ООО «Стратегия Защиты»

ПРОГРАММНЫЙ МОДУЛЬ
«Система предупреждения кибератак "Сонар-1М"
Шифр: СПК "Сонар-1М"

Описание программы

2018

АННОТАЦИЯ

Настоящий документ предназначен для изучения сведений о логической структуре и функционировании программного комплекса СПК "Сонар-1М". Документ также содержит сведения о назначении и функциональных возможностях.

Документ состоит из трех частей:

- раздел «Назначение программы». Здесь указаны сведения о назначении программы и информация, достаточная для понимания функций программы и ее эксплуатации
- раздел «Условия выполнения программы». Здесь указаны условия, необходимые для выполнения программы (минимальный состав аппаратных и программных средств и т.п.).
- раздел «Описание программы». Здесь описаны структура и принцип функционирования СПК «СОНАР-1М».

СОДЕРЖАНИЕ

1. НАЗНАЧЕНИЕ ПРОГРАММЫ

1.1 Назначение

Программный комплекс SONAR-Framework предназначен для выполнения анализа трафика в режиме «реального времени», выявление уязвимостей, связанных с ошибками в конфигурациях системного программного обеспечения и сетевого оборудования, которые могут быть использованы нарушителем для реализации атак на систему и компрометации защищаемых данных.

1.2 Функциональные возможности

Функционал СПК «СОНАР-1М» включает в себя:

- инспектирование входящего и исходящего сетевого трафика;
- анализ входящего и исходящего трафика по сигнатурам, сравнение сигнатур с набором правил (политик), имеющихся в составе модуля. При соответствии сигнатур осуществляется запись в журнал отчета, фиксируя следующие поля:
  - дата и время события (инцидента);
  - краткая идентификация сигнатуры;
  - ip-адрес и порт отправителя;
  - ip-адрес и порт получателя;
  - данные (при их наличии).
- при обнаружении вредоносных сигнатур, атак и прочих аномалий модуль осуществляет распределение событий по срабатыванию, видам атак, сигнатурам, типам событий и собирает статистику по инцидентам;
- формирование отчетов о произошедших событиях и инцидентах.

В составе СПК «СОНАР-1М» присутствует Web-интерфейс управления организующий следующие действия:

- мониторинг за инцидентами, произошедшими в контролируемой системе или сети;
- наблюдение за атаками с распределением по видам атак;
- отображение диаграмм по ip-адресам, портам и событиям;
- геолокацию атак;
- сводную информацию по событиям за текущий день или за выбранный период;

- вывод отчетов по событиям за текущий день или за выбранный период;
- подсчет обнаруженных событий, выводит информаци по наиболее часто встречающимся сигнатурам, самым частым атакующим и атакуемым ip-адресам.

1.3 Функциональные ограничения

Для выполнения анализа трафика требуется подключение сервера СПК «СОНАР-1М» к порту, работающему в режиме зеркалирования трафика (SPAN порту), поскольку программный комплекс выполняет пассивное сканирование уязвимостей удаленных подсетей и устройств.

По результатам проводимого анализа зарегистрированные инциденты безопасности помещаются в базу данных и хранятся локально. Необходимый объем устройств хранения информации зависит от интенсивности трафика и требований по времени хранения событий. Рекомендуется выделять объем исходя из расчета – 500Мб в неделю при регистрации 100 событий ежедневно.

Развернутый программный комплекс занимает до 4 Гб дискового пространства.

2. УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММЫ

2.1 Требования к техническим средствам

2.1.1 Минимальные системные требования (нерекомендуемые):

- Сервер с процессором Intel Atom 1.6 Ггц;
- 1 Гб ОЗУ;
- 20 Гб свободного места на жестком диске ПЗУ;
- 1 ethernet-карта.

2.1.2 Оптимальные (рекомендуемые) системные требования:

- Сервер, с процессором Intel Xeon 2 ГГц;
- 4 Гб ОЗУ;
- 300 Гб свободного места на жестком диске, желательно, распределение отдельного диска или раздела для /SONAR, /var;
- 2 ethernet-карты с поддержкой pf_ring.

2.2 Требования к программным средствам

СПК «СОНАР-1М»-Framework включает несколько готовых программных пакетов, подготовленных для работы с операционной системой CentOS 6.9. Для корректного функционирования комплекса в системе должны быть установлены следующие компоненты:

- mysql-server-5.1.73
- php-5.3.3
- libpcap-1.4.0
- apache-2.2.15

Примечание: версии программных компонентов должны быть не ниже указанных.

