Методы и средства защиты информации

СИСТЕМЫ ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ

Выполнил: Колышев Дмитрий Алексеевич

Проверила: Писчасова Екатерина Федоровна

Системы мониторинга сетей

- Системы обнаружения и предотвращения вторжений (IDS/IPS).
- Системы предотвращения утечек конфиденциальной информации (DLP-системы).

Целью данной работы является изучение системы обнаружения вторжений.

Исходя из поставленной цели, данная работа ставит перед собой следующие основные задачи:

- Проанализировать литературу по выбранной теме;
- Определить состав системы обнаружения вторжений;
- В данной работе изучили и проанализировали основные направления системы обнаружения вторжений.

Системы обнаружения вторжений

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

Архитектура СОВ

- сенсорная подсистема - сбор событий, связанных с безопасностью защищаемой системы
- подсистема анализа - выявление атак и подозрительных действий на основе данных сенсоров
- хранилище, обеспечивающее накопление первичных событий и результатов анализа
- консоль управления - конфигурирование СОВ, наблюдать за состоянием защищаемой системы и СОВ, просматривать выявленные подсистемой анализа инциденты

Сетевая СОВ Network-based IDS (NIDS)

- Отслеживает вторжения, проверяя сетевой трафик и ведет наблюдение за несколькими хостами. Сетевая система обнаружения вторжений получает доступ к сетевому трафику, подключаясь к хабу или свитчу, настроенному на зеркалирование портов, либо сетевое TAP устройство.
- Пример – Snort (www.snort.org).

Основанная на протоколе СОВ (PIDS)

Система (либо агент), которая отслеживает и анализирует коммуникационные протоколы со связанными системами или пользователями. Для веб-сервера подобная СОВ обычно ведет наблюдение за HTTP и HTTPS протоколами. При использовании HTTPS СОВ должна располагаться на таком интерфейсе, чтобы просматривать HTTPS пакеты еще до их шифрования и отправки в сеть.

Узловая СОВ Host-based IDS (HIDS)

Система (или агент), расположенная на хосте, отслеживающая вторжения, используя анализ системных вызовов, логов приложений, модификаций файлов (исполняемых, файлов паролей, системных баз данных), состояния хоста и прочих источников. Пример – OSSEC (www.ossec.net).

Гибридная СОВ Hybrid IDS

- Совмещает два и более подходов к разработке СОВ. Данные от агентов на хостах комбинируются с сетевой информацией для создания наиболее полного представления о безопасности сети.
- Пример – Prelude (www.prelude-ids.org).

Пассивные и активные СОВ

- **Пассивная СОВ** - при обнаружении нарушения безопасности, информация о нарушении записывается в лог приложения, а также сигналы опасности отправляются на консоль и/или администратору системы по определенному каналу связи.
- **Активная СОВ** (Система Предотвращения Вторжений, IPS, Intrusion Prevention system) ведет ответные действия на нарушение, сбрасывая соединение или перенастраивая межсетевой экран для блокирования трафика от злоумышленника. Ответные действия могут проводиться автоматически либо по команде оператора.

Классификация систем предотвращения вторжений

- Сетевые IPS (Network-based Intrusion Prevention, NIPS): отслеживают трафик в компьютерной сети и блокируют подозрительные потоки данных.
- IPS для беспроводных сетей (Wireless Intrusion Prevention Systems, WIPS): проверяет активность в беспроводных сетях. В частности, обнаруживает неверно сконфигурированные точки беспроводного доступа к сети, атаки человек посередине, спуфинг mac-адресов.
- Поведенческий анализ сети (Network Behavior Analysis, NBA): анализирует сетевой трафик, идентифицирует нетипичные потоки, например DoS и DDoS атаки.
- Система предотвращения вторжений для отдельных компьютеров (Host-based Intrusion Prevention, HIPS): резидентные программы, обнаруживающие подозрительную активность на компьютере.

Эксплойт

- От англ., - эксплуатировать
- Компьютерная программа, фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на вычислительную систему.
- Целью атаки может быть как захват контроля над системой (повышение привилегий), так и нарушение её функционирования (DoS-атака).

Виды эксплойтов

- Эксплойты для операционных систем
- Эксплойты для прикладного ПО (проигрыватели, офисные пакеты и т. д.)
- Эксплойты для браузеров
- Эксплойты для интернет-продуктов (IPB, WordPress, VBulletin, phpBB)
- Эксплойты для интернет-сайтов (facebook.com, hi5.com, livejournal.com)
- Прочие эксплойты

СОВ и Межсетевой экран

- Межсетевой экран отличается тем, что ограничивает поступление на хост или подсеть определенных видов трафика для предотвращения вторжений и не отслеживает вторжения, происходящие внутри сети.
- СОВ, напротив, пропускает трафик, анализируя его и сигнализируя при обнаружении подозрительной активности. Обнаружение нарушения безопасности проводится обычно с использованием эвристических правил и анализа сигнатур известных компьютерных атак.

Спасибо за внимание