Развитие систем обнаружения вторжения

Одной из важнейших задач систем информационной безопасности является наблюдение за данными, передающимися по сети, чтобы находить потенциально опасные действия в отношении определенного компьютера, чтобы предотвратить доступ злоумышленника. Существует множество разновидностей подобных систем, особенно много их появилось в последние годы. В моём докладе рассматривается история возникновения и развития технологии Систем Обнаружения Вторжения (Intrusion Detection System = IDS) с первого их появления.

Компоненты IDS

Для начала, следует определить, из чего состоит IDS и чем каждый из её компонент занимается.

Обнаружение вторжения через сеть (Network Intrusion Detection = NID)

Обнаружение вторжения через сеть работает с данными, передающимися по проводам между компьютерами. IDS-устройства часто называют “packet-sniffers”, то есть “анализаторы пакетов”, так как они перехватывают пакеты, передающиеся по разным коммуникационным средам и протоколам, обычно TCP/IP. Будучи перехваченными, пакеты анализируются множеством разных способов. Затем некоторые NID-устройства просто сравнивают пакет с базой данных, состоящей из известных атак и “отпечатков пальцев” пакетов “злоумышленников”, некоторые смотрят на аномальную активность пакета, которая может означать опасное поведение.

Анализатор берет пакет, дефрагментирует его, получает кусок кода и сравнивает его с базой данных атак. Поэтому одной из проблем анализа является то, что злоумышленник может сделать высокий уровень фрагментации пакетов, и тогда системе придется расходовать ресурсы на дефрагментацию и затем (в случае NID) сборку пакета обратно.

Аномальная активность означает, что число обращений резко возрастает; это также скорее всего означает, что началось вторжение.

Исторически, NID не могли работать в следующих условиях:

1. Переключаемые сети (switched networks).
2. Шифрованные сети (encrypted networks).
3. Высокоскоростные сети (high-speed networks) – свыше 100 Мб/с.

В дальнейшем, однако, компания Cisco произвела модуль для их системы Catalyst 6000 switch, который встраивает обнаружение вторжения через сеть прямо в switch, исключив, таким образом, первый пункт. Кроме того, ISS/Network ICE заявили, что они сейчас могут обеспечивать “packet-sniffering” на гигабитных скоростях.

Преимущество NID-систем в том, что можно установить одну систему на всю подсеть (на входе в неё), и анализировать данные сразу для всех хостов. То есть не требуется больших мощностей локальных компьютеров для работы систем на каждом хосте.

Недостатком является то, что их можно перегрузить ненужными данными, чтобы они не успевали справляться с потоком, например, посылать пакеты на несуществующие в сети адреса.

Централизованное обнаружение вторжения (Host-based Intrusion Detection = HID)

Централизованные системы обнаружения вторжения созданы чтобы наблюдать, определять и сообщать пользователю и системе об активности и атаках на заданный хост. Некоторые более сложные инструменты также предлагают управление и централизацию политики аудита (которая определяет тип регистрируемых событий безопасности в отношении к домену или отдельному компьютеру), поставку характеристик информации,

статистический анализ и доказательную поддержку, и в некоторых случаях меру контроля над доступом. Разница между host-based и network-based ID в том, что NID работает с информацией, передаваемой от хоста к хосту, а HID относится к тому, что происходит на самих хостах.

Host-based intrusion detection больше всего пригодна для борьбы с внутренними опасностями благодаря их возможности наблюдать и реагировать на специальные действия пользователя и доступы к файлам хоста. Большинство компьютерных опасностей появляется в больших организациях, где много различных ресурсов; обиженные работники и корпоративные шпионы – вот два самых простых примера. На самом деле, эксперт по обнаружению вторжения Ричард Пауэр утверждает: "каждый год мы просим респондентов, чтобы они оценили вероятные источники атак. Неизменно, обиженные и нечестные работники оказываются на вершине списка с 80% голосов".

Итак, HID используется в случае, если злоумышленник находится внутри подсети.

Смешанное обнаружение вторжения (Hybrid Intrusion Detection)

Смешанные системы обнаружения вторжения предлагают управление и предупреждения и от network и от host-based ID устройств. Смешанные решения обеспечивают логическую завершенность NID и HID – центральное управление предупреждением вторжения.

