаки, разработчикам приходится регулярно обновлять свой набор сигнатур. Такой подход недостаточно эффективен. Необходимо научиться с помощью инструментария обнаружения аномалий выявлять новые виды атак, но при этом избежать свойственного этому подходу большого числа ложных тревог. Многие исследователи высказываются за использование смешанного подхода, сочетающего в себе возможности обнаружения аномалий и обнаружения злоупотреблений, но для этого необходимы дальнейшие исследования.

##

## Производительность

Просто определять атаки недостаточно. Системы обнаружения вторжений должны иметь возможность анализировать поток входных событий, генерируемых высокоскоростными сетями и высокопроизводительными компьютерами, которые стоят в узлах сети.

Сети Gigabit Ethernet используются повсеместно, растет популярность быстрых оптических каналов. Связанные сетями компьютеры также становятся быстрее, обрабатывают все больше данных и генерируют все более объемные журналы регистрации. Это возвращает нас к проблеме, которую когда-то вынуждены были решать системные администраторы, сталкивавшиеся с огромными объемами информации. Существует два способа анализа такого количества информации в реальном времени: разделение потока событий или использование периферийных сетевых датчиков.

При первом подходе модуль-«секатор» (slicer) расщепляет поток событий на более управляемые потоки меньшего размера, которые датчики обнаружения вторжений могут анализировать в реальном времени. Для этого доступ ко всему потоку событий должен осуществляться в одном месте. В силу этого исследователи обычно рекомендуют использовать разделение событий в централизованных системах или на сетевых шлюзах.

Недостаток такого подхода состоит в том, что «секатор» должен делить поток событий таким образом, чтобы гарантировать выявление всех соответствующих сценариев атак. Если поток событий делится произвольным образом, датчики могут не получить необходимые данные для обнаружения вторжения, поскольку различные части проявления атаки могут оказаться в разных фрагментах потока событий.

Второй подход состоит в развертывании множества датчиков на периферии сети, близко к хостам, которые должна защищать система. Этот подход предполагает, что при переносе анализа на периферию сети возникает естественное разделение трафика.

Недостаток такого подхода состоит в том, что развертывать широко распределенный набор датчиков, а затем управлять им достаточно трудно. Во-первых, корректное размещение датчиков может оказаться довольно сложным делом. Атаки, которые зависят от сетевой топологии (например, атаки, основанные на маршрутизации и фальсификации соединений), требуют, чтобы датчики устанавливались в определенных позициях сети. Во-вторых, существуют серьезные вопросы управления и координации. Сети — это весьма динамичные конструкции, которые развиваются во времени, как и их потенциальные угрозы. Новые виды атак появляются чуть ли не ежедневно; инфраструктура датчиков должна развиваться соответствующим образом.

## Анализ в масштабе всей сети

Установка датчиков в критических для работы сети местах позволяет администраторам выявлять атаки против сети в целом. Другими словами, сеть, оснащенная датчиками, может дать интегрированную, полную картину состояния сетевой защиты. Атаки, которые представляются невинными действиями в рамках одного хоста, могут оказаться крайне опасными в масштабах всей сети.

Рассмотрим, к примеру, атаку, которая ведется в несколько этапов. Пусть каждый этап осуществляется на своем хосте, но, поскольку атакуемая система поддерживает разделяемую файловую систему, эффект проявится во всей сети. Система может оказаться не в состоянии выявить каждый этап злонамеренных действий при анализе информации с одного датчика, однако более развернутый анализ сетевой активности должен позволить выявить признаки атаки. Эта корреляция или объединение предупреждений — идентификация шаблонов вторжения на основе группы сигналов датчиков — является одной из самых сложных проблем в современных системах обнаружения вторжений.

## Уведомления о взломе

Благодаря использованию метода, который называется "уведомления о взломе" ("burglar alarms"), IDS может предоставить полезное и надежное уведомление об определенных классах инцидентов безопасности. Для того чтобы понять, как работают уведомления о взломе, рассмотрим, как они применяются в "реальном мире". Рассмотрим простой пример. В доме есть сигнализация, которая проводит в жизнь простую политику безопасности: когда хозяина нет дома, никто не должен проникнуть через двери или окна, и никто не должен разбить стекла. Более того, в доме есть несколько скрытых датчиков, размещенных в наиболее важных местах. Когда хозяина нет дома, никто не должен пройти через дверь невредимым. Опираясь на эту образную политику, можно спроектировать систему уведомления о взломе на основе датчиков на окнах и дверях, детекторов разбитого стекла и некоторых поддельных датчиках. Можно ещё добавить требование, что никто не должен передвигаться внутри дома, когда хозяина там нет. Другой дом может иметь отличающуюся политику безопасности. В этом и заключается секрет: система уведомления о взломе - это IDS, которая опирается на понимание сети и того, что не должно происходить внутри нее.

