12. Лекция: Обнаружение вторжений

Лекция посвящена вопросам обнаружения вторжений. Рассмотрены основные типы систем обнаружения вторжений и датчиков вторжений. Уделено внимание вопросам установки, управления IDS и предотвращения вторжений посредством их.

Обнаружение вторжений - это еще одна задача, выполняемая сотрудниками, ответственными за безопасность информации в организации, при обеспечении защиты от атак. Обнаружение вторжений - это активный процесс, при котором происходит обнаружение хакера при его попытках проникнуть в систему. В идеальном случае такая система лишь выдаст сигнал тревоги при попытке проникновения. Обнаружение вторжений помогает при превентивной идентификации активных угроз посредством оповещений и предупреждений о том, что злоумышленник осуществляет сбор информации, необходимой для проведения атаки. В действительности, как будет показано в материале лекции, это не всегда так. Перед обсуждением подробностей, связанных с обнаружением вторжений, давайте определим, что же это в действительности такое.

Системы обнаружения вторжений (IDS) появились очень давно. Первыми из них можно считать ночной дозор и сторожевых собак. Дозорные и сторожевые собаки выполняли две задачи: они определяли инициированные кем-то подозрительные действия и пресекали дальнейшее проникновение злоумышленника. Как правило, грабители избегали встречи с собаками и, в большинстве случае, старались обходить стороной здания, охраняемые собаками. То же самое можно сказать и про ночной дозор. Грабители не хотели быть замеченными вооруженными дозорными или охранниками, которые могли вызвать полицию.

Сигнализация в зданиях и в автомобилях также является разновидностью системы обнаружения вторжений. Если система оповещения обнаруживает событие, которое должно быть замечено (например, взлом окна или открытие двери), то выдается сигнал тревоги с зажиганием ламп, включением звуковых сигналов, либо сигнал тревоги передается на пульт полицейского участка. Функция пресечения проникновения выполняется посредством предупреждающей наклейки на окне или знака, установленного перед домом. В автомобилях, как правило, при включенной сигнализации горит красная лампочка, предупреждающая об активном состоянии системы сигнализации.

Все эти примеры основываются на одном и том же принципе: обнаружение любых попыток проникновения в защищенный периметр объекта (офис, здание, автомобиль и т. д.). В случае с автомобилем или зданием периметр защиты определяется относительно легко. Стены строения, ограждение

вокруг частной собственности, двери и окна автомобиля четко определяют защищаемый периметр. Еще одной характеристикой, общей для всех этих случаев, является четкий критерий того, что именно является попыткой проникновения, и что именно образует защищаемый периметр.

Если перенести концепцию системы сигнализации в компьютерный мир, то получится базовая концепция системы обнаружения вторжений. Необходимо определить, чем в действительности является периметр защиты компьютерной системы или сети. Очевидно, что периметр защиты в данном случае - это не стена и не ограждение. Периметр защиты сети представляет собой виртуальный периметр, внутри которого находятся компьютерные системы. Этот периметр может определяться межсетевыми экранами, точками разделения соединений или настольными компьютерами с модемами. Данный периметр может быть расширен для содержания домашних компьютеров сотрудников, которым разрешено соединяться друг с другом, или партнеров по бизнесу, которым разрешено подключаться к сети. С появлением в деловом взаимодействии беспроводных сетей периметр защиты организации расширяется до размера беспроводной сети.

Сигнализация, оповещающая о проникновении грабителя, предназначена для обнаружения любых попыток входа в защищаемую область, когда эта область не используется. Система обнаружения вторжений IDS предназначена для разграничения авторизованного входа и несанкционированного проникновения, что реализуется гораздо сложнее. Здесь можно в качестве примера привести ювелирный магазин с сигнализацией против грабителей. Если кто-либо, даже владелец магазина, откроет дверь, то сработает сигнализация. Владелец должен после этого уведомить компанию, обслуживающую сигнализацию, о том, что это он открыл магазин, и что все в порядке. Систему IDS, напротив, можно сравнить с охранником, следящим за всем, что происходит в магазине, и выявляющим несанкционированные действия (как, например, пронос огнестрельного оружия). К сожалению, в виртуальном мире "огнестрельное оружие" очень часто остается незаметным.

Вторым вопросом, который необходимо принимать в расчет, является определение того, какие события являются нарушением периметра безопасности. Является ли нарушением попытка определить работающие компьютеры? Что делать в случае проведения известной атаки на систему или сеть? По мере того как задаются эти вопросы, становится понятно, что найти ответы на них не просто. Более того, они зависят от других событий и от состояния системы-цели.

Определение типов систем обнаружения вторжений

Существуют два основных типа IDS: узловые (HIDS) и сетевые (NIDS). Система HIDS располагается на отдельном узле и отслеживает признаки атак на данный узел. Система NIDS находится на отдельной системе, отслеживающей сетевой трафик на наличие признаков атак, проводимых в подконтрольном сегменте сети. На рисунке 12.1 показаны два типа IDS, которые могут присутствовать в сетевой среде.

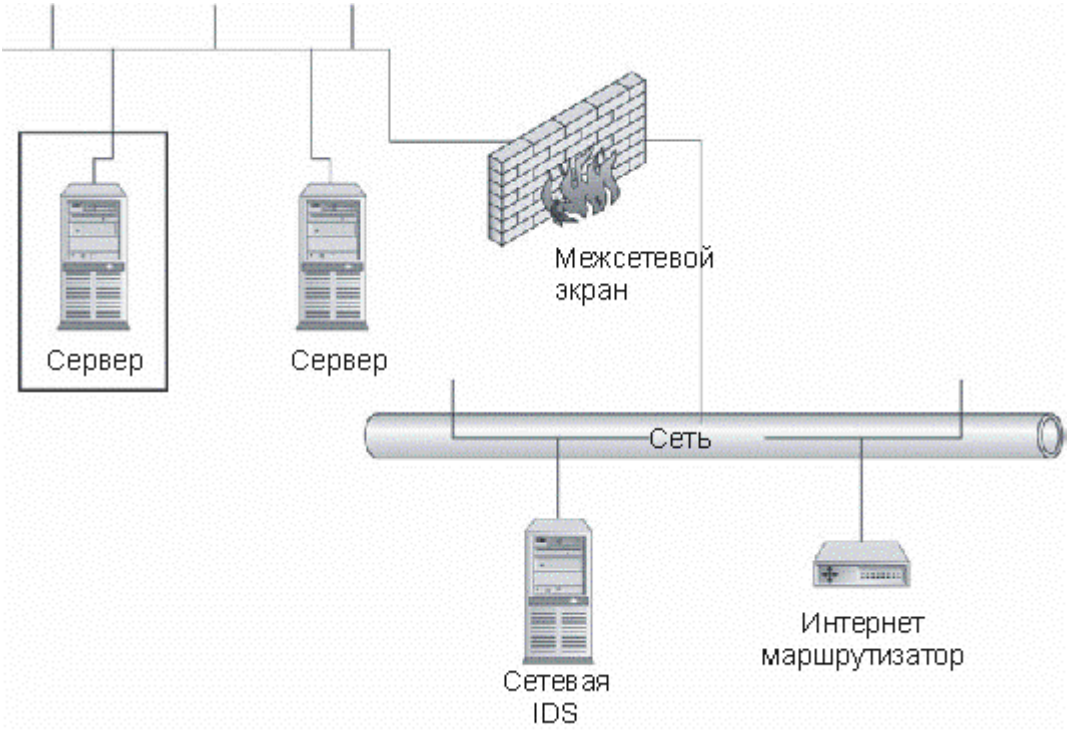

Рис. 12.1. Примеры размещения IDS в сетевой среде

Узловые IDS

Узловые IDS (HIDS) представляют собой систему датчиков, загружаемых на различные сервера организации и управляемых центральным диспетчером. Датчики отслеживают различные типы событий (более детальное рассмотрение этих событий приводится в следующем разделе) и предпринимают определенные действия на сервере либо передают уведомления. Датчики HIDS отслеживают события, связанные с сервером, на котором они загружены. Сенсор HIDS позволяет определить, была ли атака успешной, если атака имела место на той же платформе, на которой установлен датчик.

Как будет показано далее, различные типы датчиков HIDS позволяют выполнять различные типы задач по обнаружению вторжений. Не каждый тип датчиков может использоваться в организации, и даже для различных серверов внутри одной организации могут понадобиться разные датчики. Следует заметить, что система HIDS, как правило, стоит дороже, чем сетевая

система, так как в этом случае каждый сервер должен иметь лицензию на датчик (датчики дешевле для одного сервера, однако общая стоимость датчиков больше по сравнению со стоимостью использования сетевых IDS).

С использованием систем HIDS связан еще один вопрос, заключающийся в возможностях процессора на сервере. Процесс датчика на сервере может занимать от 5 до 15 % общего процессорного времени. Если датчик работает на активно используемой системе, его присутствие отрицательно скажется на производительности и, таким образом, придется приобретать более производительную систему.

Примечание

Вероятно возникновение разногласий, связанных с управлением и настройкой, между администраторами безопасности (управляющими работой IDS) и системными администраторами. Так как процесс должен постоянно находиться в активном состоянии, необходима хорошая координация в их работе.

Существует пять основных типов датчиков HIDS.

- Анализаторы журналов.
- Датчики признаков.
- Анализаторы системных вызовов.
- Анализаторы поведения приложений.
- Контролеры целостности файлов.

Следует заметить, что количество датчиков HIDS увеличивается, и некоторые продукты предлагают функциональные возможности, предусматривающие использование датчиков более чем пяти основных видов.

