ОСНОВНЫЕ ТИПЫ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ В ЗАВИСИМОСТИ ОТ КОЛИЧЕСТВА ПРЕДОСТАВЛЯЕМОЙ ИНФОРМАЦИИ О СИСТЕМЕ

Кармаз Е. В.
Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь
Яшин К. Д. – кандидат технических наук, доцент

Цель - разработка методик тестирования на проникновение для оценки уровня защищенности информационной системы.

Для безопасности собственной информационной системы ряд организаций регулярно проводят тестирование на проникновение – выявление возможных уязвимостей, используемых для создания сценария проникновения в информационно-вычислительную сеть предприятия. Тестирование на проникновение позволяет получить объективную оценку возможности осуществить несанкционированный доступ к ресурсам корпоративной сети или сайтах [1].

Существует три основных типа тестирования на проникновение в зависимости от количества предоставляемой информации о системе (см. рисунок 1). Этот фактор имеет существенное значение, поскольку тестирование выполняется в условиях ограниченного времени, которое в случае недостатка информации придется потратить на её сбор и анализ:

– внутреннее тестирование («White Box», модель «белого ящика») – тестирование проводится с расчетом на то, что злоумышленник действует внутри организации и знает схему ИС;

– внешнее тестирование («Black Box», модель «черного ящика») – тестирование выполняется из общедоступных сетей и моделирует поведение злоумышленника, нападающего из Интернета либо из-за границы контролируемой зоны заказчика;

– модель «серого ящика» является компромиссом между двумя упомянутыми ранее. В этом варианте заказчик передает экспертам заранее согласованный ограниченный набор сведений [2].

Рисунок 1 – Три основных типа тестирования на проникновение

Реальный злоумышленник, в отличие от специалистов по тестированию на проникновение, в большинстве случаев не стеснен сроками выполнения работ по договору и имеет значительный запас времени на предварительный сбор информации [3]. Поэтому правильный выбор модели нарушителя и метода тестирования важен для объективности результатов работы.

Разработанные методики тестирования на проникновение эффективны и могут служить рекомендательной основой для оценки уровня защищенности информационной системы.

Список использованных источников:

1. Актуальность угроз информационной безопасности для информационных систем [Электронный ресурс]. – Режим доступа: https://novainfo.ru/article/8345/.

2. Тестирование на проникновение [Электронный ресурс]. – Режим доступа: http://www.amt.ru/pentest/.

3. Туманов, С. Средства тестирования информационной системы на проникновение/ С.А. Туманов // Электроника. – 1989. – №12. – С. 21–25