Система обнаружения вторжений Dragon

Что такое система Dragon

Dragon - система обнаружения вторжений (Intrusion Detection System - IDS), предназначенная для обнаружения атак, нацеленных на сетевые ресурсы или хосты. Для этого Dragon собирает всю необходимую информацию через своих агентов (сенсоров), анализирует ее и результаты посылает на станцию управления или системному администратору.

Использование межсетевых экранов позволяет удаленным пользователям подключаться к ресурсам сети. Правильно настроенный межсетевой экран может снизить риск проникновения в сеть и защитить ее от внешних воздействий, но не полностью. Используя большое количество существующих приложений и технологий компьютерным взломщикам удается проходить через межсетевые экраны и попадать в сеть. Для борьбы с такими взломщиками внутри сети и предназначена система Dragon.

Архитектура и составные части системы

Система Dragon состоит из сенсоров, сервера, процессоров потоков сообщений и агентов. Архитектура системы позволяет гибко использовать каждый из этих компонентов в различных конфигурациях и комбинациях друг с другом.

Сенсор может быть либо типа Network Intrusion Detection System (NIDS), либо Host Based Intrusion Detection System (HIDS). Сенсоры могут работать самостоятельно или в паре с другими компонентами. В конфигурации, когда сенсоры работают самостоятельно, Policy Manager не может централизованно управлять ими и данные от сенсоров не передаются в процессоры для сбора и анализа информации.

Сетевой сенсор осуществляет пассивный мониторинг сети, распознает атаки и вырабатывает информацию о событиях в зависимости от установленных в нем сигнатур и сетевых настроек. Данный сенсор анализирует пакеты на уровне протоколов и приложений, применяя метод сигнатур и аномалий для идентификации злонамеренных действий в сети.

Хост-сенсор устанавливается непосредственно на персональный компьютер или сервер для их мониторинга и способен отслеживать атрибуты файлов MD5 (зашифрованный файл), установки доступа, размеры и содержимое файлов, трэпы SNMP, системные журналы и настройки регистра Windows NT. Этот сенсор может отслеживать системные журналы приложений, запущенных на хосте (почтовый сервер, веб-сервер, DNS-сервер и FTP-сервер).

Хост-сенсор может также просматривать log-сообщения межсетевых экранов, сообщения от маршрутизаторов или от любого другого устройства, которое поддерживает протокол SNMP или SYSLOG. Для маршрутизаторов и межсетевых экранов, которые не имеют локальной операционной системы для установки сенсора, используют syslog-серверы, на которые устанавливаются хост?сенсоры, принимающие syslog-сообщения и передают их дальше на сервер Dragon для последующего анализа. Поддерживаются коммерческие (Checkpoint FW-1, Symantec Raptor, Rapidstream, Netscreen, Cyberguard, Cisco PIX) и свободно распространяемые межсетевые экраны.

Также как и сетевой, хост?сенсор использует сигнатуры для идентификации и анализа полученных сообщений. Библиотека сигнатур включает в себя список подозрительных событий для большинства операционных систем. Библиотека сигнатур также включает сообщения поступающие от многих приложений и сервисов, таких как: Secure Shell, Sendmail, Qmail, Bind, Internet Information Server и Apache.

Хост?сенсор способен читать log-сообщения приложений, которые шифруют свой трафик, просматривать SSH-приложения или транзакции веб-сервера, защищенные с помощью протокола SSL. Этот сенсор можно использовать для идентификации таких протоколов, но он не может расшифровать полученные данные и "заглянуть" внутрь сессии. Однако он предоставит такую SSH-информацию, как отказ пользователю в доступе, кто пытается экспортировать X-сессию через SSH и т. д.

У хост-сенсора имеется функция проверки целостности файлов, которая оповещает сетевого администратора в случае, если системные файлы или файлы защиты были изменены, удалены или к ним осуществлялся доступ.

Если сенсоры имеют конфигурацию типа Enterprise Sensor, то они могут передавать свои данные в Event Flow Processor, и Policy Manager может управлять ими. В противном случае события хранятся локально на диске.

Сервер Dragon является системой управления и отчетности. Сенсоры взаимодействуют с ним через защищенный (зашифрованный) канал. Связь между сенсорами может быть инициализирована в обоих направлениях - от агентов к серверу и от сервера к агентам. Это является важным моментом, так как межсетевые экраны защищают входящий трафик, а сервер может инициализировать исходящий трафик. Сервер Dragon включает в себя пять приложений (policy manager, alarmtool config, real time console, forensics console, trending console), каждое из которых может быть доступно через веб-броузер.

Модуль Policy Manager осуществляет управление настройкой сенсоров. Библиотеки сигнатур и настройки конфигурации могут быть применены и записаны для каждого сенсора (существует возможность обновления библиотек сигнатур). Конфигурация загружается в сенсоры через зашифрованное соединение. Для распределения нагрузки на Policy Manager можно использовать несколько таких модулей. Один сенсор может контролироваться только одним таким модулем.