Анализаторы журналов

Анализатор журнала представляет собой именно то, что отражает само название датчика. Процесс выполняется на сервере и отслеживает соответствующие файлы журналов в системе. Если встречается запись журнала, соответствующая некоторому критерию в процессе датчика HIDS, предпринимается установленное действие.

Большая часть анализаторов журналов настроена на отслеживание записей журналов, которые могут означать событие, связанное с безопасностью системы. Администратор системы, как правило, может определить другие записи журнала, представляющие определенный интерес.

Анализаторы журналов по своей природе являются реактивными системами. Иными словами, они реагируют на событие уже после того, как оно произошло. Таким образом, журнал будет содержать сведения о том, что проникновение в систему выполнено. В большинстве случаев анализаторы журналов не способны предотвратить осуществляемую атаку на систему.

Анализаторы журналов, в частности, хорошо адаптированы для отслеживания активности авторизованных пользователей на внутренних системах. Таким образом, если в организации уделяется внимание контролю за деятельностью системных администраторов или других пользователей системы, можно использовать анализатор журнала для отслеживания активности и перемещения записи об этой активности в область, недосягаемую для администратора или пользователя.

Датчики признаков

Датчики этого типа представляют собой наборы определенных признаков событий безопасности, сопоставляемых с входящим трафиком или записями журнала. Различие между датчиками признаков и анализаторами журналов заключается в возможности анализа входящего трафика.

Системы, основанные на сопоставлении признаков, обеспечивают возможность отслеживания атак во время их выполнения в системе, поэтому они могут выдавать дополнительные уведомления о проведении злоумышленных действий. Тем не менее, атака будет успешно или безуспешно завершена перед вступлением в действие датчика HIDS, поэтому датчики этого типа считаются реактивными. Датчик признаков HIDS является полезным при отслеживании авторизованных пользователей внутри информационных систем.

Анализаторы системных вызовов

Анализаторы системных вызовов осуществляют анализ вызовов между приложениями и операционной системой для идентификации событий, связанных с безопасностью. Датчики HIDS данного типа размещают программную спайку между операционной системой и приложениями. Когда приложению требуется выполнить действие, его вызов операционной системы анализируется и сопоставляется с базой данных признаков. Эти признаки являются примерами различных типов поведения, которые являют собой атакующие действия, или объектом интереса для администратора IDS.

Анализаторы системных вызовов отличаются от анализаторов журналов и датчиков признаков HIDS тем, что они могут предотвращать действия. Если приложение генерирует вызов, соответствующий, например, признаку атаки на переполнение буфера, датчик позволяет предотвратить этот вызов и сохранить систему в безопасности.

Внимание!

Необходимо обеспечивать правильную конфигурацию датчиков этого типа, так как их некорректная настройка может вызывать ошибки в приложениях либо отказы в их работе. Такие датчики, как правило, обеспечивают возможность функционирования в тестовом режиме. Это означает, что датчик отслеживает события, но не предпринимает никаких блокирующих действий; этот режим можно использовать для тестирования конфигурации без блокировки работы легитимно используемых приложений.

Анализаторы поведения приложений

Анализаторы поведения приложений аналогичны анализаторам системных вызовов в том, что они применяются в виде программной спайки между приложениями и операционной системой. В анализаторах поведения датчик проверяет вызов на предмет того, разрешено ли приложению выполнять данное действие, вместо определения соответствие вызова признакам атак. Например, веб-серверу обычно разрешается принимать сетевые соединения через порт 80, считывать файлы в веб-каталоге и передавать эти файлы по соединениям через порт 80. Если веб-сервер попытается записать или считать файлы из другого места или открыть новые сетевые соединения, датчик обнаружит несоответствующее норме поведение сервера и заблокирует действие.

При конфигурировании таких датчиков необходимо создавать список действий, разрешенных для выполнения каждым приложением. Поставщики датчиков данного типа предоставляют шаблоны для наиболее широко используемых приложений. Любые "доморощенные" приложения должны анализироваться на предмет того, какие действия им разрешается выполнять, и выполнение этой задачи должно быть программно реализовано в датчике.

Контролеры целостности файлов

Контролеры целостности файлов отслеживают изменения в файлах. Это осуществляется посредством использования криптографической контрольной суммы или цифровой подписи файла. Конечная цифровая подпись файла будет изменена, если произойдет изменение хотя бы малой части исходного файла (это могут быть атрибуты файла, такие как время и дата создания). Алгоритмы, используемые для выполнения этого процесса, разрабатывались с целью максимального снижения возможности для внесения изменений в файл с сохранением прежней подписи.

При изначальной конфигурации датчика каждый файл, подлежащий мониторингу, подвергается обработке алгоритмом для создания начальной подписи. Полученное число сохраняется в безопасном месте. Периодически для каждого файла эта подпись пересчитывается и сопоставляется с

оригиналом. Если подписи совпадают, это означает, что файл не был изменен. Если соответствия нет, значит, в файл были внесены изменения.

Примечание

Работа датчика данного типа сильно зависит от качества контроля над конфигурацией. Если организация не осуществляет управление датчиком на должном уровне, то датчик, как правило, обнаруживает все типы изменений, вносимых в файл, которые, на самом деле, могут быть легитимными, но неизвестными датчику.

Контролер целостности файлов не осуществляет идентификацию атаки, а детализирует результаты проведенной атаки. Таким образом, в случае атаки на веб-сервер сама атака останется незамеченной, но будет обнаружено повреждение или изменение домашней страницы веб-сайта. То же самое относится и к другим типам проникновений в систему, так как в процессе многих из них осуществляется изменение системных файлов.

Вопрос к эксперту

Вопрос. Является ли в действительности контролер целостности файлов системой обнаружения вторжений?

Ответ. Хотя контролер целостности файлов не обнаруживает атаку как таковую, он обнаруживает изменения, являющиеся следствием этой атаки. В случае атаки все датчики IDS обнаруживают признаки атаки. Например, анализатор журналов обнаруживает записи журнала, которые могут означать атаку. Можно предположить, что атаку как таковую на самом деле обнаруживает система, работающая по принципу сопоставления признаков. Тем не менее, даже такие системы отслеживают действия или информацию, соответствующую признаку. Признак построен таким образом, что всякий элемент, соответствующий этому признаку, вероятнее всего является атакой.

Кроме всего прочего, здесь следует рассмотреть вопрос о том, что же такое "вторжение". В некоторых организациях вторжением могут считаться действия разработчика, изменяющего файлы без выполнения соответствующих процедур по контролю над конфигурацией.

Сетевые IDS

NIDS представляет собой программный процесс, работающий на специально выделенной системе. NIDS переключает сетевую карту в системе в неразборчивый режим работы, при котором сетевой адаптер пропускает весь сетевой трафик (а не только трафик, направленный на данную систему) в программное обеспечение NIDS. После этого происходит анализ трафика с использованием набора правил и признаков атак для определения того,

представляет ли этот трафик какой-либо интерес. Если это так, то генерируется соответствующее событие.

На данный момент большинство систем NIDS базируется на признаках атак. Это означает, что в системы встроен набор признаков атак, с которыми сопоставляется трафик в канале связи. Если происходит атака, признак которой отсутствует в системе обнаружения вторжений, система NIDS не замечает эту атаку. NIDS-системы позволяют указывать интересуемый трафик по адресу источника, конечному адресу, порту источника или конечному порту. Это дает возможность отслеживания трафика, не соответствующего признакам атак.

Примечание

На рынке начали появляться системы NIDS, базирующиеся на обнаружении аномалий. Эти системы осуществляют поиск аномалий в сетевом трафике для выявления атак. Полезность использования этих устройств на момент написания книги еще не доказана.

Чаще всего при применении NIDS используются две сетевые карты (см. рис. 12.2). Одна карта используется для мониторинга сети. Эта карта работает в "скрытом" режиме, поэтому она не имеет IP-адреса и, следовательно, не отвечает на входящие соединения.

У скрытой карты отсутствует стек протоколов, поэтому она не может отвечать на такие информационные пакеты, как пинг-запросы. Вторая сетевая карта используется для соединения с системой управления IDS и для отправки сигналов тревоги. Эта карта присоединяется ко внутренней сети, невидимой для той сети, в отношении которой производится мониторинг.

Рис. 12.2. Конфигурация NIDS с двумя сетевыми картами

Среди преимуществ использования NIDS можно выделить следующие моменты.

- NIDS можно полностью скрыть в сети таким образом, что злоумышленник не будет знать о том, что за ним ведется наблюдение.
- Одна система NIDS может использоваться для мониторинга трафика с большим числом потенциальных систем-целей.
- NIDS может осуществлять перехват содержимого всех пакетов, направляющихся на систему-цель.

Среди недостатков данной системы необходимо отметить следующие аспекты.

- Система NIDS может только выдавать сигнал тревоги, если трафик соответствует предустановленным правилам или признакам.
- NIDS может упустить нужный интересуемый трафик из-за использования широкой полосы пропускания или альтернативных маршрутов.
- Система NIDS не может определить, была ли атака успешной.
- Система NIDS не может просматривать зашифрованный трафик.
- В коммутируемых сетях (в отличие от сетей с общими носителями) требуются специальные конфигурации, без которых NIDS будет проверять не весь трафик.

Какой тип IDS лучше?

Является ли один из двух типов IDS более предпочтительным по сравнению с другим? Все зависит от обстоятельств. У устройств обоих типов есть свои преимущества и недостатки, как уже было показано в этой лекции. В то время как NIDS более эффективен с точки зрения стоимости (одна система NIDS осуществляет мониторинг трафика большого количества систем), HIDS больше подходит для организаций, в которых уделяется повышенное внимание отслеживанию работы штатных сотрудников. Иными словами, выбор типа устройства IDS зависит от первоочередных целей, которых необходимо достичь в сети организации.

