СИСТЕМА ОБНАРУЖЕНИЯ АТАК ЗАСТАВА-IDS

ЗАСТАВА-IDS — комплекс программного обеспечения, предназначенный для обнаружения компьютерных атак на систему или сеть на основе анализа сетевого трафика стека протоколов TCP/IP со скоростью передачи данных не менее 1 Гбит/сек сигнатурным методом.

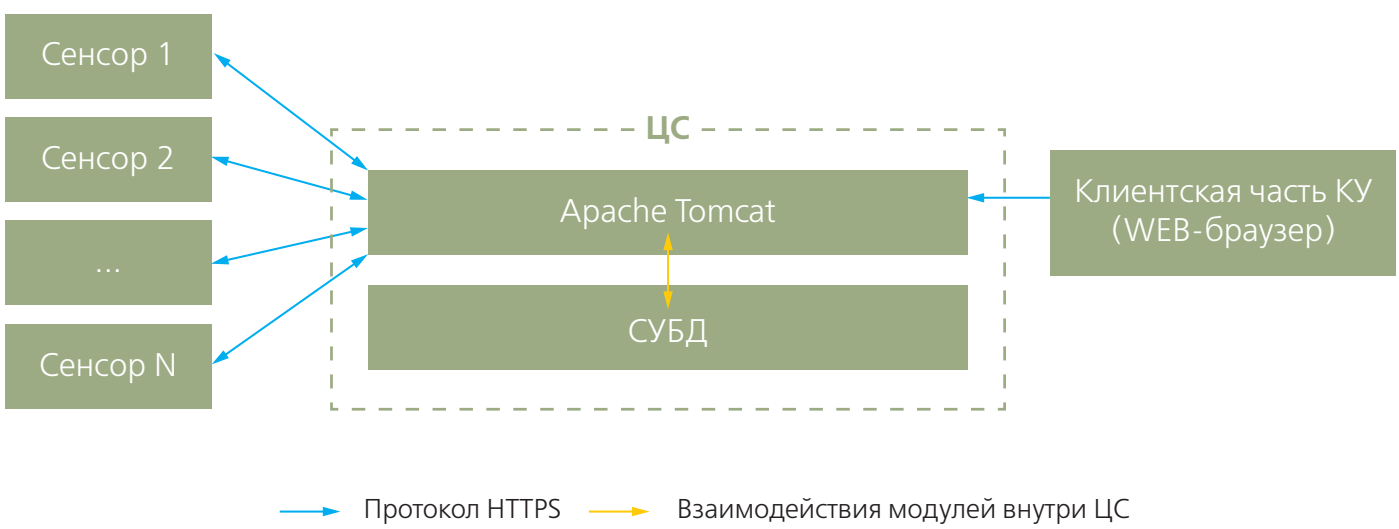
КЛЮЧЕВЫЕ ПРЕИМУЩЕСТВА

- Подключение до 100 сенсоров к одному серверу.
- Гибкая настройка системы:
  - задание контролируемых подсетей и IP-адресов;
  - создание и выбор сигнатур;
  - задание индивидуальных правил для каждого сенсора.
- Маскирование СОА в сети и невыявление её на сетевом уровне стандартными средствами операционных систем.
- Различные способы подключения к каналам связи: по схеме «Т-образие» или «в разрыв».
- Обнаружение атак, описанных в базе сигнатур, с вероятностью более 99,5%.

сделано в РОССИИ

АРХИТЕКТУРА И ОСНОВНЫЕ ФУНКЦИИ

ЗАСТАВА-IDS состоит из датчиков (сетевых сенсоров) и центрального сервера (ЦС). Сетевой сенсор подключается к контролируемым каналам связи по схеме «Т-образие» или «в разрыв». Также устанавливается соединение каждого сенсора с центральным сервером.



В основе работы сетевого сенсора лежит сигнатурный анализ сетевого трафика – выявление короткого шаблона (сигнатуры) для каждой известной атаки и проверка всего трафика на наличие этого шаблона. Основные задачи центрального сервера – управление подключенными сетевыми сенсорами, а также сбор с них и отображение администратору комплекса информации об обнаруженных компьютерных атаках.

УСТРОЙСТВО И ВОЗМОЖНОСТИ СЕТЕВОГО СЕНСОРА

Сенсор состоит из следующих компонент:

- Модуль захвата трафика.
- Сигнатурный анализатор.
- Модуль взаимодействия с центральным сервером.

Сенсор может работать в одном из трёх режимов:

- basic-ids: сенсор подключен по схеме «Т-образие», может наблюдать один или несколько интерфейсов, при обнаружении атаки возможно только уведомление о ней;
- bridge-ids: сенсор подключен к двум интерфейсам по схеме «в разрыв», т.е. в качестве моста между двумя подсетями; обнаруживает атаки как происходящие внутри каждой подсети, так и из одной подсети в другую;
- inline-ips: сенсор также подключен к двум интерфейсам по схеме «в разрыв», однако может блокировать подозрительный трафик, выступая при этом как система не только обнаружения, но и предотвращения вторжений.

По сравнению с любыми другими продуктами подобного назначения, где наиболее часто применяется технология PCAP, отличающаяся очень высокой нагрузкой на процессор, в ЗАСТАВА-IDS используется библиотека (модуль ядра) PF_RING, которая обеспечивает минимальную нагрузку на процессор и отсутствие потерянных пакетов. В случае необходимости, PF_RING имеет обратную совместимость с PCAP.

В ПО сенсора входит сервис для управления им непосредственно из консоли, что позволяет произвести первичную настройку и проверить работу сенсора сразу после установки.

УСТРОЙСТВО И ВОЗМОЖНОСТИ ЦЕНТРАЛЬНОГО СЕРВЕРА (ЦС)

ЦС состоит из следующих компонент:

- СУБД PostgreSQL.
- Сервер-приложения Apache Tomcat.
- Модуль приёма информации об обнаруженных компьютерных атаках.
- Модуль управления.
- Модуль консоли управления (КУ).

Серверные приложения центрального сервера осуществляют управление сенсорами, собирают с них информацию об атаках, а также обеспечивают работу веб-интерфейса консоли управления.

КОНСОЛЬ УПРАВЛЕНИЯ (КУ)

После установки ЗАСТАВА-IDS работа с системой может осуществляться через веб-интерфейс центрального сервера. Кроме того, в КУ есть раздел для индивидуальной работы с каждым сенсором, в котором предусмотрены следующие основные команды: запуск, остановка, добавление и обновление правил и настроек, самотестирование. Для каждого сенсора можно просмотреть журнал атак, имеющий разнообразные возможности фильтрации и сортировки для удобного отображения и сбора статистики.