Модуль Alarmtool реализует механизм генерации тревожных сообщений. Сигналы генерируются в зависимости от степени важности: по типу события, времени появления события и механизму отправки тревожных сообщений, которые могут быть посланы по SNMP, SMTP (e-mail), SYSLOG. Например, Alarmtool можно настроить так, чтобы все сообщения отправлялиь по электронной почте разным адресам, или одни сообщения посылаются по одним адресам, а другие по другим. Механизм генерации тревожных сообщений находится только на сервере и не встраивается в сенсоры. Такая архитектура не требует от сенсоров останавливать свои процессы и заниматься отправкой сообщений в тот момент, когда они следят за поступающей к ним информацией.

Консоль реального времени отображает любые изменения, произошедшие в сети и позволяет анализировать их. События считываются из процессора потока событий и записываются в буфер. Хранение одного миллиона событий в буфере занимает около 24 Мбайт памяти. Поскольку система не считывает события из базы данных, а хранит их в памяти, то события, произошедшие за определенный период времени, всегда доступны из оперативной памяти. Консоль позволяет автоматически обновлять события через 1, 5 или 15 минут. Для анализа за более длительный период используются Forensics и Trending-консоли.

Историческая консоль позволяет осуществлять детальное изучение событий, произошедших в прошлом в зависимости от того, как долго записывались данные в базу.

Консоль трендов анализирует данные за более длительный период времени. Эта консоль основана на реляционной базе данных MySQL, где все данные хранятся в виде архивов. События считываются из процессора потока событий и записываются в базу MySQL. Эта база может расширяться с использованием других баз, таких как Oracle, Sybase или MS-SQL. Информация может быть проанализирована за любой период времени: недели, месяцы и даже годы, для идентификации возможной или произошедшей атаки.

Процессор потока событий (Event Flow Processor - EFP) получает данные о событиях от одного или более сенсоров. Эти события могут либо передаваться другому EFP на более верхний уровень, либо храниться локально. Архитектура системы Dragon позволяет работать со множеством процессоров, расположенных в разных местах сети, создавая иерархическую структуру. Например, EFP могут быть размещены так, чтобы каждый администратор отвечающий за EFP, мог просматривать события, относящиеся только к его зоне ответственности.

Агенты Dragon:

- Агент базы данных Dragon записывает каждое полученное событие в базу данных dragon.db. Отчет по событиям можно получить через командную строку или графический интерфейс.
- Агент MD5 читает MD5-ссылки (ссылки зашифрованных событий), поступающие от хост?агента и записывает их в свою базу. В случае несоответствия информации в MD5, этот агент записывает соответствующее событие.
- Replication-агент используется для передачи событий между компонентами Dragon и может передавать события от сенсора к EFP, или между двумя EFP. Replication-агент устанавливается на сенсор, или EFP, который инициализирует соединение. Для примера, если EFP(A) посылает события на верхний уровень к EFP(B), то агент должен быть установлен на EFP(B), если соединение инициализируется EFP(B). Или если агент находится на EFP(A), то соединение инициализируется EFP(A).
- Alarmtool-агент вырабатывает и посылает предупреждающие сообщения (по электронной почте, SNMP, Syslog) в соответствии с определенными событиями.
- ??Export Log-агент - генерирует в формате ASCII запись для каждого события, которая используется для экспорта данных о событиях из Dragon в другую систему и для посылки их в Trend Analysis Tool.

Принцип работы Dragon

Dragon использует три метода для определения подозрительной активности:

1. Программирование для сенсоров сигнатур;
2. Сенсоры программируются для определения аномалий, которые похожи на атаки взломщиков. Эти аномалии неточно отражают саму технику взлома, но все же высокоэффективны для определения сканируемого порта, сетевых зондов, атак типа переполнения буферов и отказа в сервисе;
3. Сенсоры могут определять возникшие отклонения при обходе защиты, включающие использование неавторизованных сетевых сервисов, запущенные приложения с необычными номерами портов и регистрационные записи межсетевых экранов о запрете сетевых сессий.

Анализ информации о возможности вторжения является важной частью в системе обнаружения вторжения. Существуют три техники определения сходства со вторжением:

1. Система конфигурируется таким образом, чтобы искать потенциальные вторжения. Эта система не создает отчета по атакам для которых нет сигнатур, определяющих вторжение;
2. Система определяет факт и время появления события и после этого снова сканирует систему, чтобы убедиться в правильности принятия решения. Эта техника удобна, когда количество IP?адресов слишком велико и полное сканирование затруднительно;
3. Создается база данных по всем известным видам вторжений и когда происходит событие, исследуется база данных на любое с ним сходство. Если сходство найдено, тогда вырабатывается сообщение, в котором указывается событие и обнаруженное сходство со вторжением.

Основные технические характеристики Dragon

- Производительность системы в осуществлении мониторинга от 50 до 500 Мбит/сек;
- Поддержка сетевым сенсором 10/100/1000 Ethernet;
- Библиотека более чем 3000 сигнатур;
- Поддержка с одной консоли до 50 сетевых сенсоров и до 500 хост?сенсоров;
- Хост?сенсор поддерживает операционные системы Linux, Solaris, HP-UX, FreeBSD, OpenBSD, Windows NT/2000;
- Сетевой сенсор поддерживает операционные системы Solaris Sparc, Linux, FreeBSD;
- Сервер Dragon поддерживает операционные системы Solaris, Linux, FreeBSD.