В этом случае предупреждаются атаки и изнутри подсети, и снаружи; каждой из задач занимается отдельная часть системы.

Обнаружение вторжения в узле сети (Network-Node Intrusion Detection = NNID)

NNID было разработано чтобы избежать ошибок обычного NID. Здесь технология перехватывания пакетов переносится из проводов в сам хост. В NNID "packet-sniffer" расположен таким образом, что он захватывает пакеты после того, как они достигли своей конечной цели – хоста получателя. Затем пакет анализируется точно так же как и в случае обычного NID и "packet-sniffer"-а. Такая схема основа на предположении преимущества HID. При таком подходе, network-node – это просто ещё один модуль, который можно подключить к HID агенту. Главный недостаток network-node - что он исследует только пакеты, адресованные на тот хост, где он расположен, в то время, как традиционные NID могут наблюдать за пакетами во всей подсети. Хотя даже при этих условиях, "packet-sniffers" также не могут наблюдать за всей подсетью, в случае если сеть использует высокоскоростную связь, шифрование или switch-и. То есть они по сути "без нюха" ("packet-sniffers without a sense of smell"). Преимущество NNID состоит в его способности защитить определенные хосты от packet-based атак в сложных условиях, когда обычный NID неэффективен.

Плюсом таких систем является то, что пакеты анализируются уже в пункте назначения, поэтому сложнее становится перегрузить систему. Во-первых, это связано с тем, что пакеты уже не надо дефрагментировать, т.е. так легче восстановить передаваемые между машинами данные. Во-вторых, системе не приходится обрабатывать лишние пакеты, она работает только с пакетами, адресованными на данный хост. В итоге существенно возрастает надёжность системы по сравнению с обычными NID.

Недостатком является сложность. Ведь куда проще установить одну NID-систему на всю подсеть, чем NNID на каждый хост. И действительно NID-системы намного удобнее, но, к сожалению, они не всегда справляются со своими задачами, поэтому приходится использовать более сложные NNID-системы.

Системы обнаружения вторжения: краткая история

Целью обнаружения вторжения является наблюдение за сетевыми ресурсами, чтобы определить их аномальное поведение или неправильное использование. Такое понятие существовало уже около 20 лет, но только недавно произошел огромный скачок популярности, и IDS стали встраивать во все структуры безопасности информации. Первое представление об IDS появилось в 1980 году в работе Джеймса Андерсена ”Computer Security Threat Monitoring and Surveillance”. С тех пор основные части технологии IDS развились до нынешнего уровня. Давайте подробнее рассмотрим как изменялись IDS начиная с первых ступеней.

“Зародышевая” работа Джеймса Андерсена, написанная для правительственных организаций, представила понятие о проверке и записи важной информации, которая могла бы быть полезной для обнаружения неправильного использования и понимания поведения пользователя. С выходом этой работы возникли такие понятия как “засечение” неправильного использования и специальные действия пользователя. Его рассмотрение проблемы проверки информации и её важности привело к огромному прорыву в системах проверки практически всех операционных систем. Предположения Андерсена также стали фундаментов для разработки и дизайна систем обнаружения вторжения. Его труд положил начало центральному обнаружению вторжения (host-based intrusion detection) и IDS вообще.

В 1983 году компания “SRI International” и в частности доктор Дороти Деннинг (Dorothy Denning) начали работу над правительственным проектом, который запустил новый виток разработки обнаружения вторжения. Их целью было проанализировать контрольный след из основных правительственных компьютеров и создать профили пользователей на основе их деятельности. Год спустя доктор Деннинг помогла разработать первую модель для обнаружения вторжения, Экспертную Систему Обнаружения Вторжения (the Intrusion Detection Expert System = IDES), которая обеспечила начало разработки технологии IDS, которая вскоре последовала.