Установка IDS

Чтобы использовать IDS по максимуму, необходимо провести большой объем процедур планирования перед непосредственной установкой устройства. Перед созданием соответствующей политики нужно осуществить сбор необходимой информации, провести анализ сети и реализовать задачи по управлению. Как в большинстве комплексных систем, политику необходимо создать, утвердить и протестировать перед применением. При создании политики IDS необходимо выполнить следующие шаги:

1. Определить цели создания IDS.
2. Выбрать объекты мониторинга.
3. Выбрать ответные действия.
4. Установить пороги.
5. Применить политику.

Определение целей применения IDS

Цели использования IDS определяют требования для политики IDS. Потенциально целями применения IDS являются следующие.

- Обнаружение атак.
- Предотвращение атак.
- Обнаружение нарушений политики.
- Принуждение к использованию политик.
- Принуждение к следованию политикам соединений.
- Сбор доказательств.

Имейте в виду, что цели использования устройства могут комбинироваться, и конкретные цели применения любой IDS зависят от организации. Набор целей ни в коем случае не ограничивается этим списком. IDS позволяет организации обнаруживать начало проведения атаки и осуществлять сбор доказательств или предотвращение дополнительного повреждения посредством устранения аварийных ситуаций. Разумеется, это не единственная цель, для достижения которой применяется IDS. Так как IDS осуществляет сбор детализованной информации по многим событиям,

происходящим в сети и на компьютерах организации, она также может идентифицировать действия, нарушающие политику, и реальный уровень использования сетевых ресурсов.

Распознавание атак

Распознавание атак является одной из главных целей использования IDS. Система IDS запрограммирована на поиск определенных типов событий, которые служат признаками атак. В качестве простого примера приведем соединение через TCP-порт 80 (HTTP), за которым следует URL, содержащий расширение .bat. Это может быть признаком того, что злоумышленник пытается использовать уязвимость на веб-сервере IIS.

Большую часть атак идентифицировать не просто. Например, до сих пор в интернете широко распространены атаки с угадыванием пароля. Система HIDS может содержать правило, согласно которому после трех неудачных попыток входа через короткие промежутки времени вход в данную учетную запись блокируется. Для этого HIDS должна отслеживать время и число неудачных попыток входа на каждой учетной записи, фиксируемой в журнале, и сбрасывать счетчик в случае успешного входа или истечения времени.

Еще более сложным примером распознавания атак является ситуация, когда злоумышленник пытается угадать пароли на нескольких учетных записях и системах. В данном случае атакующий не будет пробовать войти в одну и ту же учетную запись дважды за короткий промежуток времени, а попытается использовать этот пароль в каждой учетной записи. Если время каждой попытки достаточно велико, счетчики на отдельных учетных записях будут сбрасываться, перед тем как злоумышленник трижды осуществит неудачный вход в систему с использованием данной учетной записи. Единственным способом выявить такую атаку является сопоставление информации из журналов различных систем. Такой анализ осуществляет система HIDS, способная сопоставлять информацию с нескольких компьютеров.

Мониторинг политики

Мониторинг политики - это менее заметный аспект деятельности по обнаружению атак. Целью системы IDS, настроенной на отслеживание политики, является отслеживание выполнения или невыполнения политики организации. В самом простом случае NIDS можно настроить на отслеживание всего веб-трафика вне сети. Такая конфигурация позволяет отслеживать любое несоответствие политикам использования интернета. Если в системе сконфигурирован список веб-сайтов, не отвечающий веб-стандартам корпоративного использования, NIDS зафиксирует любые подключения к таким сайтам.

Система NIDS также проверяет соответствие конфигурациям маршрутизатора или межсетевого экрана. В этом случае NIDS настраивается на отслеживание трафика, который не должен проходить через маршрутизатор или межсетевой экран. При обнаружении такого трафика определяется нарушение корпоративной политики межсетевых экранов.

Внимание!

Использование IDS для мониторинга политики может занять очень много времени и потребовать большого количества действий по конфигурированию.

Принуждение к использованию политики

Применение системы IDS в качестве средства принудительного использования политики выводит конфигурацию мониторинга политики на более высокий уровень. При отслеживании политики IDS настраивается на выполнение действий при нарушении политики. В первом примере в разделе "Мониторинг политики" IDS с принуждением к использованию политики не только определит попытку соединения с недоступным веб-сайтом, но и предпримет меры по предотвращению этого действия.

Обработка инцидента

Система IDS может оказаться полезной после обнаружения инцидента. В этом случае с помощью IDS можно собрать доказательства. NIDS можно настроить на отслеживание определенных соединений и ведение полноценного журнала по учету трафика. В то же время можно использовать и HIDS для фиксирования всех записей журнала для определенной учетной записи системы.

Выбор объекта мониторинга

Выбор объекта мониторинга зависит от целей, поставленных перед системой IDS, и от среды, в которой IDS будет функционировать. Например, если цель IDS заключается в обнаружении атак, и IDS расположена в интернете за пределами межсетевого экрана компании, то IDS потребуется отслеживать весь трафик, поступающий на межсетевой экран, для обнаружения входящих атак. В качестве альтернативы IDS можно разместить в пределах зоны, защищаемой межсетевым экраном, для определения только тех атак, которые успешно преодолели межсетевой экран. Исходящий трафик в данном случае может игнорироваться (см. рис. 12.3). В таблице 12.1 приводятся примеры объектов мониторинга при использовании конкретных политик.

Выбор объекта мониторинга определяет расположение датчиков. Датчики могут быть расположены вне межсетевого экрана, внутри сети, на системах с

секретной информацией или на системах, используемых специально для сбора и обработки данных журнала. Ключевым моментом, о котором необходимо помнить при вынесении решения по поводу размещения датчика IDS, является то, что датчик должен иметь возможность просмотра интересуемых событий, будь то сетевой трафик или записи журнала. Если интересуемые события не преодолевают межсетевой экран, то не рекомендуется размещать датчик NIDS в области, защищаемой межсетевым экраном. Аналогично, если интересуемые события фиксируются только на главном контроллере домена сети Windows NT, программное обеспечение HIDS должно быть расположено на главном контроллере домена, даже если злоумышленник физически располагается на рабочей станции внутри сети.

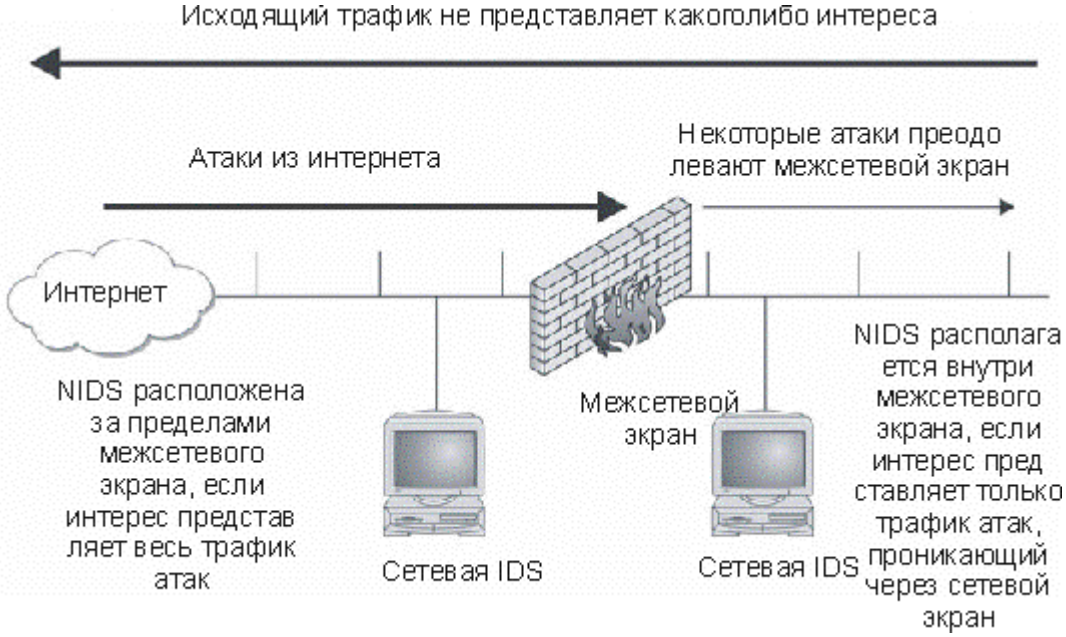

Рис. 12.3. Пример выбора объекта мониторинга

Таблица 12.1. Примеры информации, отслеживаемой при наличии политики IDS

Политика	NIDS	HIDS
Обнаружение атак	Весь трафик, поступающий на потенциально атакуемые системы (сетевые экраны, веб-серверы, серверы приложений и т.д.)	Неудачные попытки входа. Попытки соединения. Удачный вход с удаленных систем.
Предотвращение атак	То же, что и для обнаружения атак	То же, что и для обнаружения атак.
Обнаружение нарушений политики	Весь трафик HTTP, формируемый на системах клиентах. Весь трафик FTP, формируемый на системах клиентах	Успешные HTTP-соединения. Успешные FTP соединения. Загружаемые файлы.
Принуждение к использованию политик	То же, что и для обнаружения нарушений политики	То же, что и для обнаружения нарушения политики.

Принуждение к соответствию политикам соединений	Весь трафик, нарушающий принудительно используемую политику соединения	Успешные соединения с запрещенных адресов или по запрещенным портам.
Сбор доказательств	Содержимое всего трафика, формируемого на системе-цели или атакующей системе	Все успешные подключения, исходящие с атакующей системы. Все неудачные соединения с атакующих систем. Все нажатия клавиш из интерактивных сеансов на атакующих системах.

