УДК 004.415.53:519.711

Чжан ЛИЦЗЯН,
преподаватель Юго-западного университета науки и техники (г. Цзяотун, Китай)

Юрий Петрович ГОРЕЛОВ,
кандидат технических наук, доцент, доцент кафедры информационных технологий и кибербезопасности факультета № 4 Харьковского национального университета внутренних дел

Юрий Валерьевич ГНУСОВ,
кандидат технических наук, доцент, заведующий кафедры информационных технологий и кибербезопасности факультета № 4 Харьковского национального университета внутренних дел

РАЗРАБОТКА АЛГОРИТМА ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ В КОМПЬЮТЕРНУЮ СИСТЕМУ

Проведенные исследования показали, что основной целью тестирования на проникновение является определение возможностей существующего уровня защищённости инфраструктуры в сдерживании попыток вторжения потенциального кибер злоумышленника. При этом вопрос полноты обнаруженных уязвимостей не стоит, но отражаются все уязвимости, имеющие отношение к направлениям атаки.

Основным фокусом данного вида тестирования безопасности является глубина исследования. Данная характеристика является более важной, чем ширина охвата тестовых примеров. Это является одной из особенностей, которую целесообразно учитывать в процессе математического моделирования.

Как указано в руководящих документах и планах тестирования уровень зрелости информационной безопасности, которую обеспечивает данный вид тестирования можно характеризовать в пределах от среднего до высокого.

Результатами процесса тестирования на проникновение являются факты и/или вероятность взлома (проникновения) и получения информации злоумышленником.

Проведенные исследования позволили выделить ряд примеров решаемых задач тестирования:

- получить несанкционированный доступ к информации о клиентах, их средствах и другим данным;
- проникнуть из офисного сегмента в «боевой», где расположены рабочие серверы;
- нарушить доступность определённого сервиса;
- получить доступ к файловой системе с необоснованно завышенными правами;
- скомпрометировать исходные коды программного обеспечения из системы контроля версий.

Для достижения поставленных целей и решения приведенных выше задач возможно использование всех доступных методов и средств, удовлетворяющих ограничениям, поставленным заказчиком (в т. ч. социальная инженерия, атаки перебором и др.). При этом исследователи ищут кратчайший и самый дешёвый путь достижения целей.

Проект заканчивается либо, когда поставленная цель будет достигнута, либо по истечению времени на проект (если рассматриваются многие вектора).

Прежде чем более подробно описывать основные этапы тестирования на проникновение и реализовывать соответствующую математическую модель необходимо отметить отличительные особенности и специфику тестирования различных компьютерных и инфокоммуникационных систем, а также их составляющих. Для этого выберем наиболее часто используемые объекты тестирования, которые можно рассматривать в совокупности по принципу единства платформ выполнения задач и функций. Это компьютерные системы управления с элементами SCADA и IOT, сайты и web-приложения, мобильные средства и приложения.

Анализ основных этапов и процедур тестирования на проникновение перечисленных объектов позволил разработать и представить обобщенный алгоритм тестирования.

Структурная схема алгоритма представлена на рис. 1.

Следует заметить, что в представленный обобщенный алгоритм не включены ряд возможных для реализации процедур тестирования. Например, при тестировании «SCADA-компьютерных систем» можно воспользоваться услугами зондирования или процедурами эксплойт исследования. Для более глубокой оценки мобильных приложений можно использовать дополнительно оценку уязвимостей OWASP Mobile Top 10. Перечень и спектр таких услуг и процедур увеличивается с каждым годом. Связано это с появлением новых рисков кибератак.

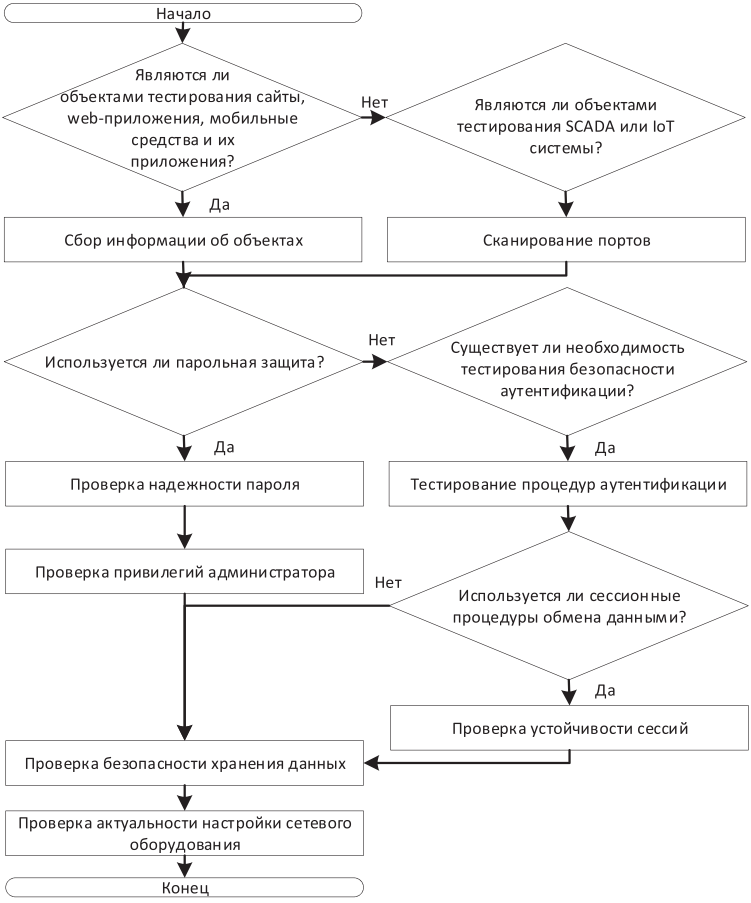

Рис. 1. Структурная схема обобщенного алгоритма тестирования на проникновение

Однако, по нашим оценкам, решение о включении дополнительных процедур как составляющих отдельных этапов обобщенного алгоритма (рис. 1.) значительно не снизит точности результатов моделирования. Необходимо только учитывать эти дополнительные факторы при задании вероятностного распределения каждого из этапов и выборе коэффициентов распределения.

Одержано 30.04.2020