В 1984 году SRI также изобрели источник слежения и анализирования контрольного следа, содержащего информацию аутентификации пользователей ARPANET, затем ставшего Internet. Вскоре затем SRI завершила контракт с Navy SPAWAR, реализовав полнофункциональную систему обнаружения вторжения IDES. На основе своей работы доктор Деннинг опубликовала решающую статью “An Intrusion Detection Model”, которая содержит необходимую информацию для развития коммерческих IDS. Её работа – основа большинства работ по IDS, которые затем последовали.

Между тем, были и другие значительные исследования в Калифорнийском Университете Дэвиса Лоуренса (Lawrence Livermore Laboratories). В 1988 году проект Haystack (“стог сена”) в Lawrence Livermore Labs реализовал ещё одну версию системы обнаружения вторжения для военно-воздушных сил Соединённых Штатов. Эта система анализировала контрольный след, сравнивая его с определёнными образцами. В телефонном интервью с его автором, Кросби Марксом (Crosby Marks), участником команды разработки проекта Haystack и работником лаборатории, он сказал, что “отыскание в этом огромном количестве данных одного специфического неправильного использования было подобно поиску иголки в стоге сена”.

Следующий шаг такого инструмента был назван Распределённая Система Обнаружения Вторжения (Distributed Intrusion Detection System = DIDS). DIDS усилила существующую систему за счёт того, что клиентские машины проверяются также, как и серверы. В итоге, в 1989 году, разработчики проекта Haystack создали коммерческую компанию “Haystack Labs” и выпустили систему последнего поколения Сталкер. Кросби Маркс говорит, что “Сталкер это централизованная система обнаружения вторжения, работающая на основе сравнения с образцами, которая имеет большие поисковые

способности, чтобы автоматически или вручную проверять данные". Успехи проекта Haystack, удвоенные работой SRI и Деннинг очень усилили разработку технологии HID.

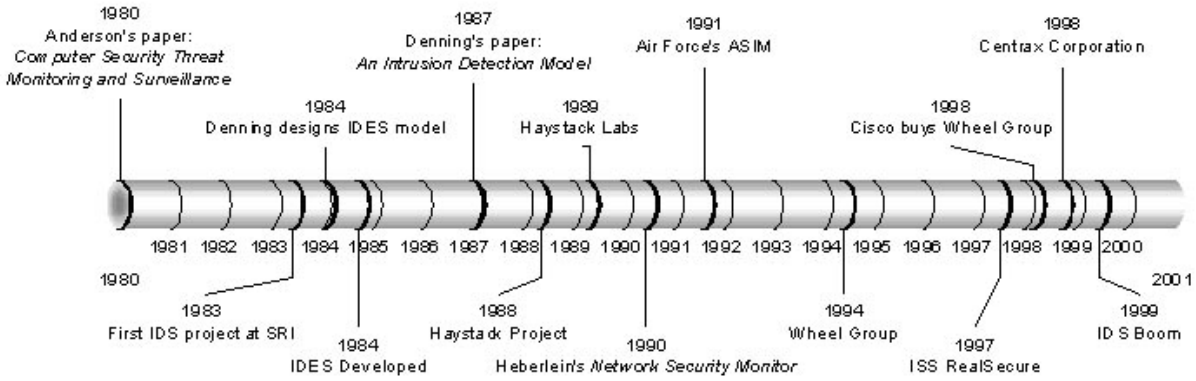
В начале 90-х Тодд Хеберлейн (Todd Heberlein) из UC Davis's представил идеи системы обнаружения вторжения через сеть. В 1990 году Хеберлейн был основным автором и разработчиком системы "Network Intrusion Monitor" = NIM – первой NID. NSM была установлена на основных правительственных системах, где требуется обработка большого количества информации, поступающей через сеть. Это привлекло ещё больший интерес к области систем обнаружения вторжения, и вложения в этот рынок значительно увеличились. Вклад Хеберлейна также расширил проект DIDS, где вместе с командой Haystack он представил первые идеи смешанного обнаружения вторжения. Работы проекта Haystack и выпуск Network Security Monitor произвели революцию в области IDS и вывели её в коммерческий мир.