При размещении датчиков NIDS необходимо руководствоваться еще одним ключевым правилом. Если в сети используются коммутаторы вместо концентраторов, датчик NIDS не будет правильно работать, если он просто подключен к порту коммутатора. Коммутатор будет отправлять только трафик, направленный на датчик, к тому порту, к которому подключен датчик. В случае с коммутируемой сетью существуют два варианта использования датчиков NIDS: применение порта, отслеживающего коммутатор, или применение сетевого разветвителя. На рисунке 12.4 показаны конфигурации обоих типов.

При использовании порта может возникнуть конфликт с персоналом по обслуживанию сети из-за того, что этот порт может использоваться для разрешения проблем, возникающих в сети. Кроме этого, многие коммутаторы позволяют вести мониторинг (некоторыми производителями вместо этого слова используется термин "связывание") только одного порта единовременно. Порт мониторинга, как правило, не позволяет осуществлять мониторинг магистрали коммутатора. Эта функция не будет работать в любом случае, так как магистраль коммутатора передает данные со скоростью в несколько мегабит в секунду, и датчик NIDS использует соединение 100BaseT (скорость 100 мегабит в секунду). Такое соединение не позволяет осуществлять передачу данных NIDS, поэтому в данной конфигурации не представляется возможным прерывание соединений.

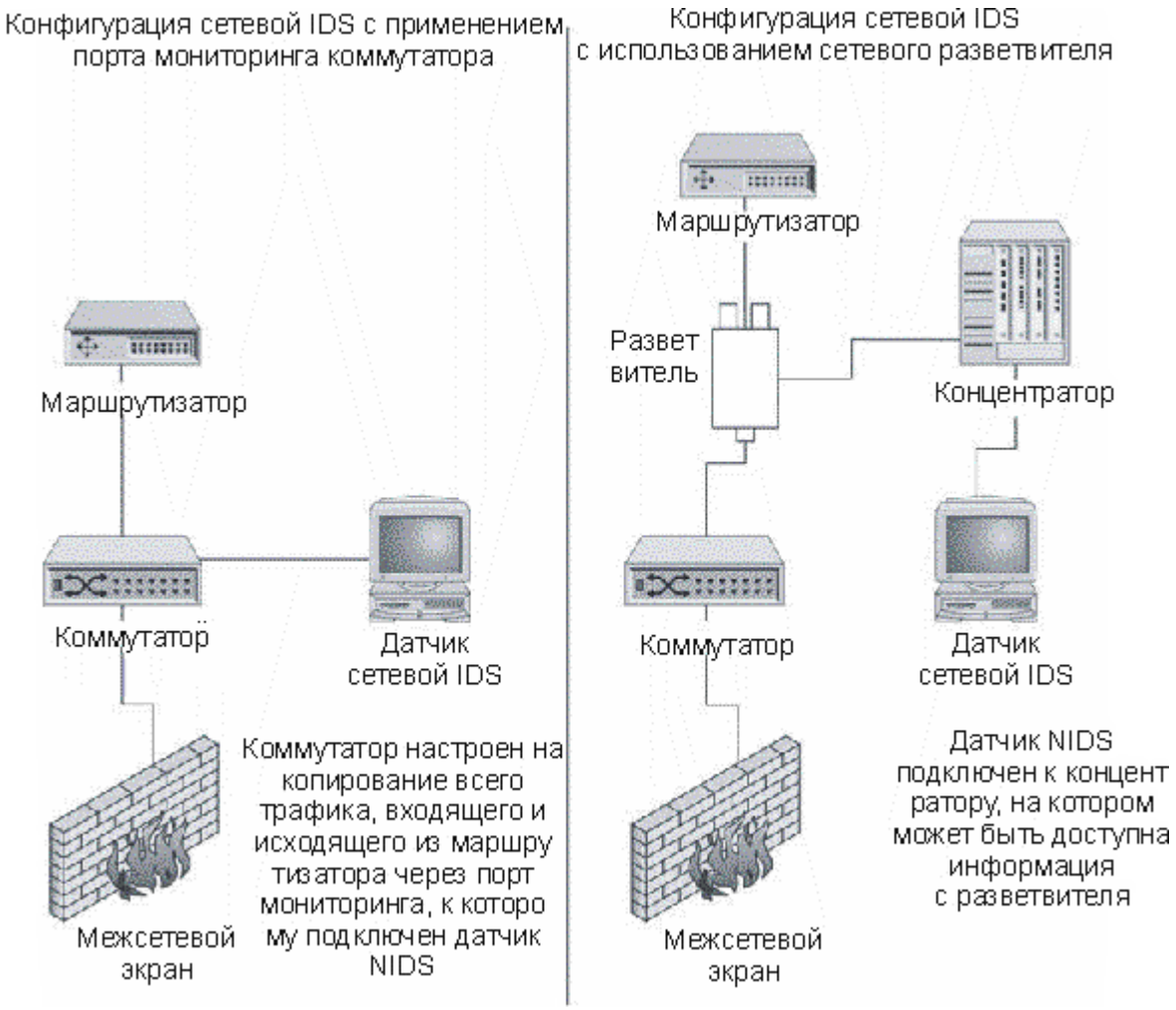

Рис. 12.4. Конфигурации датчика сетевой IDS для коммутируемой сети

Разветвители - это пассивные проводные соединения между двумя устройствами (например, между маршрутизатором и коммутатором). Как правило, разветвитель подключается к концентратору, к которому также подсоединен датчик NIDS. Это позволяет датчику отслеживать трафик.

Примечание

Разветвитель не позволяет датчику NIDS осуществлять передачу данных, поэтому в данной конфигурации прерывание соединений также недопустимо.

Выбор ответных действий

Аналогично выбору объекта мониторинга, выбор ответных действий зависит от целей, для которых используется система IDS. При возникновении события можно выбрать пассивную обработку (ответное действие, не препятствующее действиям атакующего) или активную обработку (ответное действие, препятствующее действиям злоумышленника). Пассивные ответные действия не обязательно подразумевают разрешение продолжения

события, но не допускают выполнение непосредственных операций самой системой IDS. Этот момент необходимо иметь в виду. Также следует взвешенно подойти к выбору автоматической или ручной обработки событий.

Пассивная обработка событий

Пассивная обработка - это наиболее распространенный тип действий, предпринимаемых при обнаружении вторжения. Причина этому проста - пассивные ответные действия обеспечивают меньшую вероятность повреждения легитимного трафика, являясь, в то же время, наиболее простыми для автоматического применения. Как правило, пассивные ответные действия осуществляют сбор большего числа информации или передают уведомления лицам, имеющим право на принятие более жестких мер.

Предотвращение. Предотвращение попытки атаки является сегодня наиболее широко используемым методом обработки события атаки. В большинстве случаев такой метод обработки событий остается установленным по умолчанию после установки в организации подключения к интернету и межсетевого экрана. В дальнейшем, после выполнения всех действий по настройке, организации доверяют защиту от атак из интернета межсетевым экранам.

Данный тип ответных действий может использоваться в более сложных системах IDS. IDS настраивается на игнорирование атак через несуществующие службы или службы, относительно которых межсетевой экран является неуязвимым.

Веским основанием для игнорирования атаки служит тот факт, что системы не чувствительны к рассматриваемому типу атак; например, это относится к атаке Microsoft IIS, направленной на веб-сервер Unix, и к атаке Sendmail на сервер Microsoft Exchange. Ни одна из этих атак не будет успешной, так как их цели не являются уязвимыми для данных конкретных атак.

Совет

С помощью информации, получаемой в результате сканирования уязвимостей, можно определить, какие события можно безопасно игнорировать.

Ведение журналов. При возникновении события любого типа должно генерироваться максимально возможное количество информации для обеспечения детализованного анализа или для помощи в принятии дальнейших мер. Занесение события в журнал является пассивным ответным действием, в рамках которого больше не осуществляется никаких операций.

Посредством сбора основных данных (IP-адреса, дата и время, тип события, идентификаторы процесса, идентификаторы пользователя и т.д.) IDS идентифицирует событие как что-то, требующее дальнейшего внимания.

Ведение дополнительных журналов. Пассивная обработка событий является более эффективной, если осуществляется сбор большего количества данных о фиксируемом в нормальном режиме событии. Например, если обычный журнал настроен на сбор IP-адресов и номеров портов для всех соединений, то в случае обнаружения события может производиться фиксирование пользовательских идентификаторов, идентификаторов процессов или фиксирование всего трафика, проходящего через соединение.

Еще одной разновидностью данного типа обработки события является использование выделенного сервера журналов. В организации может в различных местах сети присутствовать набор систем ведения журналов, которые включаются только в случае обнаружения события. Эти выделенные серверы журналов осуществляют сбор детализованной информации, которая затем используется для изолирования источника трафика, а также в качестве потенциальных доказательств, если происшедшее событие вызовет судебное разбирательство.

Уведомления. В отличие от простой констатации того факта, что событие произошло, уведомления позволяют IDS информировать лиц о происшедшем событии. Уведомление может иметь самые различные формы, начиная от мерцающих окон и звуковых сигналов и заканчивая почтовыми и пейджинговыми сообщениями. В зависимости от обстоятельств тот или иной тип предпочтительней другого. Например, мерцающие окна и сирены не очень полезны, если система IDS ведет круглосуточный мониторинг. Почтовые сообщения отправляются в удаленные места, но могут не дойти до получателя вовремя. Они также могут вызвать большой объем сетевого трафика, в результате чего злоумышленник догадается о присутствии системы IDS. Пейджинговые сообщения приходят вовремя (при условии бесперебойного функционирования спутника), но могут не предоставить достаточно информации для принятия соответствующих мер без предварительного просмотра журналов IDS.

