МЕТОД ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ НА ОСНОВЕ ВЕРОЯТНОСТНОЙ ЛОГИКИ

Никитина Л.А., Будашев И.В.
Национальный технический университет «Харьковский политехнический институт», г. Харьков

Атака сервера - один из самых распространенных типов кибератак, который представляет серьезную проблему для любого типа учреждений. Атака проводится для достижения недоступности целевых сетевых ресурсов и представляет собой крупномасштабную скоординированную атаку, запущенную косвенно через множество взломанных компьютеров в Интернете.

Был предложен метод для обнаружения атак DoS с передачей информационных пакетов по протоколам TCP и ICMP - LandAttack, Mail-BombAttack, SmurfAttack, PingofDeathAttack. Для проверки адекватности метода был использован подход на основе вероятностной логики и построения байесовой сети доверия.

Согласно предложенному методу анализируется входной поток информационных пакетов. В случае выявления возможной атаки оценивается ее серьезность, поток пакетов направляется во временное хранилище и предлагаются соответствующие действия для системного администратора.

Предлагаемый метод реализуется как системный монитор обнаружения вторжений, в состав которого входят: база данных с параметрами известных атак; конфигурационные данные - параметры серверной системы; база правил для обнаружения атак; детектор атаки - он получает входной сетевой поток и производит вывод, если имеют место сигналы тревоги; блок измерения серьезности атаки - на основе разработанной модели оценок по уровням защищенности серверной системы рассчитывает степень серьезности атаки; блок принятия решения - на основании серьезности атаки генерирует список возможных действий по защите и отправляет сообщение системному администратору.

Разработанный метод выявления атак может быть расширен. В систему могут быть добавлены новые шаблоны с параметрами атак, правила для выявления атак и шаблоны реакции системы в случае опасности.

Моделирование разработанного метода было выполнено в приложении Hugin, предназначенного для построения байесовых сетей доверия. Результаты моделирования показали, что метод дает правильную оценку сетевого потока в 96% случаев.