Удивительно, но одним из самых лучших инструментов для построения системы обнаружения атак с уведомлением о взломе (burglar alarm intrusion detection system) является MD-IDS. Сетевому администратору надо сесть и описать, опираясь на свои знания сети, какого типа события он хочет отслеживать. Затем настроить MD-IDS на обнаружение и уведомление о них. Например, предположим, что сеть находится за межсетевым экраном (МСЭ), который блокирует IP трафик из Internet: надо проанализировать его и отправьте уведомление, если диапазон внешних IP-адресов из Internet виден в локальной сети. Предположим, что МСЭ не позволяет проходить какому-либо трафику, за исключением E-mail (SMTP), новостей USENET (NNTP) и запросов к DNS-серверу: установите MD-IDS, чтобы она начинала выдавать уведомления, если через МСЭ все же устанавливаются какие-либо соединения с внутренними системами для других, отличных от разрешенных, сервисов.

Вероятно наиболее мощная способность IDS с уведомлением о взломе состоит в том, что они действуют неожиданно для хакера. Администратор знаете свою сеть, а они нет. Если они проникли внутрь, им необходимо изучить сеть для того, чтобы эффективно реализовать свои атаки. Также как и взломщик, который может открыть несколько чуланов и шкафов в поисках денег или ювелирных изделий, сразу же после того, как он проник за охраняемый периметр, хакер будет сканировать сеть в поисках систем, которые стоит атаковать, или шлюзов к другим сетям. Поиск попыток внутреннего сканирования - эффективный способ обнаружения хакера. Большинство хакеров не ожидают встретить достойной обороны, - они проникают внутрь и полагают, что как только они прошли МСЭ, то их уже никто не видит. IDS с уведомлением о взломе разрушает это предположение и, что также является многообещающим, хакер будет ступать по виртуальному минному полю, как только он проникнет за периметр защиты.

Вероятно, большинство IDS в настоящее время развертываются не как системы обнаружения вторжения (Intrusion Detection Systems), а как системы обнаружения атак (Attack Detection Systems, ADS). Обнаружение атак представляет парадокс: если администратор знает, что конкретная атака существует, и блокируете ее, зачем ему заботиться о том, что кто-то пытается использовать ее против него?

Фактор, заставляющий сетевых администраторов использовать MD-IDS в ADS режиме - обычное любопытство. Интересно в короткий промежуток времени успеть задокументировать частоту и уровень атак, которым подверглась сеть. Но $10000 и больше - это куча денег, которую придется потратить на это сомнительное удовольствие. Инструменты аудита также управляют рынком MD-IDS - если аудит сети проводится экспертами в области защиты, вы будете раскритикованы, если их операции по тестированию и проникновению не будут обнаружены. Поскольку многие аудиторы используют широкий спектр автоматизированных средств анализа защищенности типа "Internet Scanner" от компании Internet Security Systems. Inc. или "CyberCop Scanner" от компании "Network Associates", то существует возможность немедленной, эмоциональной расплаты, если у администратора есть ADS, которая обнаруживает сканирование.

Теоретически, ADS вас будет предупреждать и повышать бдительность администратора в течение определенного периода времени, повышая его шансы в обнаружении и противодействии реальной атаке. Это является выгодным, поскольку хакер является достаточно "вежливым", чтобы предупредить администратора запуском программы SATAN против сети, прежде чем он запустит реальную атаку.

Маркус Ранум (Marcus Ranum) - CEO из Network Flight Recorder, Inc., работает в фирме, специализирующейся на ПО для анализа сетевого трафика. В 1991 году он создал первый коммерческий Internet-продукт - межсетевой экран, и впоследствии разработал и внедрил несколько других значительных систем защиты, включая комплект инструментов TIS Firewall, TIS Gauntlet и Whitehouse.gov. Маркус часто выступает с лекциями на конференциях и дает консультации как аналитик по сетевой защите промышленного применения.

Маркус Ранум построил свою первую защищенную и важную Internet-систему в 1991 году, как часть Internet-шлюза крупной корпорации. Программное обеспечение на межсетевом шлюзе имело большое количество довольно элементарных систем уведомления о взломе, но даже в 1991 году тревоги раздавались приблизительно два раза в неделю. Уведомления были коварными и появлялись только после того, как система уже была взломана до определенной степени. Он обычно прослеживал атаки и часто вылавливал хакеров. Процесс отслеживания атаки и документирование инцидента занимал примерно 4 часа на каждую атаку. Конечно, его усилия не сыграли особой роли, потому что по мере увеличения количества пользователей сети Интернет, увеличилось и количество атак. В конце концов, Маркус Ранум понял, что если работать "по старинке", то это займет приблизительно 16 часов в неделю. Поскольку он создавал эту систему, то знал, что она может противостоять атакам, которые были обнаружены. По сути, Маркус ничего не достиг в том, что касается его времени, потому что ему приходилось выполнять функции суррогатного родителя для кучи плохо подготовленных выпускников высших учебных заведений. Следующее поколение его систем уведомления о взломе было настроено на автоматическое выполнение определенных процедур, когда возникали ситуации, которые, как он считал, никогда не должны были происходить.