Внимание!

Настройка IDS на отправку уведомления при возникновении события может вызвать проблемы в почтовых или пейджинговых системах, если произойдет большое число событий за очень малый промежуток времени.

Активная обработка событий

Активная обработка события позволяет наиболее быстро предпринять возможные меры для снижения уровня вредоносного действия события.

Однако если недостаточно серьезно отнестись к логическому программированию действий в различных ситуациях и не провести должного тестирования набора правил, активная обработка событий может вызвать повреждение системы или полный отказ в обслуживании легитимных пользователей.

Прерывание соединений, сеансов или процессов. Вероятно, самым простым действием для понимания является прерывание события. Оно может осуществляться посредством прерывания соединения, используемого атакующим злоумышленником (это возможно только в том случае, если событие использует TCP-соединение), с закрытием сеанса пользователя или завершением процесса, вызвавшего неполадку.

Определение того, какой объект подлежит уничтожению, выполняется посредством изучения события. Если процесс использует слишком много системных ресурсов, лучше всего завершить его. Если пользователь пытается использовать конкретную уязвимость или осуществить нелегальный доступ к файлам, то рекомендуется закрыть сеанс этого пользователя. Если злоумышленник использует сетевое соединение в попытках изучения уязвимостей системы, то следует закрыть соединение.

Внимание!

Действие по уничтожению может вызвать отказ в обслуживании легитимных пользователей. Разберитесь в потенциальной возможности ложных сигналов тревоги, прежде чем выполнять соответствующую операцию.

Перенастройка сети. Предположим, произошло несколько попыток доступа к компьютерам организации с конкретного IP-адреса, следовательно, есть вероятность того, что с этого IP-адреса осуществлена попытка атаки на информационную систему. В данном случае может понадобиться перенастройка межсетевого экрана или маршрутизатора. Изменение настроек может быть временным или постоянным, в зависимости от IP-адреса и запрограммированных логических действий (прерывание всего трафика между партнером по бизнесу может негативно сказаться на производительности). Новые фильтры или правила могут запретить установку любых соединений с удаленным узлом либо запретить соединение лишь по конкретным портам.

Обманные действия. Наиболее сложным типом активной обработки событий являются обманные действия. Ответ обманом направлен на введение злоумышленника в заблуждение посредством создания впечатления успешного и необнаруженного проведения атаки. В то же время система-цель защищается от атаки злоумышленника либо посредством его перенаправления на другую систему, либо посредством перемещения жизненно важных компонентов системы в безопасное место.

Одним из типов обманных действий является "горшок с медом". Под "горшком с медом" подразумевается система или иной объект, выглядящий для злоумышленника настолько привлекательным, что он не может его пропустить. В то же время за атакующим ведется наблюдение, и все его действия записываются. Разумеется, информация в "горшке с медом" не является актуальной, но внешне этот объект выглядит как наиболее важный компонент информационной системы.

Вопрос к эксперту

Вопрос. Допускается ли встречная атака в качестве ответного действия на вторжение?

Ответ. Проводить встречную атаку настоятельно не рекомендуется. Во-первых, такие атаки в большинстве случае являются нелегальными, и их следствием может стать судебное разбирательство. Во-вторых, источником атаки часто является атакованная система, вследствие чего ответная атака может навредить ни в чем не повинному пользователю.

Автоматический и автоматизированный ответ

Автоматический ответ - это набор предустановленных операций, которые выполняются при возникновении определенных событий. Такие ответные действия, как правило, осуществляются в рамках штатной процедуры, определяющей конкретные триггеры, инициирующие набор действий. Эти действия могут варьироваться от пассивных до активных. Автоматические ответные действия могут управляться людьми или компьютерами.

В случае если ответ на инцидент полностью контролируется компьютером без участия человека, такие ответные действия называются автоматизированными. Этот тип ответных действий должен контролироваться точно определенным, тщательно продуманным и хорошо протестированным набором правил. Так как ответные действия не требуют участия пользователя, они будут выполняться в случае обнаружения соответствия установленному набору правил. Реализовать автоматизированные ответные действия, принудительно уничтожающие сетевой трафик, очень просто.

В таблице 12.2 приведены примеры соответствующих пассивных и активных ответных действий с использованием набора политик, который был определен выше.

Таблица 12.2. Примеры ответных действий, определяемые политикой IDS

Политика	Пассивные ответные действия	Активные ответные действия
Обнаружение атак	Ведение журналов Ведение	Нет ответного активного действия.

	дополнительных журналов Уведомление	
Предотвращение атак	Ведение журналов Уведомление	Закрытие соединения. Завершение процесса. Возможна перенастройка маршрутизатора или межсетевого экрана.
Обнаружение нарушений политики	Ведение журналов Уведомление	Нет ответного активного действия.
Принудительное использование политик	Ведение журналов Уведомление	Закрытие соединения. Возможно перенастройка прокси.
Принудительное использование политик соединения	Ведение журналов Уведомление	Закрытие соединения. Возможно перенастройка маршрутизатора или межсетевого экрана.
Сбор доказательств	Ведение журналов Ведение дополнительных журналов Уведомление	Обманные действия.Возможно закрытие соединения.

Вопросы для самопроверки

1. Датчик IDS, отслеживающий нелегальные операции, проводимые приложением, называется _____.
2. После определения целей применения IDS следующим шагом является _____.

Определение порогов

Пороговые значения обеспечивают защиту от ложных срабатываний, что повышает эффективность политики IDS. Пороговые значения могут использоваться для фильтрации случайных событий с целью их отделения от тех событий, которые в действительности представляют собой угрозу безопасности. Например, сотрудник может подключиться к веб-сайту, не связанному с деловой активностью, перейдя по ссылке, предоставленной поисковой системой. Сотрудник может выполнять легитимный поиск, но из-за некорректно заданных параметров поиска может отобразиться не относящийся к работе сайт. В данном случае это отдельное событие не вызовет генерацию отчета в системе IDS. Такой отчет попусту занял бы ресурсы при изучении совершенно безобидного действия пользователя.

Аналогично, пороговые значения, обнаруживающие атаки, должны быть настроены на игнорирование зондирования низкого уровня или отдельных событий, связанных со сбором информации. Среди таких событий можно выделить отдельную попытку "фингеринга" (указания) сотрудника. Программа-указатель (фингер), распространенная в системах Unix, как правило, используется для проверки корректного адреса электронной почты или для получения открытых ключей. Тем не менее, попытки фингеринга большого числа сотрудников за небольшой промежуток времени могут являться признаком того, что злоумышленник собирает необходимую информацию для проведения атаки.

Выбор пороговых значений для системы IDS напрямую зависит от типов событий и потенциальных нарушений политики. Невозможно идентифицировать конкретный универсальный набор пороговых значений. Тем не менее, возможно определить параметры, которые необходимо принимать в расчет при настройке пороговых значений. Ниже приведены эти параметры.

- Опыт пользователя. Если пользователь недостаточно опытен и допускает множество ошибок, может выдаваться слишком много ложных сигналов тревоги.
- Скоростные характеристики сети. В сетях с низкими скоростями передачи данных могут выдаваться ложные сигналы о событиях, которые требуют получения определенных пакетов в течение определенного промежутка времени.
- Ожидаемые сетевые соединения. Если система IDS настроена на выдачу сигнала тревоги для определенных сетевых соединений, и эти соединения часто имеют место, то будет происходить слишком много ложных срабатываний.
- Нагрузка на сотрудника по администрированию или безопасности. Большой объем работы сотрудников, ответственных за безопасность, может потребовать установку более высоких пороговых значений для снижения числа ложных срабатываний.
- Чувствительность датчика. Если датчик очень чувствителен, может потребоваться установка более высоких пороговых значений, чтобы снизить число ложных срабатываний.
- Эффективность программы безопасности. Если программа безопасности организации очень эффективна, она может предусматривать пропуск некоторых атак, пропущенных IDS вследствие наличия в информационной среде других средств защиты.
- Имеющиеся уязвимости. Нет причины для выдачи сигнала тревоги в случае атак на отсутствующие в сети уязвимости.
- Уровень секретности систем и информации. Чем выше уровень секретности информации, используемой в организации, тем ниже должны быть пороговые значения для выдачи сигналов тревоги.
- Последствия ложных срабатываний. Если последствия ложных срабатываний очень серьезны, может понадобиться установка более высоких пороговых значений для выдачи сигналов тревоги.
- Последствия несрабатывания. Наоборот, если очень серьезны последствия несрабатывания (или пропущенных событий), может понадобиться установка более низких пороговых значений.

Примечание

Пороговые значения являются строго индивидуальными для каждой организации. Можно иметь в виду основные принципы их определения, но в

каждой организации необходимо в отдельном порядке рассматривать конкретную ситуацию и задавать пороговые значения согласно приведенным выше параметрам.

Применение системы

Непосредственное применение политики IDS должно тщательно планироваться, как и сама политика. Следует иметь в виду, что до данного момента политика IDS разрабатывалась на листе бумаги с учетом (хорошо, если это так) реальных тестов и опыта использования. Чтобы подвергнуть хорошо организованную сеть большой опасности, в ней достаточно всего лишь установить неправильно сконфигурированную систему IDS. Следовательно, после разработки политики IDS и определения изначальных пороговых значений необходимо установить IDS согласно конечной политике, с минимальным числом каких-либо активных мер. В течение некоторого времени при оценке пороговых значений следует внимательно следить за работой IDS. Таким образом, политика может быть проверена на практике без повреждения легитимного трафика или прерывания легального доступа пользователей к компьютерам.

Не менее важно во время испытательного или начального срока работы системы тщательно проводить изучение работы IDS по исследованию процессов, происходящих в системе, чтобы оценить степень корректности информации, выдаваемой IDS.

