УДК:004.7

Системы обнаружения вторжений

Южук З.С., Госуниверситет — УНПК, 11-ИБ

Актуальность: Данная статья предоставляет базовую информацию о системах обнаружения вторжений, что должно помочь избежать традиционных промахов в приобретении, развертывании и поддержании систем обнаружения вторжений.

Цель: Повысить уровень знаний в данной области на конкретном примере. Рассмотреть устройство, принцип работы и применение.

Система обнаружения вторжений (СОВ) — программное или аппаратное средство, предназначенное для выявления фактов неавторизованного доступа в компьютерную систему или сеть либо несанкционированного управления ими в основном через Интернет. Соответствующий английский термин — Intrusion Detection System (IDS).

Системы обнаружения вторжений обеспечивают дополнительный уровень защиты компьютерных систем. Системы обнаружения вторжений используются для обнаружения некоторых типов вредоносной активности, которая может нарушить безопасность компьютерной системы. К такой активности относятся сетевые атаки против уязвимых сервисов, атаки, направленные на повышение привилегий, неавторизованный доступ к важным файлам, а также действия вредоносного программного обеспечения (компьютерных вирусов, троянов и червей).

Существует несколько способов классификации СОВ в зависимости от типа и расположения сенсоров, а также методов, используемых подсистемой анализа для выявления подозрительной

активности. Во многих простых СОВ все компоненты реализованы в виде одного модуля или устройства.

IDS состоят из трех функциональных компонентов: информационных источников, анализа и ответа. Система получает информацию о событии из одного или более источников информации, выполняет определяемый конфигурацией анализ данных события и затем создает специальные ответы – от простейших отчетов до активного вмешательства при определении проникновений.

Системы обнаружения вторжений (IDS - Intrusion Detection Systems) - один из важнейших элементов систем информационной безопасности сетей любого современного предприятия. Системами обнаружения вторжений (СОВ) называют множество различных программных и аппаратных средств, объединяемых одним общим свойством - они занимаются анализом использования вверенных им ресурсов и, в случае обнаружения каких-либо подозрительных или просто нетипичных событий, способны предпринимать некоторые самостоятельные действия по обнаружению, идентификации и устранению их причин.

Но системы обнаружения вторжений лишь один из инструментов защитного арсенала и он не должен рассматриваться как замена для любого из других защитных механизмов. Защита информации наиболее эффективна, когда в интрасети поддерживается многоуровневая защита. Она складывается из следующих компонентов:

- политика безопасности интрасети организации;
- система защиты хостов в сети;
- сетевой аудит;
- защита на основе маршрутизаторов;
- межсетевые экраны;
- системы обнаружения вторжений;

- план реагирования на выявленные атаки.

Следовательно, для полной защиты целостности сети необходима реализация всех вышеперечисленных компонентов защиты. И использование многоуровневой защиты является наиболее эффективным методом предотвращения несанкционированного использования компьютерных систем и сетевых сервисов. Таким образом, система обнаружения вторжений – это одна из компонент обеспечения безопасности сети в многоуровневой стратегии её защиты.

Использование IDS помогает достичь нескольких целей:

1. возможность иметь реакцию на атаку позволяет заставить атакующего нести ответственность за собственную деятельность;
2. возможность блокирования означает возможность распознать некоторую активность или событие как атаку и затем выполнить действие по блокированию источника.

В сетевой СОВ, сенсоры расположены на важных для наблюдения точках сети, часто в демилитаризованной зоне, или на границе сети. Сенсор перехватывает весь сетевой трафик и анализирует содержимое каждого пакета на наличие вредоносных компонентов.

Системы IDS производят непрерывный мониторинг информации, получаемой при помощи:

- мониторинга сети/сетевого адаптер.;
- мониторинга логов брандмауэра (используется обычно только в интегрированных решениях брандмауэр - IDS).

После того, как система IDS обнаружит признаки атаки, обычно она в автоматизированном режиме выполняет определенные администратором действия, например:

- оповещает администратора (звуковым предупреждением, сообщением электронной почты/net send/пейджер/SMS и т.п.);

- изменяет настройки брандмауэра, блокируя IP-адрес нападающего;
- разрывает установленное нападающим TCP-соединение;
- запускает определенную администратором программу/скрипт;
- протоколирует атаку и т.п.