Многие организации, которые в настоящее время не обнаруживают и не учитывают атаки, не осознают, что их ждет неприятный сюрприз, когда они проинсталлируют IDS или ADS. Они обнаружат, что даже когда они знают, что атака запущена, не существует эффективных способов противодействия, которые они могли бы применить против нее. Сегодня нельзя полагаться на адрес, из которого, как видно, происходит атака. Он может принадлежать безвредному "парню, чей компьютер уже скомпрометировали". Даже если знать, откуда происходит атака, то почти всегда оказывается, что она идет от пользователя, чей пароль был украден, или с адреса, который был зарегистрирован по украденной кредитной карточке. Полное отслеживание такой атаки - это отвратительно долгая по времени и сложности задача, которая связана с публичным доступом.

По-прежнему, наиболее эффективным по стоимости методом будет просто перестать гоняться за хакерами и вернуться к работе. Но зачем тогда нужно обнаруживать атаку, если администратор знает, что ничего не сможет сделать против нее?

## Что делать?

К сожалению, "серебряной пули" не существует. Понимая ограничения и возможности IDS, можно эффективно использовать их. Для того, чтобы IDS работали наилучшим образом, необходимо сесть и составить перечень всех типов событий, которые администратор знает и которые могут вызвать серьезные проблемы в сети, затем настроить систему, чтобы она могла видеть их. Количество атак во внутренней сети должно быть очень небольшим, и будет исходить либо от аудиторов, либо от хакеров, которые каким-то образом пробрались через защиту периметра. В самом худшем, хотя и вполне возможном случае, можно обнаружить сотрудников, которые запускают атаки против внешних серверов в сети Интернет.

Что касается сети Internet, то средства защиты улучшается с большой скоростью. Современное поколение IDS - это только начало. В будущем мы увидим, что IDS комбинирует обнаружение аномалий и обнаружение злоупотреблений, и, будем надеяться, что они будут гладко интегрироваться с МСЭ и другими системами защиты.

## Заключение

Даже по мере того, как защита сетей становится все надежнее, обнаружение аномалий всегда останется неотъемлемой частью любой серьезной системы безопасности. Сложившаяся сейчас тенденция к установке распределенных и специализированных датчиков приведет к появлению систем, состоящих из сотен, возможно даже тысяч датчиков, подключенных к сети с помощью инфраструктуры, которая поддерживает связь, контроль или изменение конфигурации. Хотя тип и характеристики данной инфраструктуры могут варьироваться, все они должны иметь возможность масштабироваться в очень больших пределах. Кроме того, процедура анализа, в конечном итоге, будет перенесена с низкоуровневых датчиков на высокоуровневые анализаторы, которые предоставят администраторам более полную и точную картину событий, важных для безопасности сети в целом.

В ближайшем будущем технология датчиков будет интегрирована в повседневную вычислительную среду. Нечто похожее произошло с межсетевыми экранами, которые теперь являются неотъемлемой частью операционных систем: и Unix, и Windows снабжены функциональностью, характерной для межсетевых экранов на базе хостов. Теперь настало время, когда операционные системы и сетевое программное обеспечение должны интегрировать датчики обнаружения вторжений. Обнаружение вторжений, без сомнения, станет обязательной функцией.

Повсеместная, распределенная сеть может быть развернута, если только есть возможность интегрировать различные виды датчиков, работающих на разных платформах, в разных средах и операционных системах. В силу этого необходимы стандарты, которые обеспечат интероперабельность. Первый шаг в этом направлении — стандарт Intrusion Detection Message Exchange Format, предложенный рабочей группой Intrusion Detection Working Group в составе Internet Engineering Task Force. IDMEF определяет формат предупреждений и протокол обмена предупреждениями. Необходимо предпринять дополнительные усилия, чтобы сформировать так называемую онтологию, которая позволит датчикам достигнуть соглашения по интерпретации воспринимаемой ими информации. Без такого общего способа описания используемых объектов датчики по-прежнему будут по-разному трактовать данные при обнаружении одного и того же вторжения.

По мере развития программных технологий обнаружения вторжений они могут трансформироваться в технологию датчиков, реализуемых аппаратно. Новые виды распределенных датчиков могут одновременно открыть новые направления в области обнаружения вторжений. Возможно, когда-нибудь наша оснащенная датчиками одежда будет способна выявлять вора-карманника. Перспективы эти исключительно заманчивы, если не безграничны.

## Список используемой литературы:

1. Люцарев B.C., Ермаков К.В., Рудный Е.Б., Ермаков И.В. Безопасность компьютерных сетей на основе Windows NT. — Москва, Русская редакция. — 1998.

2. C. Ko, M. Ruschitzka, K. Levitt, «Execution Monitoring of Security-Critical Programs in Distributed Systems: A Specification-Based Approach», Proc. 1997

3. Хуотаринен А.В., Щеглов А.Ю. Технология физической защиты сетевых устройству/Экономика и производство. — №4. — 2002.

4. Щеглов А.Ю.Дарасюк М.В., Оголюк А.А. Технология защиты рабочих станций в сетевых архитектурах клиент-сервер//ВУТЕ. Россия — №1 — 2000.

## Список использованных Интернет-ресурсов:

http://www.uran.donetsk.ua/~masters/2004/fvti/zlatokrilets/library/source1.htm http://zerokool.vistcom.ru/ids.html