Внимание!

Ошибочное обвинение сотрудника или внешнего пользователя вследствие некорректного определения факта нарушения политики может отрицательно сказаться на впечатлении от функционирования системы и поставить в организации вопрос об эффективности использования программы IDS.

Управление IDS

Концепция обнаружения вторжений - уже не новинка в области информационной безопасности. Тем не менее, до недавнего времени дела обстояли несколько иначе, пока на коммерческом рынке не появились системы IDS. На момент написания этой книги различные производители предлагали свои сетевые и узловые системы IDS. Также существует ряд бесплатных систем обнаружения вторжений.

Перед принятием в организации решения об использовании IDS (будь то коммерческая система или некоммерческая) руководство организации должно четко определить цели применения программы. Правильная настройка и управление IDS требует больших усилий, и эти усилия следует как можно более эффективно использовать для обнаружения атак

(посредством реализации хорошей программы по обеспечению безопасности).

С учетом сказанного выше, если принято решение о применении IDS, то для успешной реализации программы необходимо обеспечить наличие всех нужных ресурсов. Если цели программы IDS включают возможность мониторинга в круглосуточном и ежедневном мониторинге атак, сотрудникам организации понадобится быть "наготове" круглые сутки семь дней в неделю. В то же время системным администраторам потребуется работать с сотрудниками, ответственными за безопасность, для определения успешного или безуспешного проведения атаки и, в случае успешной атаки, для определения метода обработки инцидента. В идеальном случае процедура по обработке инцидента должна быть создана и протестирована перед применением системы IDS.

О чем может сообщить система IDS

Система обнаружения вторжений может только выдавать отчеты о тех событиях, на обнаружение которых она настроена. Конфигурация IDS состоит из двух компонентов. Первым из них являются признаки атак, запрограммированные в системе. Второй компонент - любые дополнительные, определенные администратором, события, также представляющие интерес. Среди этих событий могут быть определенные типы трафика или сообщений журнала.

Посредством включения в конечный продукт признаков атак поставщик или разработчик системы по-своему интерпретирует уровень важности указанных событий. Степень важности, присваиваемая определенным событиям в той или иной организации, может быть совершенно иной, нежели та, которую предусмотрел разработчик. Может понадобиться изменить параметры по умолчанию для некоторых признаков или просто отключить признаки, не применимые к организации.

Примечание

Следует иметь в виду, что система IDS будет выдавать предупреждения только о тех событиях, которые она обнаружит. Если на системе, отслеживаемой датчиком HIDS, не заносятся в журнал определенные события, то датчик HIDS не будет их распознавать. Аналогично, если датчик NIDS не может "видеть" определенный трафик, он не выдаст предупреждение даже в том случае, если событие произойдет.

С условием правильной конфигурации IDS можно привести четыре типа событий, о которых будет сообщать система IDS.

- События исследования.

- Атаки.
- Нарушения политики.
- Подозрительные или необъяснимые события.

Большая часть времени будет уделяться исследованию подозрительных событий.

События исследования

События исследования представляют собой попытки атакующего собрать данные о системе перед непосредственным проведением атаки. Эти события можно разделить на пять категорий.

- "Скрытое" сканирование.
- Сканирование портов.
- Сканирование "троянских коней".
- Сканирование уязвимостей.
- Отслеживание файлов.

Большая часть этих событий происходит в сети, в основном, они исходят из интернета и направлены на системы с внешними адресами.

События исследования являют собой попытки сбора информации о системах. Они не являются событиями, воздействующими на систему. Некоторые коммерческие IDS воспринимают события исследования как события высокого приоритета. С учетом того, что эти события не наносят ущерба системе, такой подход можно счесть неразумным.

Примечание

Источником подобного трафика может быть и другая система-жертва, захваченная злоумышленником, поэтому данную информацию следует сообщать системным администраторам этого узла.

Скрытое сканирование. Скрытое сканирование - это попытки идентификации систем, присутствующих в сети, с целью предотвратить обнаружение системы, с которой будет проводиться атака. Этот тип сканирования будет определяться датчиками NIDS как половинчатое сканирование IP или скрытое сканирование IP, и, как правило, такое сканирование направлено на большое число IP-адресов. Ответной реакцией является идентификация источника и информирование владельца системы-источника о том, что его система, скорее всего, подверглась воздействию злоумышленника.

Сканирование портов. Сканирование портов используется для определения служб, работающих на системах сети. Системы обнаружения вторжений выявляют сканирование портов в случае, когда определенное число портов

(соответствующее пороговому значению) на одной системе открывается в течение небольшого промежутка времени. Датчики NIDS и некоторые датчики HIDS обеспечивают идентификацию данного типа сканирования и составляют соответствующие отчеты. Ответные действия на сканирование данного типа идентичны ответным действиям на скрытое сканирование.

Сканирование "троянских коней". Существует множество вредоносных программ типа "троянский конь". Датчики NIDS содержат признаки, определяющие многие из этих программ. К сожалению, трафик, направленный на "троянские" программы, как правило, определяется конечным портом пакета. Это обстоятельство вызывает большое число ложных срабатываний системы обнаружения вторжений. В случае возникновения события "Trojan" следует проверять исходный порт трафика. К примеру, трафик, исходящий с порта 80, как правило, поступает с веб-сайта.

Одним из наиболее распространенных типов "троянского" сканирования является сканирование BackOrifice. Программа BackOrifice использует порт 31337, и очень часто злоумышленники осуществляют сканирование диапазона адресов для этого порта. Консоль BackOrifice также содержит функцию "ping host" (отправка пинг-запросов на узлы), которая осуществляет сканирование автоматически. Беспокоиться не о чем, пока не будет зафиксирован исходящий трафик с внутренней системы. Опять-таки, в данном случае нужно связаться с владельцем системы-источника, так как она, вероятно, подверглась воздействию злоумышленника.

Сканирование уязвимостей. Сканирование уязвимостей распознается системой IDS при обнаружении большого набора различных признаков атак. Как правило, такое сканирование направлено на несколько систем. Редки случаи, когда сканирование уязвимостей производится по отношению к диапазону адресов без активных систем.

Сканирование уязвимостей, осуществляемое хакерами, невозможно отличить от сканирования уязвимостей, проводимого компаниями, которые проверяют уровень защищенности информационных систем (во многих случаях в этих компаниях используются те же самые средства!). Так или иначе, само по себе сканирование не причиняет системе какого-либо вреда, однако если атакующий выполнил сканирование, в результате которого выявились системы с уязвимостями к атаке, ему после этого становится известно, какие системы можно атаковать. Для обеспечения соответствия компьютерных систем актуальным проблемам безопасности следует контактировать с владельцем системы-источника и проверять внутренние системы организации на наличие самых последних надстроек безопасности и обновлений.

Совет

Как правило, сложно отличить сканирование уязвимостей от атаки, так как IDS в обоих случаях инициирует одни и те же события. Разница здесь заключается в количестве событий. Сканирование уязвимостей, как правило, сопровождается большим числом различных событий за очень малый отрезок времени, в то время как при проведении атак происходят события одного типа.

Отслеживание файлов. Отслеживание файлов или проверка файловых разрешений, как правило, осуществляется внутренним пользователем. Пользователь пытается определить, к каким файлам можно осуществить доступ и что эти файлы могут содержать. Данный тип разведки распознается только датчиком HIDS и только в том случае, если в системе ведется журнал попыток несанкционированного доступа. Отдельные события подобного рода, как правило, представляют собой невинные ошибки, однако если прослеживается определенная схема, то следует связаться с пользователем и выяснить, что же произошло.

Атаки

События атак требуют самой быстрой ответной реакции. В идеальном случае IDS должна быть настроена только на идентификацию событий высокого приоритета в случае использования известной внутренней уязвимости. В этом случае должна быть немедленно применена процедура обработки инцидента.

Имейте в виду, что IDS не распознает разницу между непосредственной атакой и сканированием уязвимостей, которое выглядит как атака. Администратор системы IDS должен проводить оценку информации, представленной системой IDS, для определения того, является ли событие атакой. Во-первых, необходимо выяснить число событий. Если в течение короткого промежутка времени наблюдался набор признаков различных атак, то это, скорее всего, сканирование уязвимостей, а не непосредственная атака. Если же обнаружен один признак атаки, направленной на одну или несколько систем, то это событие может представлять собой настоящую атаку.

Нарушения политики

Большая часть систем IDS поставляется с признаками следующих событий.

- Общий доступ к файлам (Gnutella, Kazaa и т. д.).
- Обмен мгновенными сообщениями.
- Сеансы Telnet.
- Команды "r" (rlogin, rsh, rexec).

В большей части организаций использование такого трафика является нарушением политики безопасности. К сожалению, такие нарушения политики могут представлять для организации большую опасность, нежели непосредственные атаки. В большинстве случаев событие происходит в действительности. Таким образом, открывается доступ к файлам, и системы настраиваются на разрешение выполнения команды rlogin.

Выбор метода обработки различных нарушений политики зависит от внутренних политик и процедур, имеющих место в организации. Тем не менее, необходимо разъяснить все моменты системному администратору или ответственному лицу, чтобы ему стала ясна суть политик организации.

Подозрительные события

События, не соответствующие полностью ни одной из других категорий, заносятся в категорию подозрительных событий. Подозрительным событием называется событие, которое не удалось распознать. Например, ключ реестра Windows NT был изменен по непонятной причине. Это не похоже на атаку, но в то же время не ясно, каковы причины изменения ключа. В качестве другого примера можно привести пакет с флагами заголовка, нарушающими стандарт протокола. Это может быть попытка разведывательного сканирования, результат неисправности сетевой карты системы или пакет, при передаче которого возникли ошибки. В данных, выдаваемых системой IDS, не предоставляется достаточно сведений для четкого определения конкретной ситуации и выяснения того, что произошло - безобидная ошибка или атака.

