Основы безопасности информационных технологий

Системы обнаружения атак и вторжений

Содержание лекции

- Основные понятия
- Классификация систем обнаружения вторжений
- Обнаружение сигнатур
- Обнаружение аномалий
  - Метод Data Mining
  - Методы технологии мобильных агентов
- Методы обхода сетевых СОВ
- Методы обхода хостовых СОВ

Основные понятия

Атака — действия, предпринимаемые злоумышленником, против компьютера (или сети) потенциальной жертвы.

Вторжение — несанкционированный вход в информационную систему.

Система обнаружения вторжений — комплекс, который по результатам анализа контролируемых и собираемых данных принимает решение о наличии атаки или вторжения.

Ложная тревога — генерация сигнала об обнаружении атаки (вторжения), которой не было.

Пропуск — пропуск атаки или вторжения.

Классификация систем обнаружения вторжений

Функции и особенности проектирования и реализации СОВ :

- подход к обнаружению
- защищаемая система
- структура СОВ
- источник данных (для принятия решения)
- время анализа
- характер реакции

Обнаружение сигнатур

Сигнатура - множество условий, при удовлетворении которых наступает событие, определяемое как атака или вторжение.

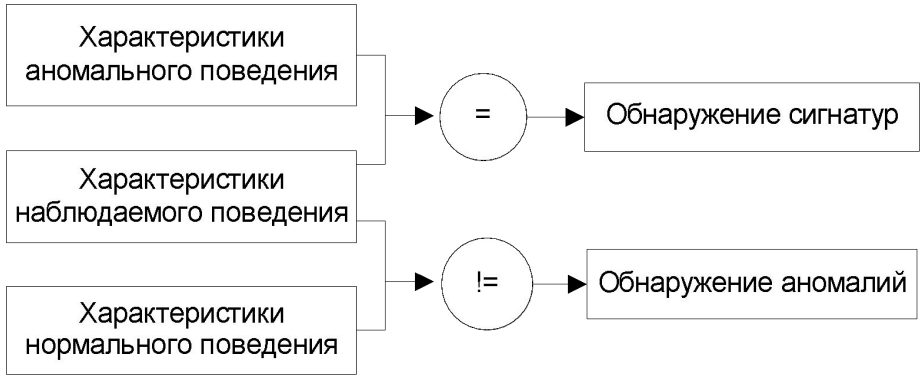
Подходы к обнаружению сигнатур:

- совпадение с шаблоном
- совпадение с шаблоном состояния
- анализ на основе шаблона используемого протокола
- эвристический подход

Виды сигнатур

- *Сигнатуры эксплойта*
- *Сигнатуры уязвимости*
- *Сигнатуры аномалий протоколов*

Обнаружение аномалий



Подходы к обнаружению:

- методы Data Mining
- методы технологии мобильных агентов
- методы построения иммунных систем
- применение генетических алгоритмов
- применение нейронных сетей

Метод Data Mining

Технологию Data Mining можно определить как процесс обнаружения в необработанных данных:

- ранее неизвестных
- нетривиальных
- практически полезных
- доступных интерпретации знаний, необходимых для принятия решений в различных

Классы Data Mining

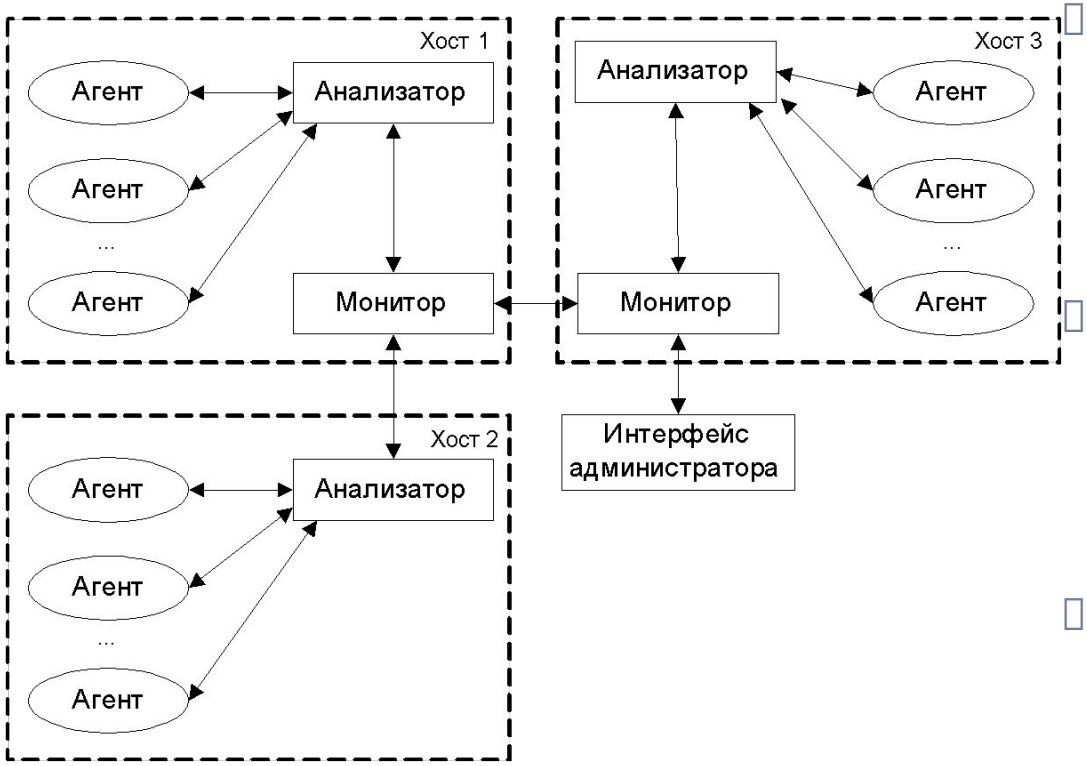
- предметно-ориентированные аналитические системы
- нейронные сети
- системы рассуждений на основе аналогичных случаев
- деревья решений

Методы технологии мобильных агентов

Достоинства использования технологии агентов для сбора и анализа :

- каждый агент можно запрограммировать на получение данных из своего источника
- возможность независимого старта и остановки работы различных агентов
- агенты могут быть программами, написанными на различных языках программирования

Autonomous Agent For Intrusion Detection



Возможности:

- обучение агентов с использованием различных методов машинного обучения
- эволюция агентов во времени с использованием генетического программирования
- сохранение состояния контролируемых сеансов между сеансами
- мобильность агентов

Методы обхода сетевых СОВ

Основные методы:

- сбивание с толку
- фрагментация
- шифрование
- перегрузка

Методы обхода хостовых СОВ

Основные методы:

- контроль расположения и целостности файлов
- сбивание с толку
- вставка нулевого знака в запрос после указания метода
- перехват приложения