

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; модуль, реализующий атаку «отказ в обслуживании» (DoS); модуль, реализующий атаку «подмены» (Spoofing); модуль фаззинга (Fuzzing); модули нагрузки и кодирования.

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.

АНАЛИЗ МЕТОДОВ И СРЕДСТВ УПРАВЛЕНИЯ ТОПОЛОГИЕЙ СЕТИ MANET

Д.Д. Альхимович

Рассматриваются сети MANET (Mobile Ad-Hoc Networks) — мобильные самоорганизующиеся сети с динамической архитектурой, предполагающие отсутствие фиксированной сетевой инфраструктуры (базовых станций) и централизованного управления. Одной из основных задач оперативного управления сетью MANET является управление ее топологией. Топология определяет потенциальные возможности сети по доставке данных между взаимодействующими узлами. Мобильность (отказы, уничтожение) узлов приводит к разнообразным сетевым топологиям. Тем не менее, сеть должна поддерживать необходимый уровень пропускной способности, который во многих ситуациях не удастся достичь только за счет маршрутизации. Изменение топологии сети может иметь более значительный эффект, в отличие от использования адаптивной маршрутизации. Разработан алгоритм оперативного управления топологией MANET. Алгоритм предполагает оценку параметров функционирования MANET и при их уменьшении ниже допустимых значений — выработку управляющих воздействий (изменение мощностей передач узлов), позволяющих осуществить пользовательскую или системную оптимизацию. Применение алгоритма позволяет увеличить пропускную способность сети 1,5–2 раза. Таким образом, для повышения эффективности функционирования MANET, необходимо осуществлять оперативное управление топологией сети и осуществлять управление построением и поддержанием маршрутов при полученной топологии.

Литература

1. *Миночкин А.И., Романюк В.А.* Методика оценки методов управления в мобильных радиосетях // 15-я международная Крымская конференция «СВЧ-техника и телекоммуникационные технологии» (КрыМиКо), Севастополь, 2005. С. 43–44.