3. ОПИСАНИЕ ПРОГРАММЫ

СПК «СОНАР-1М» представляет собой программный комплекс, предназначенный для обнаружения вторжений, позволяющие отслеживать такие виды вредоносной деятельности, как DoS атаки, сканирование портов, попытки проникновения в сеть и другие. Функционирование подсистемы обеспечивается операционной системой CentOS 6.9. Ядром подсистемы является СПК «СОНАР-1М» Framework включающий набор программных проектов (в том числе проектов с открытым кодом), подготовленных скриптов и конфигурационных файлов. Фреймворк обеспечивает пассивный анализ трафика, контроль, хранение и работу с инцидентами информационной безопасности. Функциональная схема СПК «СОНАР-1М» представлена на рисунке 1.

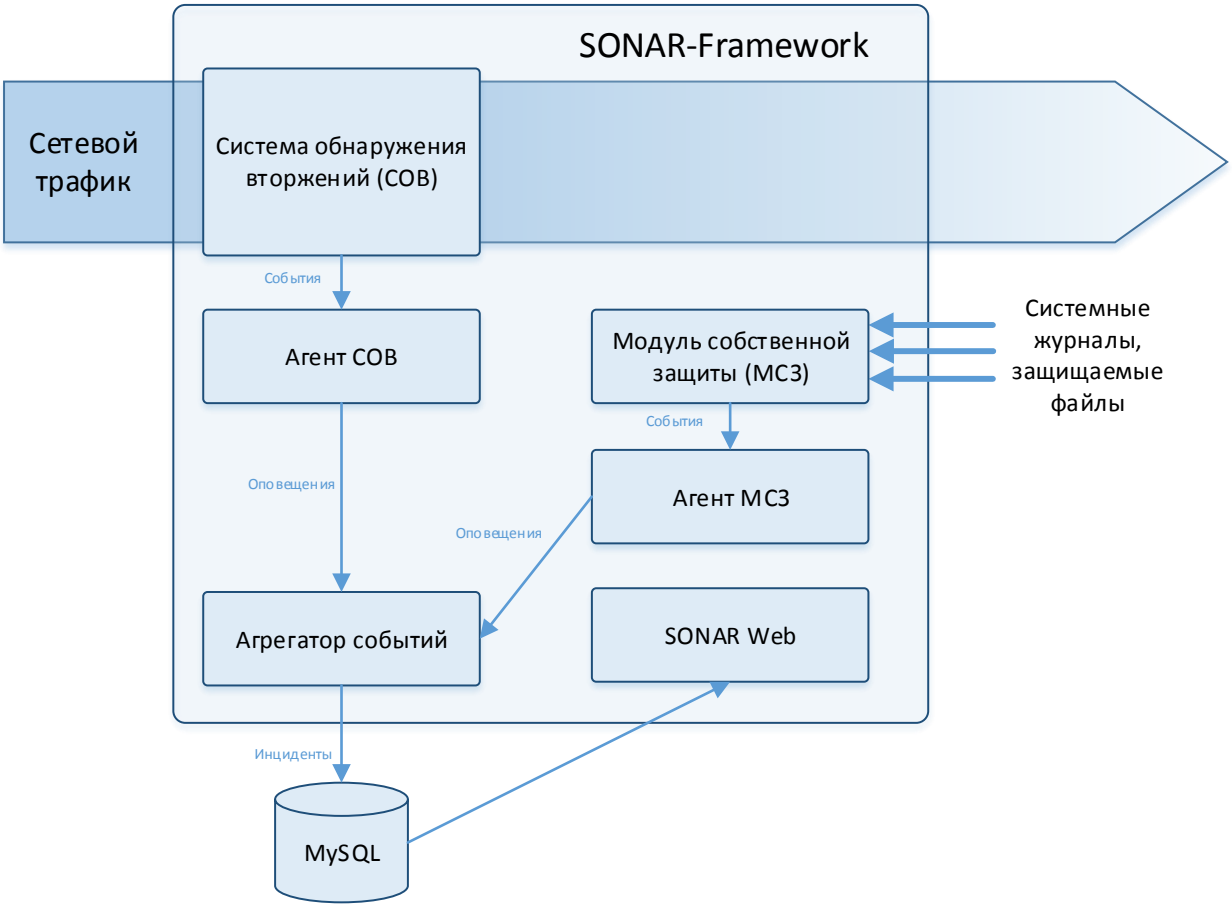

Рисунок 1. Функциональная схема СПК «СОНАР-1М»

Анализ сетевого трафика выполняется многопоточной системы предупреждения кибератак (СПК), позволяющей выполнять обработку большого объема трафика. СПК состоит из нескольких модулей: захвата, разбора захваченных пакетов, обнаружения сигнатур и вывода событий. Обнаружение сигнатур выполняется по правилам СПК совместимым с

форматом правил snort, что позволяет подключать правила из широкого спектра баз правил. Правила содержат компоненты: действие (pass, drop, reject или alert), заголовок (IP/порт источника и назначения), маску, применяемую к полезной нагрузке и описание.

