УДК 004.056:004.89

АУДИТ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ С ИСПОЛЬЗОВАНИЕМ ТЕСТОВ НА ПРОНИКНОВЕНИЕ

Чуб В.С.
Донской государственный технический университет, Ростов-на-Дону, Российская Федерация
vadim-chub13@mail.ru

Рассматриваются особенности и различные сценарии тестирования на проникновение. Предлагается выполнение теста на проникновение в информационную систему с использованием всех имеющихся методов.

Ключевые слова: тестирование на проникновение, аудит безопасности.

UDC 004.056:004.89

INFORMATION SYSTEM SAFETY AUDIT USING PENETRATION TESTING

Chub V. S.
Don State Technical University, Rostov-on-Don, Russian Federation
vadim-chub13@mail.ru

The article considers features and various scenario of penetration testing. It is proposed to perform information system penetration test using all available methods.

Keywords: penetration testing, security audit

Введение. В настоящее время ни одна организация в своей деятельности не может обойтись без информационных технологий [1]. Однако при их использовании необходимо увеличить защищенность информационных систем (ИС), в которых хранятся персональная и конфиденциальная информации [2, 3]. С этой целью разрабатываются способы защиты информации от утечек [4, 5] и способы оценки защищенности [6, 7].

Преимущества тестирования на проникновение. Тестирование на проникновение — частный случай аудита информационной безопасности (ИБ) (тест на преодоление защиты, penetration testing, pentest, пентест). Тестирование на проникновение позволяет в достаточно короткие сроки объективно оценить реальный уровень защищенности информационных активов организации в условиях современного состояния способов несанкционированного доступа к информации.

Главной целью тестирования на проникновение является выявление уязвимостей, которые могут быть успешно использованы злоумышленником [8].

Оценка защищенности обеспечивается путем моделирования атак потенциальных злоумышленников — поиском уязвимостей системы защиты и их последующей эксплуатацией.

По сравнению с традиционным аудитом ИБ, основной отличительной особенностью теста на проникновение являются: меньшая глубина охвата информационной инфраструктуры организации; большая детализация найденных уязвимостей; более точная оценка рисков ИБ, основанная на результатах реализации найденных уязвимостей; большая достоверность результатов аудита по сравнению с классическими методами аудита, такими как заполнение анкет, опрос сотрудников и т. д.

Тестирование на проникновение позволяет осуществить оценку бóльшего количества процессов ИБ, чем инструментальный аудит.

Методики проведения тестирования на проникновение. Международных методик проведения тестирования на проникновение, направленных на сетевую инфраструктуру организации, существует несколько. К таким методикам относятся Open Source Security Testing Methodology Manual (OSSTMM) и The Information Systems Security Assessment Framework (ISSAF).

Компании, которые занимаются предоставлением услуги по тестированию на проникновение, при проведении работ могут использовать собственную методику, включающую в

себя возможность моделирования не только технических атак на информационные ресурсы, но и атак, направленных на пользователей корпоративных систем (социальная инженерия), беспроводные сети IEEE 802.11 (Wi-Fi), 802.15 (Bluetooth) и 802.16 (Wi-Max), переносные компьютеры и мобильные устройства, а также атак с использованием физического или логического доступа к компонентам корпоративной ИС.

Тестирование не завершается на стадии проникновения в информационно-вычислительную сеть заказчика. После проникновения рассматриваются другие варианты атак, с помощью которых можно проникнуть в ИС.

Понятие тестирования на проникновение использует «футпринтинг» (англ. footprinting), который позволяет получить информацию об ИС и лицах, которым эти системы принадлежат. Применение тестирования на проникновение с использованием футпринтинга необходимо для поиска публично доступной информации об организации в Интернете. Аудитор, с помощью публичных ресурсов, вполне вероятно, сможет найти приватную информацию.

При футпринтинге используются сетевой способ и социальная инженерия. Сетевой способ футпринтинга связан с получением информации о сети (диапазоны сетей, составление карты сетей, определение ОС и т. д.). Сбор информации происходит на этапе, когда аудитор находится в локальной сети проверяемой организации. Социальная инженерия основана на особенностях психологии человека. Социальный инженер, в первую очередь, должен адекватно воспринимать психологию человека. Методика основана на использовании психологических слабостей людей, «выманивая» у жертвы конфиденциальную информацию. Дополнительные методы социальной инженерии: социальные сети, информация из мусорных баков, подслушивание, подглядывание.

Футпринтинг можно провести с помощью различных средств [3].

