УДК 004.942:004.056.53

А.И. Михалев, Ю.О. Калиберда

ПОСТРОЕНИЕ IDS НА ОСНОВЕ ИСКУССТВЕННОЙ ИММУННОЙ СЕТИ

Аннотация. Предлагается использовать метод построения системы обнаружения вторжений в локальной вычислительной сети, основанный на принципах организации искусственной иммунной сети. Приводятся примеры выявления атак и не санкционированных программных действий.

Ключевые слова: искусственная иммунная система, клональная селекция отрицательный отбор, безопасность.

Постановка задачи

Программные продукты класса IDS (Intrusion Detection System) всё чаще становятся необходимым дополнением инфраструктуры сетевой безопасности. В дополнение к межсетевым экранам, работа которых происходит на основе политики безопасности, IDS служат механизмами мониторинга и наблюдения подозрительной программной активности. Они позволяют обнаружить атакующих программных агентов, которые обошли firewall, и выдают отчет администратору, который, в свою очередь, может предпринять дальнейшие шаги по предотвращению атаки. В свою очередь, система, основанная на принципе организации ИИС, сама может предпринять ряд программно-комплексных мероприятий для предотвращения несанкционированных действий в сети [1].

Основная часть

Современные подходы к обнаружению атак в основном базируются на исследовании только одного источника информации, например, сетевого трафика, использования системных ресурсов или логирования. Благодаря своей масштабируемости и модульности, IDS на основе ИИС может использовать все виды доступной информации для получения более точного заключения о факте атаки или вредоносных действий.

В данной системе реализована обобщённая концепция с использованием двух типовых принципов IDS:

 ISSN 1562-9945

Host IDS (HIDS) – системы, обнаруживающие атаки, направленные на конкретный узел сети;

Network IDS (NIDS) – системы, обнаруживающие атаки, направленные на всю сеть или сегмент сети.

Вся информация собирается как от отдельных узлов, находящиеся в данном сегменте сети (информация, полученная из журналов регистрации операционной системы и различных приложений: web-сервер, СУБД и т.д., либо, вместо этого, используется весь входящий/исходящий сетевой трафик), так и из потокового трафика устройств, обеспечивающих маршрутизацию данных.

В общем случае, обнаружение атак требует выполнения одного из двух условий: понимания, как себя должен вести каждый объект сети, или знания всех возможных (на практике – известных) вариантов атак. В первом случае используется технология обнаружения аномального поведения (anomaly detection), а во втором случае – технология сравнения с шаблонами (сигнатурами) всех имеющихся в базе атак.

Технология сравнения с шаблонами по сути своей очень похожа на технологию работы антивирусного ПО. Система может обнаружить все известные ей на данный момент атаки, но она мало приспособлена для обнаружения новых, еще не известных атак. Данный подход, очень прост, и у него мала вероятность ложного срабатывания (false positive), по сравнению с технологией обнаружения аномального поведения.

Для генерации нового шаблона поведения используется один из алгоритмов искусственной иммунной сети — клонирование. Полученные шаблоны применяются на так называемой «песочнице», (под «песочницей» следует понимать, часть функционирующей системы, при проведении над ней некоторых преобразований путем действий, которые были получены в результате клонирования, не повлияет на общую работу сети, однако сообщит свои параметры состояния. Из этих параметров будет сделан вывод, является ли полученный шаблон атакующим, или же он представляет собой обычное поведенческое состояние в сети. Если система смогла распознать новый шаблон как «потенциально опасный шаблон поведения», то она сообщает системному администратору о наличии

небезопасного участка в сети и рекомендации по её устранению, или же сама предпримет действия для локализации данной уязвимости. При новом шаблоне, который распознался как «безопасный шаблон поведения», этот шаблон записывается в базу системы, и при обнаружении активности в сети по этому шаблону, система не предпринимает ни каких действий.

Каждый компонент в сети представляет собой некое подобие детекторов, которые связаны друг с другом в одну логическую сеть. Детекторы атак анализируют деятельность системы, используя для этого событие или множество событий на соответствие заранее определенному образцу, который описывает известную атаку. Соответствие образца известной атаке называется *сигнатурой*.

В то же время, технология обнаружения аномального поведения рассматривается как более перспективная. Как показывает практика, новые атаки и вирусы могут быть легко сгенерированы из уже известных атак, лишь с небольшими изменениями. Для IDS это означает необходимость содержания и поиска данных по огромной и постоянно расширяющейся базе, что приводит к замедлению реакции устройств. К тому же, новая атака не может быть детектирована и отражена до тех пор, пока она не будет детерминирована и размещена в базе.

