ВНЕШНИЙ АКТИВНЫЙ АУДИТ БЕЗОПАСНОСТИ КОРПОРАТИВНОЙ СЕТИ

В.В. АНИЩЕНКО, Ю.В. ЗЕМЦОВ

В настоящее время все более востребованной на рынке информационной безопасности становится услуга внешнего активного аудита безопасности корпоративной сети. Данный вид аудита представляет собой моделирование действий злоумышленника, намеренного проникнуть в корпоративную сеть извне. При этом аудитор искусственно ставится именно в те условия, в которых работает злоумышленник, – ему предоставляется только та информация, которую можно раздобыть в открытых источниках. Естественно, атаки только моделируются и не оказывают де-

структивного воздействия на корпоративную сеть. Результатом внешнего активного аудита является информация об уязвимостях, степени их критичности и методах устранения, сведения о широкодоступной информации (информация, доступная любому потенциальному нарушителю) сети.

Объектами внешнего активного аудит обычно являются корпоративные сети и Web-сайты. Однако не так давно появилась новая методика – имитация атаки на внутренних пользователей системы путем применения реверсивных "троянских коней". Эта прогрессивная технология взлома, в которой используются уязвимости клиентского ПО рабочих станций и методы социальной инженерии, позволяет проникать в защищенные корпоративные сети и контролировать их изнутри. По сути, она дискредитировала концепцию защиты от атак путем обеспечения безопасности только внешнего периметра сети, вынудив защищать каждое рабочее место с помощью комплекса мер верхнего уровня в соответствии со стандартом ISO 17799.

В данной работе описывается процесс проведения внешнего активного аудита безопасности корпоративной сети, анализируется ее структура, функции и особенности, выявляются наиболее значимые угрозы информационной безопасности и основные пути их реализации, а также проводится проверка возможности получения несанкционированного доступа к данным, несанкционированной модификации данных и нарушения работоспособности тестовой корпоративной сети.