XXX Юбилейная Неделя науки СПбГТУ. Материалы межвузовской научной конференции. Ч. VII: С133-134, 2002.

УДК 50.41.00

А.И. Бовт (4 курс, каф. ИБКС), Д.П. Зегжда, к.т.н., доц.

АНАЛИЗ СОВРЕМЕННЫХ IDS. ВЫЯВЛЕНИЕ ВАРИАНТОВ ИХ ИСПОЛЬЗОВАНИЯ

В области защиты вычислительных систем давно сформировалась область первичных средств защиты, таких как средства идентификации/аутентификации, контроля доступа и контроля целостности, но в силу специфики развития компьютерных технологии, первичных средств уже не хватает — слишком ценна информация, слишком много стало нарушителей и слишком изощренными стали их методы. В таком случае, на помощь приходит, уже близкий к окончательному формированию, класс вторичных средств защиты, таких как IDS и сканеры уязвимости. Попытаемся охарактеризовать одно из таких вторичных средств защиты — IDS.

За последние годы, начал формироваться и уже становится близким к окончательному формированию, второй эшелон средств защиты информации, к которой относятся рассматриваемые IDS.

В задачи данной работы входило рассмотрение современных IDS и их возможностей, а в качестве результата — выделить варианты их использования, рассмотрев часть из них детально.

Использование IDS рассматривается в трех аспектах: во-первых, стандартное использование IDS - как вторичное средство защиты, во-вторых, интеграция IDS в комплексную систему защиты, в-третьих - использование IDS как инструментария администратора. Стандартное использование - это применение отдельной IDS, интегрированное использование - применение комплексной системы защиты, в которой IDS является одним из компонентов, второстепенное использование - использование IDS как инструментария для решения различных частных задач.

Объект данных исследований, IDS (Intrusion Detection System, Система обнаружения вторжений) является системой, занимающейся анализом сетевого трафика, конфигурационных параметров (влияющих на безопасность системы) на хостах, всевозможных логов и других сущностей системы с целью обнаружения вторжений в систему, не остановленных первичными средствами защиты. В задачи IDS входит: сбор достаточного количества информации для анализа, обнаружение нарушений и при нахождении нарушения - извещение администратора и принятие соответствующих ответных действий.

В ходе работы, на основании программной документации и веб сайтов, были рассмотрены архитектуры, функциональные возможности и особенности следующих IDS:

Snort, NFR (Network Flight Recorder), T-Sight, Real Secure, eTrust Intrusion Detection, Dragon, Kane Secure Enterprise, Cisco Secure IDS, POLYCENTER Security Intrusion Detector.

Также, были рассмотрены особенности следующих стандартов / протоколов / проектов: OPSEC (Open Platform for Security) (разработчик – CheckPoint), Intrusion Detection Exchange Format (Internet Drafts), разработчик - idwg (intrusion detection working group, подразделение IETF'a)

Как показал анализ данного формирующегося класса систем, IDS не является первичным механизмом защиты системы, так как она не может предотвратить неавторизированный доступ и поддерживать политику безопасности. Однако она может обнаружить нарушение безопасности, вызванное авторизированными действиями. Было выделено место IDS в системе защиты, суть которого изображена на рис.1.

Анализ современных IDS показал, что большинство из IDS систем имеют возможности для тесной интеграции IDS со средствами защиты. К этому можно отнести взаимодействие IDS со средствами защиты (например, использование функций мониторинга пакетов на межсетевом экране), а также интеграцию IDS (как компонента) в комплексную систему безопасности. Среди вариантов такой интеграции, я выделил два подхода: во-первых, унифицирование интерфейсов (например, научная стандартизация IETF'ом, стандарт OPSEC, интерфейсы систем Tivoli и HP Open View и т.д.), во-вторых, создание комплексных систем безопасности одним производителем (например, система POLYCENTER). Проанализировав данные документацию по данным стандартам и системам, можно сделать следующие выводы: унификация является достаточно сложным процессом, и существующие стандарты берутся рассматривать только одну конкретную часть интерфейса (например, подсистему уведомлений) взаимодействия IDS. В то же время системы от одного производителя имеют существенный плюс в том, что значительно облегчается выработка единых интерфейсов взаимодействия компонентов (так как это делается в рамках одной компании), но такие системы обладают малой функциональностью, например в системе POLYCENTER вся реализация политики безопасности сводится к банальной политике учетных записей.

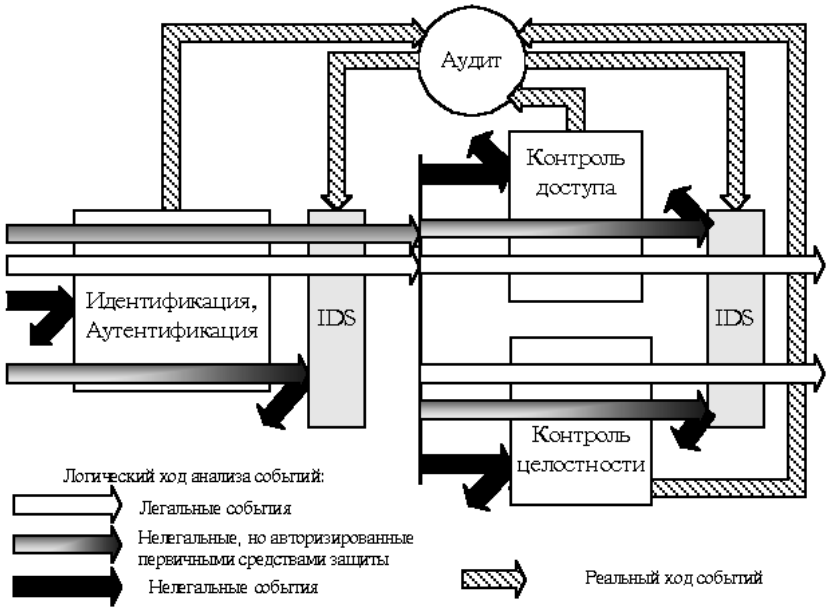

Рис. 1. Место IDS в системе защиты

В качестве дополнительных вариантов использования IDS, выявлены следующие направления: обнаружение частных видов вторжений, мониторинг отдельных сервисов; исследование критериев обнаружения путем итеративного изменения правил и анализа получаемого результата, дополнение различных (не только первичных) средств защиты Среди данных направлений, затрагивались такие концепции, как взаимодополнение двух различных IDS, «пассивные ловушки», «сосредоточенный контроль».

Рассмотренные нами варианты использования IDS (как вторичное средство защиты, как компонент комплексной системы защиты, как инструментарий) являются актуальными для современного состояния информационной безопасности компьютерных систем. Безусловно, в будущем рассмотренные альтернативы использования будут трансформироваться: часть из вариантов использования будут реализовывать уже отдельные средства защиты, которые появятся в будущем; часть функций, безусловно, останется за IDS; а некоторые функции, возможно, в силу ненадобности пропадут.