Коммерческое развитие технологий обнаружения вторжения началось в начале 90-х. Haystack Labs стали первой компанией, продающей IDS, в частности линию HID продуктов Сталкер. Компания SAIC также разрабатывала разновидность централизованной системы, названной Компьютерной Системой Обнаружения Неправильного Использования (Computer Misuse Detection System = CMDS). В то же время, Центр Криптографической Поддержки военно-воздушных сил разработал Автоматизированную Систему Мер Безопасности (Automated Security Measurement System = ASIM) чтобы наблюдать за данными в сети военно-воздушных сил Соединённых Штатов. Система ASIM произвела значительный прогресс в вопросах расширяемости и портативности, которые были слабым звеном в продуктах NID. Кроме того, ASIM была первой системой, которой удалось объединить NID решения и на уровне программного обеспечения, и на уровне оборудования. Эта система до сих пор используется и управляется командой Air Force's Computer Emergency Response Team (AFCERT) по всему миру. Как это часто происходит, группа разработчиков проекта ASIM сформировали коммерческую компанию в 1994 году и назвали её Wheel Group. Их продукт, NetRanger, был первой коммерчески жизнеспособной системой NID. Однако, коммерчески системы IDS развивались очень медленно и расцвели только ко второй половине десятилетия.

Рынок Обнаружения Вторжения начал приобретать популярность и действительно приносить плоды около 1997 года. В тот год лидер рынка безопасности, ISS, разработал систему обнаружения вторжения через сеть, названный RealSecure. Год спустя, компания Cisco поняла важность NID и купила Wheel Group и тем самым добилась уровня безопасности, требуемого клиентами. Похожим образом, первая известная HID компания Centrax Corporation появилась в результате объединения коллективов разработчиков Haystack Labs и CMDS. С тех пор коммерческий мир IDS значительно расширился в результате слияний различных компаний.

На данный момент, статистики рынка показывают, что IDS входит в число наиболее продаваемых технологий и, скорее всего, будет расти и дальше. Кроме того, правительственные инициативы, такие как Federal Intrusion Detection Network (FIDNet), созданная по указанию президента, также добавляют стремительность развитию IDS. Разработки в этой области в скором времени выведут технологии безопасности на совершенно новую арену автоматизированной безопасности.

Что же дальше? Существуют прикладные системы IDS, эвристические, основанные на правилах, и ещё множество других. Независимо от того, как эта технология развивается, одно известно точно – это на данный момент крайне важный компонент систем безопасности информации.

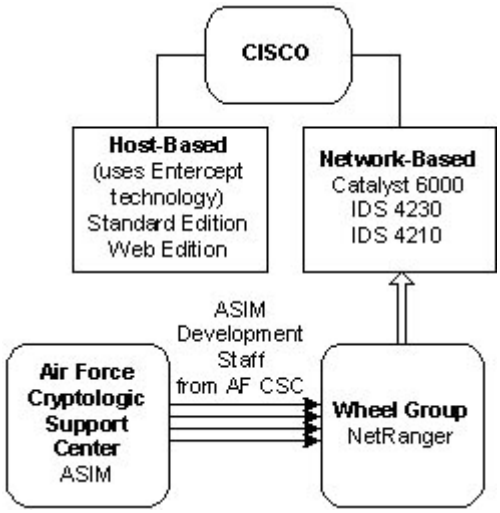


Участники

Рынок IDS растёт и сжимается вместе с фондовой биржей. В феврале 2000 года было огромное количество продавцов IDS, а на данный момент осталось только несколько самых серьёзных. Большинство исчезло или были поглощены большими компаниями. Важно заметить, как различные IDS компании пришли к данному состоянию. Давайте рассмотрим “игроков” на рынке и то, как они там оказались.