Детекторы аномалий предполагают, что атаки отличаются от "нормальной" (законной) деятельности и могут, следовательно, быть определены системой, которая умеет отслеживать эти отличия. Детекторы аномалий создают профили, представляющие собой нормальное поведение пользователей, хостов или сетевых соединений. Эти профили создаются, исходя из данных истории, собранной за период нормального функционирования системы. Затем детекторы собирают данные о событиях и используют различные метрики для определения того, что анализируемая деятельность отклоняется от нормальной

В свою очередь, для генерации данных детекторов может быть использован ещё один из алгоритмов ИИС – алгоритм отрицательного отбора. В отличие от клонального алгоритма, в данном алгоритме генерируются различные профили пользователей, хостов и сравниваются с профилями, которые были получены в результате нормального функционировании сети. Эти профили сравниваются со

стандартными профилями на предмет выявления аномалий. В случае обнаружении последних, данный профиль записывается в базу системы и информация об этом сообщается другим детекторам. Если аномалии не были обнаружены, то эти данные убираются из базы и освобождают ресурсы для генерации новых профилей, которые могут быть распознаны системой как потенциально опасные [2],[3].

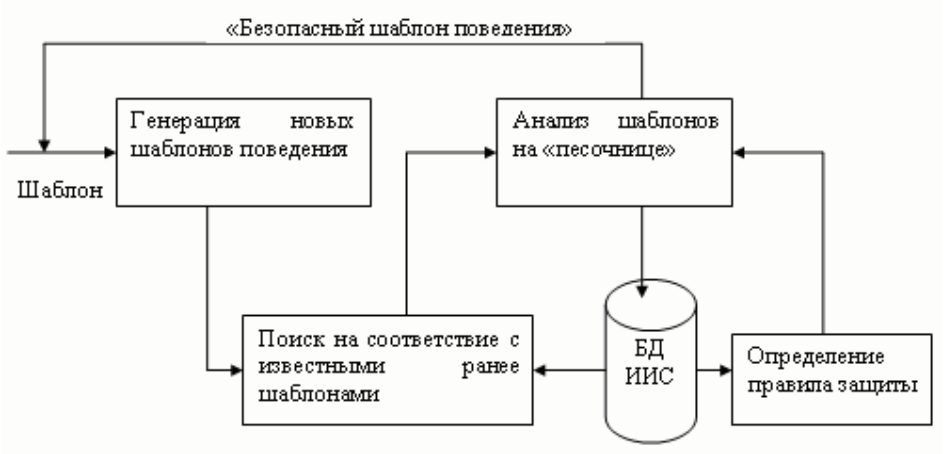

Рисунок 1 - Логическая схема IDS

Использование IDS на основе ИИС помогает достичь нескольких целей:

- Обнаружить вторжение или сетевую атаку;
- Спрогнозировать возможные будущие атаки и выявить уязвимости для предотвращения их дальнейшего развития. Атакующая система, обычно, выполняет ряд предварительных действий, таких как, например, сетевое зондирование (сканирование) или иное тестирование для обнаружения уязвимостей целевой системы;
- Обеспечить контроль качества администрирования с точки зрения безопасности, особенно в больших и сложных сетях;
- Определить расположение источника атаки по отношению к локальной сети (внешние или внутренние атаки), что важно при принятии решений о расположении ресурсов в сети.

Основными компонентами IDS на основе ИИС являются:

- Сенсорная подсистема, предназначенную для сбора событий, связанных с безопасностью защищаемой сети или системы;
- Подсистема анализа, предназначенная для выявления сетевых атак и подозрительных действий;

- Хранилище, в котором накапливаются первичные события и результаты анализа;
- Консоль управления, позволяющая конфигурировать IDS, наблюдать за состоянием защищаемой системы и IDS, просматривать выявленные подсистемой анализа инциденты.

Вывод

К основным преимуществам данной IDS на основе искусственной иммунной сети можно отнести следующее:

- Большое покрытие для мониторинга и, в связи с этим, децентрализованное управление;
- Возможность контроля над событиями локально относительно хоста;
- Функционирование в окружении, в котором сетевой трафик зашифрован;
- При добавлении нового узла, система автоматически адаптируется под изменённую сеть.
- Невозможность вывода из строя данной системы основными видами атак.

ЛИТЕРАТУРА

1. D. Dasgupta and S. Forrest. Artificial Immune Systems in Industrial Applications. In the proceedings of the Second International Conference on Intelligent Processing and Manufacturing of Materials (IPMM), Honolulu, July 10-15, 1999.

2. Михалев А.И., Калиберда Ю.О. Применение искусственных иммунных систем для выявления аномалий в сетевом трафике // Міжнародна наукова конференція Інтелектуальні системи прийняття рішень та прикладні аспекти інформаційних технологій (ISDMIT` 2006) 2006 (2) - с.215-217.

3. Михалев А.И., Калиберда Ю.О. Математическая модель иммунной реакции на вторжение в компьютерную сеть // Системные технологии. Региональный межвузовский сборник научных работ. – Выпуск 3 (56). – Том 2. – Днепропетровск, 2008. – С.175-178.

 ISSN 1562-9945