Ничуть не менее подозрительным может оказаться неожиданный сетевой трафик, появившийся во внутренней сети. Если рабочая станция начинает запрашивать SNMP-данные с других систем, то это может быть как следствием атаки, так и неправильной конфигурации. Подозрительные события необходимо исследовать настолько, насколько позволяют это делать имеющиеся ресурсы.

Внимание!

Исследование подозрительных событий может быть очень трудоемкой задачей. Нередко представляется разумным пропустить некоторые из этих событий или просто передать информацию сетевому или системному администратору.

Исследование подозрительных событий

При возникновении подозрительных действий следует выполнить процедуру, состоящую из следующих шагов, чтобы определить, является ли данное

действие удавшимся вторжением или попыткой проникновения, либо оно носит безвредный характер. Итак, нужно выполнить следующие шаги.

1. Идентифицировать системы.
2. Записывать в журнал сведения о дополнительном трафике между источником и пунктом назначения.
3. Записывать в журнал весь трафик, исходящий из источника.
4. Записывать в журнал содержимое пакетов из источника.

При выполнении каждого шага необходимо определять, достаточно ли очевидных признаков для выяснения того, является ли данное действие атакой. В следующих разделах приводится описание данных шагов.

Примечание

При исследовании события необходимо иметь в виду следующий момент. Если событие происходит один раз и больше не повторяется, то очень трудно получить какую-либо дополнительную информацию (кроме того, откуда поступил трафик). Одиночные аномалии исследовать практически невозможно.

1. Идентификация систем

Первым шагом при исследовании подозрительной активности является идентификация участвующих в действии систем. Эта процедура может заключаться в преобразовании IP-адресов в имена узлов. В некоторых случаях имя узла найти не удается (система не имеет записи DNS; это клиент DHCP; удаленный DNS-сервер находится в неактивном состоянии и т. д.). Если поиск DNS оканчивается неудачей, то следует попытаться идентифицировать узел другими способами, например, поиском в реестре American Registry of Internet Numbers (ARIN) по адресу http://www.arin.net/, в Internic по адресу http://www.networksolutions.com/ или в других каталогах интернета. Утилиты, такие как Sam Spade (находятся по адресу http://samspade.org/), также помогут в данном случае. Невозможность идентификации источника или пункта назначения подозрительных действий не является достаточным доказательством того, что событие в действительности является атакой. Аналогично, успешная иденти фикация систем не является достаточным доказательством "безобидности" обнаруженных действий.

Примечание

Источник подозрительного трафика может не являться непосредственным источником атаки. Попытки проведения атаки на отказ в обслуживании, как правило, проводятся с подмененными исходными адресами, и попытки

несанкционированного доступа или зондирование могут исходить с других систем, захваченных злоумышленником.

2. Запись в журнал дополнительного трафика между источником и пунктом назначения

Одно-единственное отдельное событие (например, нарушение протокола IP) может не представлять полную информацию о трафике между двумя системами. Иными словами, необходимо понимать контекст подозрительных действий. Хорошим примером здесь служит признак атаки Sendmail WIZ. Этот признак идентифицирует попытку использования команды WIZ в программе Sendmail. Данное событие безопасности идентифицирует любое вхождение команды WIZ в сообщении. Если команда WIZ присутствует в теле сообщения, то это определенно не попытка вторжения. Понимание контекста события помогает определять ложные срабатывания.

Таблица 12.3. Пример конфигурации IDS с записью в журнал всего трафика между двумя системами

Имя события	Действие	IP-адрес источника	IP-адрес пункта назначения	Протокол	Порт источника	Конечный порт
SUS_ACT	Уведомление, занесениев журнал	Источник подозрительной активности	Пункт назначения подозрительной активности	TCP,UDP и/или ICMP, в зависимости от типа обнаруженной активности	Любой	Любой

Настройте IDS на отслеживание всего трафика между источником подозрительной активности и пунктом назначения. В качестве примера используйте таблицу 12.3.

Теперь зададимся вопросом, что же это все нам дает. Во-первых, мы получаем представление о другом трафике, имеющем место между источником и пунктом назначения. Если бы пакет WIZ был единственным трафиком между двумя системами, из этого можно было сделать вывод о том, что это похоже на попытку проникновения в систему. Напротив, если наблюдается большое число трафика SMTP (почты) между двумя системами, то, скорее всего, это обычный легитимный почтовый трафик.

3. Запись в журнал всего трафика из источника

Подразумевая, что данных, фиксируемых посредством записи всего трафика между двумя системами, недостаточно для определения того, является ли активность легитимной, можно начать сбор другого трафика, поступающего с источника. Имейте в виду, что объем этого трафика может быть ограниченным. Если источник подозрительной активности находится в некоторой удаленной сети, то будет наблюдаться только трафик, поступающий на ваш узел. Если же источник локальный, то возможен сбор всего трафика с данного компьютера, что даст гораздо более широкое представление о том, что же на самом деле происходит.

Чтобы начать сбор всего трафика с источника, настройте детектор IDS на сбор всей информации из подозрительного источника. Пример такой конфигурации приведен в таблице 12.4.

Таблица 12.4. Пример конфигурации IDS, предназначенной для занесения в журнал всего трафика, исходящего с определенного адреса источника

Имя события	Действие	IP-адрес источника	IP-адрес пункта назначения	Протокол	Порт источника	Конечный порт
SUS_SRC	Уведомление, запись в журнал	Источник подозрительных действий	Любой	TCP,UDP и/или ICMP, в зависимости от типа обнаруженной активности	Любой	Любой

Такая конфигурация, как правило, генерирует некоторую информацию, не представляющую какой-либо ценности для исследования. До тех пор, пока возможна объективная оценка информации, данный журнал можно использовать для составления подробной картины происходящих взаимодействий, имеющих место между источником и пунктом назначения. Попытайтесь вникнуть в суть наблюдаемой активности. Является ли наблюдаемая активность веб-трафиком? Исходит ли трафик из подозрительного источника, или же его источником является ваш узел?

На данном этапе исследования должна быть известна следующая информация.

- Имя системы-источника.
- Тип и частота трафика, обмен которым происходит между источником и пунктом назначения.

- Тип и частота трафика, обмен которым происходит между источником и любыми другими системами вашего узла.

Эта информация обеспечивает достаточно подробное представление о природе подозрительного трафика. Тем не менее, степень очевидности происходящего может не сказать о том, является ли наблюдаемая активность попыткой атаки.

4. Запись в журнал содержимого пакетов из источника

Конечным шагом проводимого исследования является запись в журнал содержимого пакетов, исходящих из источника. Следует заметить, что данный подход полезен только при работе с текстовыми протоколами, такими как telnet, FTP, SMTP и HTTP (в некоторой степени). Если используются двоичные протоколы или протоколы с шифрованием, данный подход совершенно бесполезен. Для реализации описанного метода необходимо изменить конфигурацию IDS, как показано в таблице 12.5.

Посредством занесения в журнал содержимого пакетов можно составить полную запись сеанса, а также зафиксировать команды, непосредственно отправляемые в пункт назначения.

После фиксирования некоторых данных необходимо просмотреть найденную информацию. Обозначает ли сеанс потенциальную атаку, или же все выглядит в пределах допустимого? Скомбинировав эти данные с другой найденной информацией, можно найти ответ на этот вопрос. Если этого сделать не удалось, попытайтесь найти человека, у которого есть опыт работы с исследуемым протоколом.

Таблица 12.5. Пример конфигурации IDS, осуществляющей перехват содержимого пакетов

Имя события	Действие	IP-адрес источника	IP-адрес пункта назначения	Протокол	Порт источника	Конечный порт
SUS_ACT	Уведомление, запись в журнал содержимого пакета	Источник подозрительной активности	Пункт назначения подозрительной активности	TCP или UDP	Любой	Порт, на который направлен подозрительный трафик
SUS_ACT	Увеомление, запись в журнал содержим	Пункт назначения подозрительной	Источник подозрительной активности	TCP илиUDP	Порт, на который направлен подозрител	Любой

	ого пакета активности			ьный трафик	

Предотвращение вторжений

Предотвращение вторжений стало основной задачей разрабатываемых в последнее время продуктов в области обнаружения вторжений. Новые концепции направлены на изменение природы IDS посредством добавления функций по предотвращению вторжений вместо только лишь обнаружения. Многие продукты, соответствующие этой концепции, являются совершенно новыми на рынке. Тем не менее, указанная функциональность реализована в ряде уже зарекомендовавших себя продуктов.

Каким образом можно предотвратить вторжения с помощью системы IDS

Чтобы предотвратить вторжение, необходимо либо остановить осуществляемую атаку перед ее достижением системы-жертвы, либо остановить действие атаки перед выполнением на системе-жертве кода, использующего уязвимость.

Механизм предотвращения атаки легче всего рассматривать на узле, использующем HIDS. Например, можно использовать анализаторы системных вызовов или поведения приложения. Если вызов приложения похож на атаку, анализатор системных вызовов предотвратит выполнение вызова операционной системой. Если приложение пытается выполнить неавторизованную операцию, анализатор поведения приложения предотвратит ее выполнение. В обоих случаях HIDS предотвращает атаку.

Процесс предотвращения атаки при помощи NIDS является более сложным. В стандартной конфигурации NIDS датчик располагается в том месте, из которого он может отслеживать трафик (см. рис. 12.2). При поступлении через канал связи данных атаки датчик перехватывает пакет и начинает его анализировать. В некоторый момент датчик определяет, что пакет представляет собой атаку, и предпринимает действие. Это действие, как правило, заключается в закрытии соединения (только если атака проводится через соединение TCP) или в перенастройке межсетевого экрана для блокировки дальнейшего трафика из источника.

