ПРОГРАММНЫЙ КОМПЛЕКС АУДИТА БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ ДЛЯ ПРОТИВОДЕЙСТВИЯ АТАКАМ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Понамарчук А. И., Вахаб Алаа

Борботько Т. В. – д-р. техн. наук, профессор

Рассмотрен состав и назначение компонентов программного комплекса обеспечивающего моделирование информационных систем, уязвимостей таких систем для оценки возможности их использования при реализации атак.

Современные информационные системы используются для обработки различных сведений, в том числе в банковском секторе. Атаки на подобные системы приносят существенный ущерб банкам и влияют на их репутацию. Одним из способов противодействия таким угрозам является обнаружение уязвимостей в информационной системе и их своевременное устранение. Для практической реализации указанного способа созданы программные средства, которые позволяют обнаруживать уязвимости, а так же проверять возможность их использования при реализации тех или иных атак. Однако существенной проблемой применения таких средств является решение задачи снижения вероятности ложных тревог. Такая задача может быть решена за счет повышения достоверности получаемых сведений, когда события безопасности регистрируются несколькими датчиками и решение о наличии угрозы принимается на основе корреляции таких событий.

Разработанный комплекс основан на использовании программного обеспечения VMware Workstation и включает в себя:

- виртуальные машины с IDS/IPS, HoneyPot и с программным обеспечением для имитации атак;
- интерфейсы настройки HoneyPot, просмотра сообщений о событиях безопасности, управления атаками.

Первая виртуальная машина содержит следующие сервисы:

- системы IDS/IPS и HoneyPot;
- HTTP-сервер и PHP-интерпретатор для интерфейса конфигурирования HoneyPot;
- систему просмотра сообщений безопасности IDS/IPS.

В качестве системы IDS/IPS использовалось программное обеспечение Snort. Система HoneyPot включает в себя подсистемы: honeyd, arpd и набор скриптов. Интерфейс настройки HoneyPot позволяет упростить конфигурирование подсистемы honeyd, за счет исключения необходимости редактирования файла настроек в ручном режиме. Базовая настройка HoneyPot заключается в создании шаблона HoneyPot и его применение.

Интерфейс просмотра сообщений о событиях безопасности реализует процедуры аутентификации пользователей программного комплекса, разграничения прав их доступа к системному журналу, отображения событий с учетом их корреляции по различным критериям в виде графиков и отчетов.

Вторая виртуальная машина обеспечивает функционирование программного комплекса моделирования атак, который выполнен по модульному принципу. Основными компонентами данного комплекса являются:

- консоль управления;
- модуль эксплоитов - для проверки целевой системы на уязвимость, а также выполнение самого кода эксплоита;
- модуль реализующий атаку «отказ в обслуживании» (DoS) – для проверки целевой системы на подверженность DoS атакам;
- модуль реализующий атаку «подмены» (Spoofing) – для проверки целевой системы на возможность такой атаки;
- модуль фаззинга (Fuzzing) - технология тестирования программного обеспечения, когда вместо ожидаемых входных данных программе передаются случайные или специально сформированные данные. В большинстве своем это некорректно составленные данные. Смысл такой проверки сводится к тому, что программист не знает, какие данные будут переданы приложению/протоколу/функции, поэтому его задача предусмотреть и проверить как можно больше вариантов;
- модули нагрузки и кодирования – для возможности установить кодирующее устройство во время выполнения процедуры передачи данных или изменить полезную нагрузку.

Разработанный программный комплекс позволяет оценить защищенность моделируемых информационных систем, выявить уязвимости их различных сервисов, проследить возможные сценарии атак, за счет использования систем-ловушек, проверить корректность работы системы обнаружения атак, за счет реализованной в нем методике, основанной на сравнении информации об атаках получаемых от различных источников.

Список использованных источников:

1. Ограбление по-российски: хакеры Carbanak сумели похитить $1 млрд // Aercom.by. Безопасность в Беларуси [Электронный ресурс]. – 2015. – Режим доступа : http://aercom.by/ograblenie-po-rossijski-xakery-carbanak-sumeli-poxitit-1-mlrd/. – Дата доступа : 12.03.2015.