XXXI Неделя науки СПбГПУ. Материалы межвузовской научной конференции. Ч. VI: С.93-94, 2003.

УДК 004.4

М.А. Галкин (6 курс, каф. АиВТ), А.Г. Новопашенный, к.т.н., доц.

СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

Актуальность проблем сетевой безопасности, появившихся с момента создания первых компьютерных сетей, непрерывно растет по мере развития локальных сетей и Internet. Постоянно совершенствуются методы и средства защиты информации, однако вместе с ними совершенствуется и арсенал средств, используемых для уклонения от этих средств защиты. Несовершенность систем защиты послужила предпосылкой возникновения системы обнаружения вторжений (СОВ), которые призваны дополнять существующие системы безопасности, такие как межсетевые экраны. На сегодняшний день рынок СОВ постоянно расширяется, увеличиваются финансовые затраты компаний на поддержание безопасности своих ресурсов. Произведенные расчеты экономической эффективности применения средств и систем безопасности подтверждается статистическими данными – суммы, выделяемые на работу служб безопасности ведущими американскими компаниями равны только десятой доле ущерба, наносимого различного рода хакерскими атаками.

Системы обнаружения вторжений, как правило, основываются на одной из двух составляющих – это sniffer или «вынюхиватель» пакетов, программа перехвата пакетов из сети и анализатора пакетов. Цель анализа – определение является ли данный пакет нормальным сетевым трафиком или относится к той или иной атаке. Современные СОВ работают с динамически настраиваемыми правилами идентификации пакетов, которые в терминах СОВ называются сигнатурами. Базы данных сигнатур атак постоянно обновляются по мере появления новых атак или уязвимостей тех или иных пакетов программ.

На данный момент существует множество готовых пакетов СОВ, некоторые из которых распространяются бесплатно (как, например Snort или LIDS), другие стоят достаточно больших денег. Однако, как показали исследования ни одна из существующих систем не отвечает всем требованиям, предъявляемым к СОВ. Типичные недостатки это – недостаточная гибкость в настройке правил, плохая устойчивость к перегрузкам сети, отсутствие должного пользовательского интерфейса, высокая доля ложных срабатываний, нерегулярность обновления сигнатур. Кроме того, большинство современных СОВ функционируют на сетевом и транспортном уровнях многоуровневой архитектуры, не предоставляя возможность проверки прикладного уровня. Это тем более важно из-за участившихся в последнее время атак, использующих ошибки в программировании конкретных сетевых приложении, таких как переполнения внутренних буферов, не документированная реакция на определенные входные данные и пр.

Очевидная актуальность СОВ, отсутствие на современном рынке систем, лишенных всех перечисленных выше недостатков и высокая стоимость большинства существующих систем послужили предпосылкой для создания собственной системы. Традиционно СОВ функционировали независимо от других систем безопасности, часто перекрывая их функции. В проектируемой системе предполагается внедрить модуль взаимодействия с некоторыми видами межсетевых экранов. Так же будет предусмотрена работа с сетевым трафиком на уровне приложений, по крайней мере, для некоторых наиболее распространенных сетевых протоколов. Возможность динамического задания и изменения рабочих сигнатур подразумевается в большинстве современных систем, и будет реализована в этом проекте, кроме того, предполагается совместимость записей сигнатур атак с сигнатурами Snort, которые, как и сама система, распространяются бесплатно и с достаточной регулярностью. Повышенное внимание будет уделено безопасности и устойчивости к атакам самой СОВ, т.к. сейчас уже известны программы, специализирующиеся на атаках на конкретные типы СОВ.