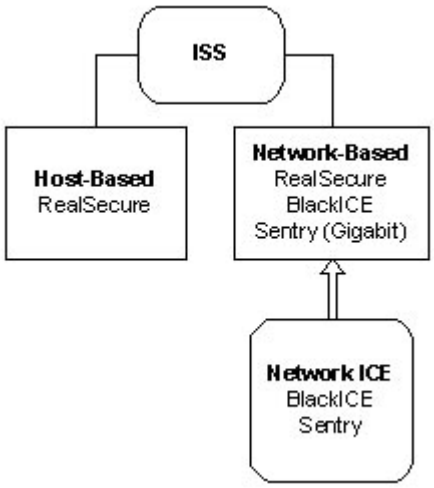
Cisco

На данный момент Cisco обеспечивает и host-based, и network-based ID – продукты. Компания впервые появилась на рынке в 1997 году, приобретя Wheel Group и её NetRanger за 124 миллиона долларов. Их серии IDS 4230 и 4210 включали типичные решения NID, в то время как модуль Catalyst 6000 был первой системой NID, встроенной в свитч, появившейся на рынке. В HID они не изобретали ничего нового, а использовали технологию Entercept.



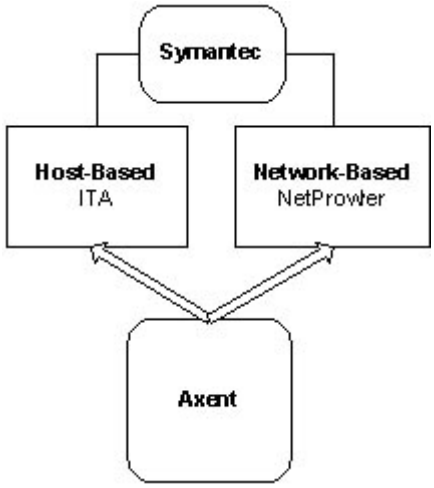
Internet Security Systems (ISS)

ISS занимается смешанными системами обнаружения вторжения и дополнительной NID системой, которая работает независимо от них. ISS начали работу с NID с производства системы RealSecure, практически в то же время, когда Cisco купили NetRanger. Только два года спустя они представили host-based компонент, который сделал их смешанную IDS систему завершённой. Недавно ISS сделали ещё один шаг к завоеванию рынка приобретя компанию Network ICE и их высоко уважаемые решения NID, включая их новую гигабитную NID систему.



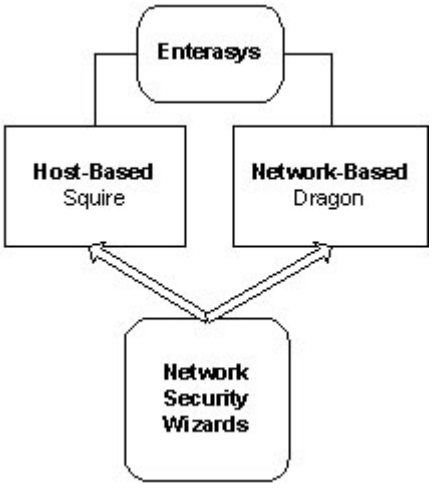
Symantec

Symantec недавно приобрели компанию Axent и таким образом получили их технологии Alert и NetProwler, что вывело их на рынок IDS. Symantec предлагает NID и HID решения, а также метод встраивания смешанных систем.



Enterasys

Так же как и Cisco, Enterasys/Cabletron поняли, что обеспечение мостов и роутеров было жизнеспособным источником предложений по обнаружению вторжения. Следовательно, Enterasys купили Security Wizards и их разработку Dragon NID и систему Squire HID.