Поисковые системы дают большое количество информации об организации: физическое расположение объекта, контактные данные и др. Сайт Google, благодаря наличию расширенных средств, дополнительно позволяет получить информацию о важных директориях; файлах, хранящих пароли; страницах, содержащих информацию о сети или уязвимостях и т. д.;

Сайт организации позволяет получить используемое программное обеспечение, версию используемой операционной системы, поддиректории и параметры сайта, имена файлов, названия полей базы данных т. д. С помощью данной информации можно обнаружить уязвимости в конфигурации сайта;

Электронная почта — возможность получить из почтовых сообщений информацию о сетевой структуре заказчика (IP-адрес хоста, название провайдера, географическое положение сервера и почтового сервера и т. д.);

DNS дает возможность получить информацию о доменах. Чаще всего используется для получения IP-адреса по имени хоста в сетевых инфраструктурах, а также IP-диапазоны домена, почтовых серверов, DNS-серверов и т. д. Таким образом сужается зона интересующих адресов.

Аудитор может на свое усмотрение выбирать используемые средства. Однако полное использование вышеперечисленных средств позволит обеспечить максимальную область действия футпринтинга.

Перечень моделируемых атак может быть сформирован на этапе подготовки технического задания и дополнительно скорректирован в ходе проведения тестирования на проникновение.

Важным этапом проведения теста на проникновение является разработка отчета о тестировании, который может содержать:

– описание границ, в рамках которых был проведен тест на проникновение;

– методы и средства, использованные в процессе проведения теста на проникновение;

– описание и возможность использования выявленных недостатков и уязвимостей злоумышленником, включая уровень риска;

– описание достигнутых результатов;

– описание примененных сценариев проникновения;

– базовую оценку рисков ИБ организации;

– базовую оценку процессов обеспечения ИБ организации;

– рекомендации по совершенствованию процессов обеспечения ИБ организации и по устранению выявленных уязвимостей;

– совершенствование процессов обеспечения ИБ организации и план работ по устранению найденных уязвимостей.

Заключение. Рассмотрены основные этапы и особенности аудита ИБ с использованием теста на проникновение.

Библиографический список

1. Айдинян, А. Р. Информационные технологии: учебное пособие / А. Р. Айдинян, О. Л. Цветкова. — Ростов-на-Дону : Издательский центр ДГТУ, 2011. — 132 с.

2. Куринных, Д. Ю. Подход к кластеризации угроз информационной безопасности предприятий / Д. Ю. Куриных, А. Р. Айдинян, О. Л. Цветкова // Инженерный вестник Дона. — 2018.— № 1. — Режим доступа : ivdon.ru/ru/magazine/archive/n1y2018/4803(дата обращения : 11.04.2018).

3. Чуб, В. С. Способ повышения защиты текстовой информации с помощью DLP-систем / В. С. Чуб, А. Р. Айдинян // Наукоемкие технологии и интеллектуальные системы в XXI веке: сб. ст. междунар. науч.-практ. конф. в 2 частях. — Ч.1. — г. Пермь, 2017 г. — С. 94–96.

4. Айдинян, А. Р. Подход к оценке DLP-систем с использованием средств нечеткой логики / А. Р. Айдинян, О. Л. Цветкова // Инженерный вестник Дона. — 2017. — № 4. — Режим доступа : http://ivdon.ru/ru/magazine/archive/n4y2017

/4432 (дата обращения : 01.11.2017).

5. Айдинян, А. Р. Методики интеллектуального выбора и оценки DLP-систем для решения задач информационной безопасности / А. Р. Айдинян, О. Л. Цветкова, Д. С. Сокол // Молодой исследователь Дона. — 2018. — №1. — С. 2–5.

6. Айдинян, А. Р. О подходе к оценке информационной безопасности предприятия / А. Р. Айдинян [и др.] // Системный анализ, управление и обработка информации: сб. тр. V междунар. науч. семинара. — п. Дивноморское, 2014. — С. 109–111.

7. Цветкова, О. Л. Интеллектуальная система оценки информационной безопасности предприятия от внутренних угроз / О. Л. Цветкова, А. Р. Айдинян // Вестник компьютерных и информационных технологий. — 2014. — №8(122). — С. 48–53.

8. Мещеряков, Р. В. Концептуальные вопросы информационной безопасности региона и подготовки кадров / Р. В. Мещеряков, А. А. Шелупанов // Труды СПИИРАН. — 2014. — № 3(34). — С. 136–159.