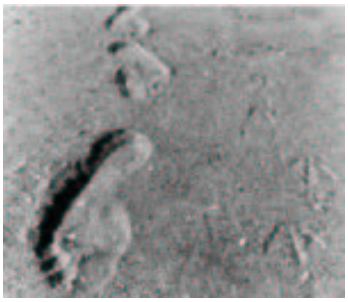
Журнал "Открытые системы", #07-08, 2002 год // Издательство "Открытые Системы" (www.osp.ru)
Постоянный адрес статьи: http://www.osp.ru/os/2002/07-08/035_1.htm

Обнаружение вторжений: краткая история и обзор

Ричард Кеммерер, Джованни Виджна

08.08.2002

Представьте, что перед вашим домом остановился странный человек. Он обернулся, внимательно оглядел окрестности, а затем подошел к двери и повернул ручку. Дверь оказалась запертой. Он подошел к ближайшему окну и попытался осторожно его открыть. Окно тоже было закрыто. По-видимому, ваш дом в безопасности. Так зачем же устанавливать сигнализацию?



Похожий вопрос часто задают защитникам технологии обнаружения вторжений. Зачем морочить себе голову обнаружением вторжений, если уже есть межсетевые экраны, «заплаты» для операционных систем вовремя устанавливаются, и системные администраторы следят за тем, чтобы у пользователей были разумные пароли? Ответ очень прост: потому что в системы по-прежнему проникают злоумышленники. Точно так же, как иногда люди забывают закрыть в доме окно, они забывают корректным образом обновить набор правил на межсетевом экране.

Даже с самой совершенной защитой компьютерные системы нельзя назвать абсолютно неуязвимыми. Большинство экспертов по компьютерной безопасности соглашаются с тем, что создать абсолютно защищенную систему никогда не удастся. Поэтому столь актуальной остается задача создания методов обнаружения вторжений и систем для выявления и реагирования на компьютерные атаки.

Обнаружение вторжений: краткая история

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 находится 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 [1]. 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.

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 [2-4].

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 [5-7]. 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 [8] 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 [9].

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.

Заключение

Даже по мере того, как защита сетей становится все надежнее, обнаружение вторжений 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 [10]. 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 [11]. 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.

Литература

[1] J.P. Anderson, Computer Security Threat Monitoring and Surveillance, James P. Anderson Co., Fort Washington, Pa. 1980
[2] D.E. Denning, «An Intrusion Detection Model», IEEE Trans. Software Eng., vol. 13, no. 2, Feb. 1987
[3] C. Ko, M. Ruschitzka, K. Levitt, «Execution Monitoring of Security-Critical Programs in Distributed Systems: A Specification-Based Approach», Proc. 1997 IEEE Symp. Security and Privacy, IEEE CS Press, Los Alamitos, Calif., 1997
[4] A.K. Ghosh, J. Wanken, F. Charron, «Detecting Anomalous and Unknown Intrusions Against Programs», Proc. Annual Computer Security Application Conference (ACSAC'98), IEEE CS Press, Los Alamitos, Calif., 1998
[5] K. Ilgun, R.A. Kemmerer, P.A. Porras, «State Transition Analysis: A Rule-Based Intrusion Detection System», IEEE Trans. Software Eng. vol. 21, no. 3, Mar. 1995
[6] V. Paxson, «Bro: A System for Detecting Network Intruders in Real-Time», Proc. Seventh Usenix Security Symp., Usenix Assoc., Berkeley, Calif., 1998
[7] U. Lindqvist, P.A. Porras, «Detecting Computer and Network Misuse with the Production-Based Expert System Toolset», IEEE Symp. Security and Privacy, IEEE CS Press, Los Alamitos, Calif., 1999
[8] M. Roesch, «Snort-Lightweight Intrusion Detection for Networks», Proc. Usenix Lisa '99 Conf., Usenix Assoc., Berkeley, Calif., 1999
[9] R. Bace, P. Mell, «Special Publication on Intrusion Detection Systems», Tech. Report SP 800-31, National Institute of Standards and Technology, Gaithersburg, Md., Nov. 2001
[10] G. Vigna, R.A. Kemmerer, P. Blix, «Designing a Web of Highly Configurable Intrusion Detection Sensors», Proc. Fourth Int'l Symp. Recent Advances in Intrusion Detection (RAID 2001), Lecture Notes in Computer Science, vol. 2212, Springer Verlag, New York, 2001
[11] D. Curry, H. Debar, «Intrusion Detection Message Exchange Format: Extensible Markup Language (XML) Document Type Definition», Dec. 2001

Ричард Кеммерер (kemm@cs.ucsb.edu) — профессор и бывший декан факультета информатики университета штата Калифорния в Санта-Барбаре. К области его научных интересов относятся компьютерная безопасность, формальная спецификация и верификация программ.

Джованни Виджна (vigna@cs.ucsb.edu) — доцент факультета информатики университета штата Калифорния в Санта-Барбаре. Он специализируется в области сетевой и компьютерной безопасности, систем обнаружения вторжений, безопасности переносимого кода, тестирования программ.

Журнал "Открытые системы", #07-08, 2002 год // Издательство "Открытые Системы" (www.osp.ru)
Постоянный адрес статьи: http://www.osp.ru/os/2002/07-08/035_1.htm