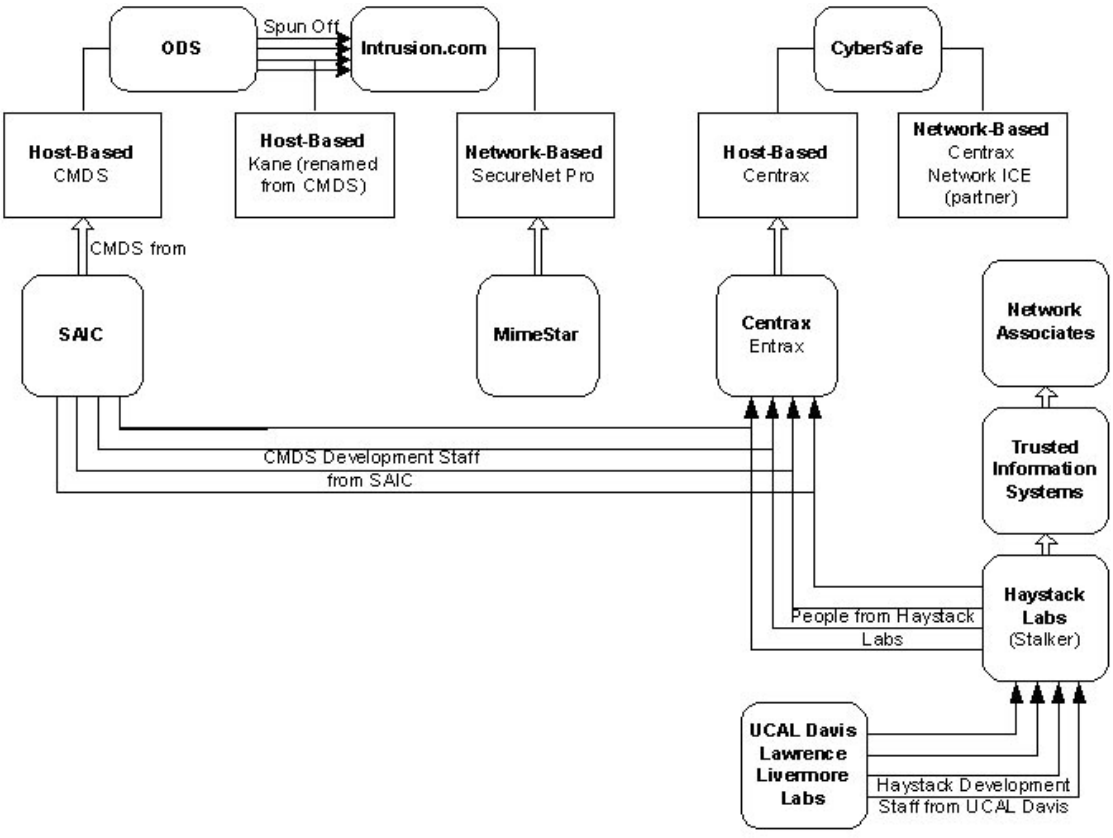


Остальные

Обсудим оставшуюся часть области IDS.

Начнём со слияния группы разработчиков компании CMDS, которая дала начало Centrax Corporation с работниками Haystack Labs. Кстати, остатки компании Haystack были куплены CyberSafe Corporation и изменили их HID продукт Entrax в Centrax. Centrax затем стал первым жизнеспособным HID продуктом. CyberSafe вскоре представили NID, а затем и NNID технологии в своём продукте Centrax, они даже сотрудничали с компанией Network ICE, чтобы завершить эту систему. Однако затем ISS купили Network ICE и прекратили это сотрудничество.

Между тем, CMDS опять переехали, когда их продали компании ODS, которая переименовала их в Kane Security Enterprise и затем сократили до Intrusion.com чтобы проще было продавать продукты. Intrusion.com затем приобрели MimeStar и их систему SecureNet.



Заключение

Подводя итоги, можно сказать, что работы Андерсена, Хеберлейна и Деннинг определили понятие IDS. Вложения правительства и корпоративный интерес помогли развить это понятие в технологию, которая в итоге нашла свою нишу в сетевой безопасности. Обнаружение Вторжения действительно прошло длинный путь, став необходимым источником наблюдения, определения и противодействия угрозе безопасности. От теории к практике и, в итоге, к коммерчески жизнеспособному оборудованию, технология IDS прошла огромное количество итераций и множество владельцев. Тем не менее, использование IDS действительно стало повсеместным. Кроме того, IDS стали необходимыми.

Литература:

1. “The Evolution of Intrusion Detection Systems”, Paul Inella, 2001, SecurityFocus. http://www.securityfocus.com/infocus/1514
2. “Computer Security Threat Monitoring and Surveillance”, James Anderson, 1980, Fort Washington, Pa. http://csrc.nist.gov/publications/history/ande80.pdf
3. “An intrusion-detection model”, D. E. Denning, 1987, IEEE Transactions on Software Engineering, Vol. SE-13(No. 2):222-232 http://www.cs.georgetown.edu/~denning/infosec/ids-model.rtf