АРХИТЕКТУРА СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

И.П. Ковятинец

Система обнаружения вторжений (Intrusion Detection System, IDS) – это программное или аппаратное средство, предназначенное для предупреждения, выявления и протоколирования некоторых типов сетевых атак. В отличие от файерволов, в обязанности IDS не входит блокировка подозрительного траффика. IDS пытается выявить подозрительную активность и поднять тревогу.

IDS сетевого уровня анализирует все поля пакетов, в том числе и поле данных, которое переносит информацию приложений. IDS хоста анализирует события, происходящие в операционной системе и приложениях.

Источниками данных для сетевой IDS являются маршрутизаторы, коммутаторы и хосты локальной сети.

Датчик копирует пакеты и передает их анализатору. Датчик может представлять собой отдельный компьютер или же это может быть программный компонент маршрутизатора.

Анализатор получает данные от датчиков и проверяет их на наличие угроз и подозрительной активности в сети. Анализатор работает на основе правил, составленных администратором системы безопасности предприятия в соответствии с политикой безопасности. При выполнении одного из правил анализатор передает сообщение «тревога» менеджеру IDS – программной компоненте, которая хранит конфигурацию IDS. Менеджер оповещает оператора о тревоге в виде уведомления.

Оператор IDS на основе данных уведомления принимает решение о реакции сети на подозрительную активность – это может быть отключение сетевого интерфейса, изменение правил файервола для блокировки пакетов или же игнорирование уведомления, если оператор считает, что вероятность вторжения очень мала.

Описанная выше архитектура является функциональной, в реальной IDS эти функции не обязательно реализуются в отдельных блоках или модулях системы. В минимальном варианте все функции IDS могут быть сосредоточены в программном обеспечении компьютера, сетевой адаптер которого выполняет роль датчика.

Литература

1. Олифер В.Г., Олифер Н А. Безопасность компьютерных сетей. – М.: Горячая линия – Телеком, 2016. – 644 с.

2. Таненбаум Э., Уэзеролл Д. Компьютерные сети. – СПб.: Питер, 2013. – 960 с.