К сожалению, в случае с NIDS время работает не в пользу достижения цели. Во время анализа пакета датчиком пакет продолжает свое движение по сети. В большинстве случаев пакет достигает цели еще перед закрытием соединения или выполнением действий по перенастройке межсетевого экрана. Следовательно, чаще всего атака опережает действия датчика по ее предотвращению.

Примечание

Закрытие соединения или блокировка трафика из атакующей системы может снизить уровень повреждения системы, но не предотвратит воздействие на нее злоумышленника.

Для предотвращения с помощью NIDS успешного проведения атак на систему решение по пакету должно приниматься до того, как пакет достигнет системы-цели. Это означает, что архитектуру системы NIDS нужно изменить таким образом, чтобы датчик NIDS был расположен на одном канале связи с трафиком (как межсетевой экран), а не просто следил за проходящим мимо трафиком (см. рис. 12.5).

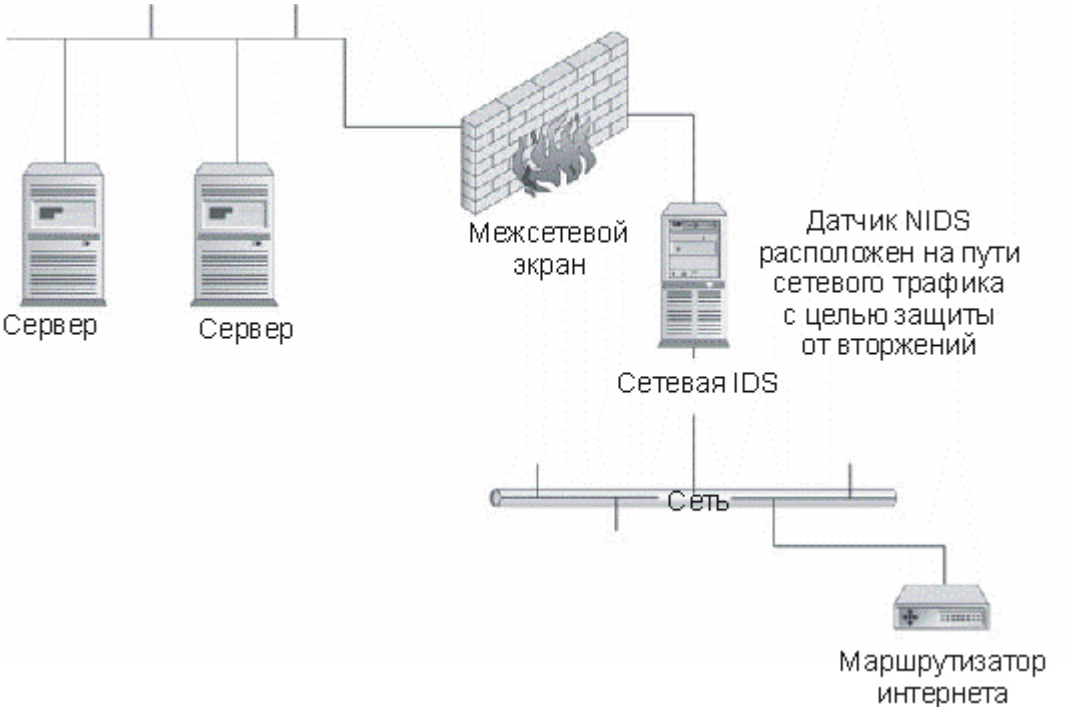

Рис. 12.5. Конфигурация, необходимая для предотвращения атак датчиком NIDS

Примечание

Рассмотренная архитектура не является единственно возможной. Также возможно расположить датчик NIDS на межсетевом экране либо реализовать его тесную взаимосвязь с межсетевым экраном, чтобы последний не пропускал трафик без разрешения датчика NIDS.

Проблемы, связанные с обнаружением вторжений

Замена реактивной природы IDS на превентивную создает некоторые проблемы. Действительно, после этого изменения возникают два серьезных вопроса: потенциальная возможность отказа в обслуживании и недостаточный средний уровень доступности.

Отказ в обслуживании

При предотвращении вторжений главным механизмом обработки больше не является уведомление системы, сети и системных администраторов. Теперь "ядром" системы является блокировка попытки выполнения действия. Когда IDS блокирует атаку, она предотвращает выполнение действия, будь то системный вызов, операция приложения или сетевое соединение. Данное блокирование предотвращает атаку. Очевидно, при этом подразумевается корректная идентификация системой IDS действия как атаки.

Если действие, попытка которого была осуществлена, на самом деле не являлось атакой, а IDS заблокировала его, то, возможно, IDS заблокировала законное действие, выполняемое в информационной среде. Вследствие этого IDS может вызвать отказ в обслуживании. Если действие, вызвавшее проблему, представляло собой некоторую аномалию (например, пакет с ошибками), то повторная передача пакета или повторная установка соединения, как правило, осуществляются успешно. Тем не менее, если IDS некорректно идентифицирует легитимные действия или трафик, принимая их за атаки, то, скорее всего, отказ в обслуживании будет происходить и в дальнейшем.

Внимание!

Современные датчики IDS выдают множество ложных сигналов тревоги. Принятие превентивных мер без полного понимания характеристик ложных срабатываний и характеристик легитимных действий, как правило, является причиной возникновения проблем.

Доступность

Доступность сетей и систем является важным свойством многих компьютерных систем. Организации затрачивают огромное количество времени и денег на настройку своих сетей и систем на снижение числа одиночных неполадок. Если датчик IDS установлен так, что через него должен проходить весь сетевой трафик, датчик NIDS должен соответствовать высокому уровню требований к доступности других компонентов сети. То же самое относится и к датчикам HIDS, расположенным на узле. Будет ли узел продолжать функционировать в случае сбоя программного обеспечения датчика, или же он также будет отключен? В информационной среде, в которой очень важен фактор доступности, необходимо решить указанные вопросы перед установкой таких систем.

Развертывание сетевой IDS

Данный проект призван продемонстрировать процесс развертывания сетевой IDS. Он начинается с предварительных этапов, которые необходимо

выполнять перед непосредственной процедурой развертывания. При желании можете на самом деле осуществить развертывание датчика сетевой IDS.

Шаг за шагом

1. Определите, какие действия вы пытаетесь осуществить посредством развертывания датчика IDS. Это поможет четко обрисовать цели применения IDS.
2. На основе целей применения IDS определите, какой сетевой трафик требуется отслеживать.
3. Теперь решите, каким образом будут обрабатываться различные события, выявляемые IDS. Попробуйте определить, что будет разумнее - поручить выполнение некоторого действия системе IDS или оператору, который будет выполнять нужную процедуру.
4. При отсутствии опыта работы с датчиком IDS вам придется нелегко при первой установке пороговых значений. Если в вашем обозрении есть уже функционирующая система IDS, можете посмотреть, какие пороговые значения установлены на этой системе для различных признаков атак.
5. Составьте план развертывания IDS. Определите, кого в организации нужно задействовать для выполнения этой задачи.
6. Если вы хотите попробовать осуществить развертывание датчика NIDS, выделите для этого компьютер и установите на него Linux, FreeBSD или другую версию операционной системы семейства Unix.
7. Загрузите последнюю версию программы Snort (бесплатная IDS) с сайта http://www.snort.org/.
8. Следуйте инструкциям по установке и выполните инсталляцию программы Snort. Можно также установить ряд дополнительных программных пакетов для упрощения процесса управления и конфигурации.
9. Подключите датчик к сети. Лучше всего сделать это при помощи концентратора. Тем не менее, можно также использовать порт разветвителя на коммутаторе.
10. Разместив датчик на нужном месте, просмотрите файлы журналов, чтобы выяснить, какие события в них фиксируются. Также можно использовать программу Acid для просмотра файлов журнала через веб-интерфейс. Acid - это веб-интерфейс, используемый для анализа данных программы Snort.

Выводы

При наличии некоторого опыта работы с операционной системой Unix вам будет несложно разобраться с программой Snort. Данное упражнение поможет выполнить шаги по установке датчика NIDS. Однако если вы намереваетесь использовать его как действующий датчик в организации,

необходимо заручиться поддержкой сетевых и системных администраторов организации. Также не следует думать, что этот проект удастся выполнить за один день. Настройка датчика и оценка результатов его работы потребует некоторых временных затрат.

Контрольные вопросы

1. Что подразумевается под обнаружением вторжений?
2. Назовите два основных типа IDS.
3. Может ли узловая IDS всегда определять успех или неудачу проведения атаки?
4. Может ли узловая IDS предотвращать атаку?
5. Возможно ли противостоять контролеру целостности файлов?
6. Назовите пять этапов реализации системы IDS.
7. Является ли идентификация действий пользователей корректной целью применения IDS?
8. Может ли сетевая IDS предотвращать достижение атаками их целей?
9. Что подразумевается под пассивными ответными действиями?
10. Что подразумевается под активными ответными действиями?
11. Должна ли применяться процедура выполнения ответных действий на инцидент в случае половинчатого IP-сканирования?
12. Почему оповещения о наличии в системе "черных ходов"часто оказываются ложными срабатываниями системы обнаружения вторжений?
13. О чем, как правило, говорит ситуация, при которой за небольшой промежуток времени наблюдается большое число различных атак?
14. Какой тип IDS следует применить в организации для защиты веб-сервера от причинения ущерба?
15. Какой тип системы IDS следует выбрать организации для защиты от атак, если в первую очередь рассматривается вопрос стоимости?