До модуля обнаружения сигнатур захваченный трафик идет одним потоком, поскольку это оптимально с точки зрения детектирования (см. Рисунок 2). Загрузка процессора модулем обнаружения напрямую зависит от количества обрабатываемых правил. Для распределения нагрузки между ядрами процессора, обнаружение сигнатур выполняется в многопоточном режиме.

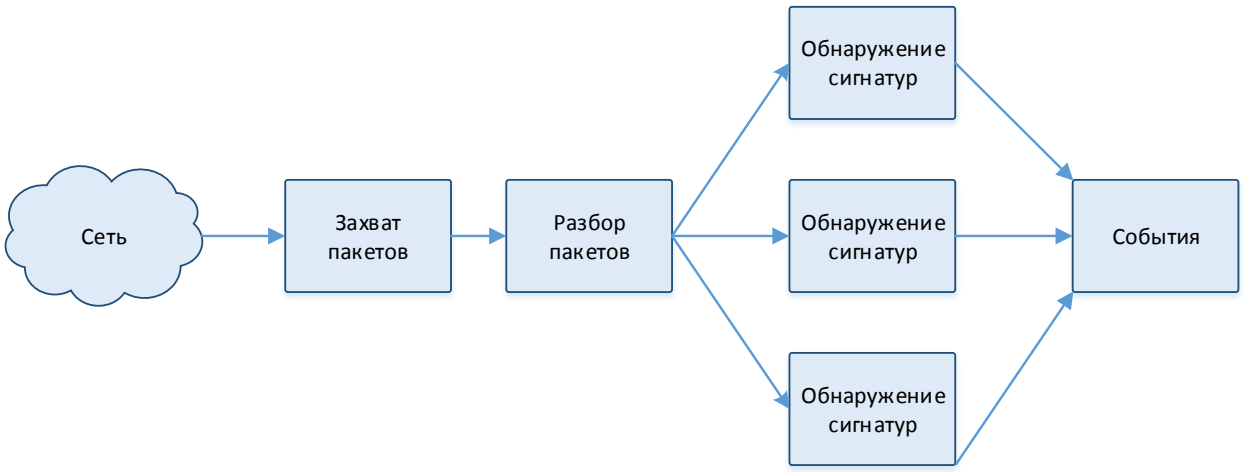

Рисунок 2. Функциональная схема СПК

При срабатывании правил СПК генерирует события, которые формируются в бинарный унифицированный файл формата unified2 и перенаправляются утилите агенту СПК. Интерпретатор, входящий в состав агента СПК, принимает на вход файлы формата unified2 и преобразует в читаемый формат для записи в лог-файлы либо в базу данных. Для обозначения выходных данных интерпретатора примем термин «оповещение». Оповещения можно записывать сразу в базу данных MySQL, но в СПК «СОНАР-1М» Framework применяется агрегатор событий, выполняющий прием информаций от разных агентов и дополнительно обрабатывающий оповещения.

Агрегатор событий представляет собой набор расширяемых серверных tcl-скриптов, получающих оповещения от различных источников, разделяющих оповещения на несколько категорий, по которым накапливается статистика. Оповещения от агентов помещаются в базу инцидентов информационной безопасности, управляемой агрегатором.

Модуль собственной защиты (МСЗ) выполняет анализ базовых журналов операционной системы CentOS 6.9 и журналов СПК , проверку целостности файлов, обнаружение вредоносных утилит или модулей ядра (rootkit). Анализ выполняется по правилам СПК совместимым с форматом правил OSSEC. Данные правила содержат описание наблюдаемого события и действие. При обнаружении события описанного в правилах МСЗ регистрирует данное событие и при наличии соответствующих опций заданных в правиле, выполняет временную блокировку (по умолчанию – 5 минут) ip адреса либо пользователя в системе. Зарегистрированные события безопасности через агента МСЗ отправляются на агрегатор событий.

База данных MySQL хранит большое количество событий, для выявления нормального поведения, обнаружения аномалий, раскрытия передовых угроз и удаления ложноположительных результатов применяется web-интерфейс, входящий в состав СПК «СОНАР-1М». Инструментарий web-интерфейса позволяет оператору проанализировать сетевые активности, обнаружить аномалии, провести корреляцию событий с целью идентификации нарушений и принятия мер. Инструментарий включает возможности формирование диаграмм, выборку по различным параметрам, детализацию событий и сетевых пакетов, вызвавших инцидент.