УДК 004.056

РАЗРАБОТКА СИСТЕМЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ПРИ АНАЛИЗЕ УЯЗВИМОСТЕЙ РАСПРЕДЕЛЕННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Кротиков Г.М. (Национальный исследовательский университет ИТМО)
Научный руководитель – к.т.н, доцент Кузнецов А.Ю.
(Национальный исследовательский университет ИТМО)

В работе обозначены основные проблемы проведения анализа уязвимостей в процессе сертификационных испытаний средств защиты информации на соответствие требованиям по защите информации. Определены способы снижения числа уязвимостей, подлежащих проверке на экспуатируемость, при проведении работ по анализу уязвимостей. Разработана система поддержки принятия решений на основе графового анализа паттернов атак с использованием обнаруженных уязвимостей.

Введение. На сегодняшний день процесс сертификации средств защиты информации осложняется двумя основными проблемами. Во-первых, процесс сертификации очень длительный, в зависимости от системы сертификации может занимать пять, шесть месяцев. Основную часть этого времени занимают непосредственно сертификационные испытания. Во-вторых, согласно новым требованиям по сертификации средств защиты информации, испытательная лаборатория должна проводить анализ уязвимостей. Проблемой является то, что в данный момент не существует документов, подробно описывающих действия при проведении анализа уязвимостей. Специалистам испытательных лабораторий приходится в каждом конкретном случае обращаться за информацией к разным источникам, изучать все новые и новые методы и принципы проведения тестирования на проникновение. Поэтому вопрос ускорения этапа анализа уязвимостей при проведении сертификационных испытаний и, как следствие, снижения затрат, является актуальным.

Основная часть. Разрабатываемая система направлена на снижение времени затрачиваемого на проведение анализа уязвимостей путем снижения числа уязвимостей, подлежащих проверке на экспуатируемость. После проведения независимого сканирования и поиска потенциальных уязвимостей специалист лаборатории получает набор уязвимостей, которые подлежат дальнейшей проверке. Снижение числа уязвимостей, подлежащих проверке на экспуатируемость, может быть достигнуто за счет использования заданного в руководящих документах потенциала нападения злоумышленника.

В руководящих документах определен уровень потенциала нападения злоумышленника (нарушителя). Определив сложность атаки, направленной на эксплуатацию потенциальной уязвимости, можно сопоставить ее с потенциалом нападения злоумышленника. В случае если эта сложность окажется выше той, которая определена потенциалом нападения нарушителя, то можно не проводить проверку эксплаутируемости этой потенциальной уязвимости. Анализ сложности выполнения атаки с использованием конкретной потенциальной уязвимости, полученной в результате сканирования, может быть проведен с использованием графовых структур. Механизм атаки, может быть разложен на последовательность промежуточных состояний – вершин графа. Ребрами графа будут являться механизмы перехода от одного шага атаки к другому. Стоит отметить, что промежуточные шаги могут совпадать для различных атак, таким образом вершина будет принадлежать сразу нескольким путям в графе. Вес ребер в данном графе может быть определен на основании экспертной оценки специалистов лаборатории. Вес ребра должен зависеть от сложности совершения перехода от одного этапа атаки к следующему. Решив задачу нахождения минимального пути в графе, можно определить минимальную сложность достижения эксплуатируемости каждой из обнаруженных (на предыдущих этапах анализа) потенциальных уязвимостей. Причем, задача может решаться, как с известной начальной вершиной (когда известно начальное состояние системы, которое может привести к атаке), так и без таковой. Во втором случае необходимо

найти кратчайший путь из любой начальной вершины (любого начального состояния). Таким образом полученный вес кратчайшего пути является выражением простейшего пути выполнения атаки с использованием потенциальной уязвимости. Если сложность кратчайшего (простейшего) пути выполнения атаки в численном выражении больше численного выражения потенциала нападения злоумышленника, то проведение проверки на эксплуатируемость такой уязвимости не является целесообразной.

Выводы. Предложена система поддержки принятия решений основанная на графовом методе. Имея взвешенный граф, а также набор потенциальных уязвимостей, которые являются конечными точками путей в этом графе, можно определить кратчайшие пути в полученном графе. Вес кратчайшего пути при сопоставлении может быть выше числового представления потенциала нападения, что говорит о том, что для выполнения самого простого способа эксплуатации обнаруженной уязвимости, необходим потенциал нападения выше потенциала нападения предполагаемого злоумышленника. Таким образом данная уязвимость может быть обоснованно проигнорирована. Снижение числа потенциальных уязвимостей, подлежащих проверке на экспуатируемость, снизит общие временные затраты при проведении анализа уязвимостей.

Кротиков Г.М.

Кузнецов А.Ю.