IDS - это только часть инфраструктуры защиты сети предприятия, и, как и все остальные компоненты, сама по себе IDS не обеспечивает абсолютной защиты. При использовании IDS обязательно необходимо учитывать следующие моменты:

- IDS обычно не могут нормально работать в сетях с большим трафиком (за исключением некоторых очень дорогих аппаратных систем);
- большинство IDS бессильно перед приемом, который называется snow blind (ослепление снегом);
- большое количество ложных срабатываний IDS, которые атакующему организовать совсем не сложно, могут привести к тому, что администратор просто отключит часть возможностей IDS.

Устанавливая IDS, нужно готовиться к тому, что большая часть срабатываний будет ложной, что потребует дополнительного времени и внимания со стороны администратора.

Что следует делать, чтобы минимизировать угрозы?

- Проводить регулярно оценку рисков в масштабах всего предприятия.
- Проводить периодические трейнинги по проблемам безопасности для всего персонала.
- Усилить разделение обязанностей и минимизировать привилегии.
- Реализовать жесткую политику и практику в отношении паролей и работы с аккаунтами.

- Действия сотрудников в сети должна мониторироваться, контролироваться и заноситься в журнальные файлы.
- Уделять повышенное внимание действиям администраторов и привилегированных пользователей.
- Выполнять все возможные меры по выявлению и удалению вредоносных кодов в масштабах сети и на каждой рабочей станции или сервере.
- Использовать многоуровневую защиту против удаленных атак (Firewall, IDS/IPS, а также DPI (Deap Packet Inspection)).
- Мониторировать и немедленно реагировать на любые подозрительные действия (активность во внеурочное время, изменение IP или MAC-адреса и т.д.).
- Деактивировать доступ к машинам после завершения на них работы допущенных сотрудников. Это же касается неиспользуемых портов хабов, переключателей и маршрутизаторов.
- Собирать и сохранять данные результатов расследований.
- Использовать безопасные процедуры восстановления конфигураций и работы с резервными копиями. Не допускать несанкционированного доступа к резервным копиям.
- Минимизировать период резервного копирования критически важных данных. Этот период должен зависеть от частоты обновления программ и информации.
- Четко документировать все операции по контролю активности сотрудников.

Концепция обнаружения вторжений основывается на том, что вторжение – это попытка получить несанкционированный доступ (НСД) к защищенной системе. Коммерческие реализации таких систем (IDS – система обнаружения вторжений) включают в себя системы обнаружения вторжений network-based (т.е. обнаруживающие атаки,

направленные на всю сеть (сегмент сети)) и системы host-based (для обнаружения атак, направленных против конкретного узла сети).

Критериями для выбора IDS является несколько факторов: репутация производителя, функциональные возможности продукта и его эффективность. При выборе решение для IDS уверенность в возможностях обновления и поддержки со стороны производителя являются очень важными. Кроме того, возможности и расширения продукта необходимы для успешной установки системы. Глубина действия и точность являются важнейшими компонентами систем IDS. И в заключении – за работу системы должен отвечать отдельный работник. Его функции заключается в управлении ежедневными задачами по обновлению и настройке системы.

Точность. Ложные срабатывания являются большой проблемой для IDS. В больших сетях ошибочное истолкование оповещений существенно затрудняет усилия по обнаружению вторжений. Этот фактор особенно заметен для только что выпущенных продуктов.

Несколько факторов влияют на решение IDS. Правильная структура продукта позволяет лицам, ответственным за безопасность, достаточно просто поддерживать и управлять обновлениями. Кроме того, для работы важно наличие комплексной консоли управления и доступ в реальном времени к данным по атакам и предупреждениям.

Взаимодействие. Взаимодействие с текущей IT архитектурой и системами является очень важным. Необходимо иметь возможность вносить индивидуальные подписи и расширять возможности IDS по взаимодействию с текущими и будущими архитектурами и средами.

Список литературы:

1. IDS/IPS—Системы обнаружения и предотвращения вторжений [Электронный ресурс]: (с изм. и доп.) – Режим доступа: http://www.netconfig.ru/server/ids-ips ; (дата обращения 06.11.2012)

2. Сети и системы связи; IDS-конструктор: постройте свою собственную систему обнаружения вторжений! [Электронный ресурс]: (с изм. и доп.) – Режим доступа: http://www.ccc.ru/magazine/depot/06_07/read.html?0501.htm;(дата обращения 06.11.2012)

3. Системы обнаружения вторжений. [Электронный ресурс]: (с изм. и доп.) – Режим доступа: http://www.icmm.ru/~masich/win/lexion/ids/ids;(дата обращения 06.11.2012)

4. Архитектура IDS;[Электронный ресурс]: (с изм. и доп.) – Режим доступа: http://citforum.ru/security/internet/ids_overview/;(дата обращения 06.04.2012)