О целях и задачах при тестировании на проникновение

ardent101.github.io/posts/manifest

February 21, 2024

февраля 21, 2024 · 2 мин · Ardent101

Изложу свое текущее виденье мероприятий по тестированию на проникновение.

Цель мероприятий по тестированию на проникновение - повысить уровень защищенности Объекта от компьютерных атак.

Для достижения цели необходимо выполнить следующие **задачи:**

Задача №1. Определить перечень негативных для Объекта последствий компьютерных атак.

> Примечание: у термина “негативные последствия” (ФСТЭК) существуют следующие альтернативны:
>
> - недопустимые события (Минцифры / Positive Technologies)
> - ключевые риски (Банк России)

Хороший перечень негативных последствий (содержит порядка 40 пунктов) представлен на сайте ФСТЭК. Некоторые примеры:

- потеря денежных средств
- остановка производственных процессов
- невозможность или снижение эффективности решения задач (реализации функций)
- нарушение деловой репутации
- вредные воздействия на окружающую среду
- нарушение законодательства РФ
- утечка информации ограниченного доступа

Задача №2. Определить модели злоумышленников.

Для начала требуется уточнить у Объекта модель нарушителя. По результатам следует сделать вывод насколько адекватной является предлагаемая модель. Если модель отсутствует, является вымышленной или недоработанной, то можно предложить свои модели злоумышленника. В качестве примера можно использовать варианты ниже.

Внутренний злоумышленник, обладает:

- возможностью физического доступа к сетевой розетке, настроенной для подключения к инфраструктуре Объекта;
- доступом к типовому рабочему месту непривилегированного сотрудника Объекта.

Внешний злоумышленник, действует:

- со стороны сети Интернет;
- со стороны подрядных или зависимых организаций (доверенный домен или сопряженная сеть);
- из-за пределов контролируемой зоны (Wi-Fi, MouseJack).

Задача №3. Согласовать критерии подтверждения возможности реализации компьютерных атак, приводящих к негативным для Объекта последствиям.

Сначала требуется определить перечень ключевых информационных систем, компьютерные атаки в отношении которых приводят к негативным для Объекта последствиям.

Примеры ключевых информационных систем:

- контроллеры домена
- система управления антивирусной защитой
- система резервного копирования
- система управления технологическими процессами
- система электронного документооборота
- система управления финансами

Примеры критериев:

- получение административного доступа к серверу, обеспечивающему функционирование ключевой системы;
- получение доступа к действующей учетной записи предназначенной для администрирования ключевой системы.

Задача №4. В рамках определенных моделей злоумышленников за отведенное время построить наибольшее количество сценариев выполнения согласованных критериев подтверждения возможности реализации компьютерных атак, приводящих к негативным для Объекта последствиям.

Чтобы сценарий считался построенным его необходимо подтвердить на практике или обосновать теоретически. Прежде чем подтверждать сценарий на практике следует утвердить перечень действий, допустимых для выполнения с целью построения сценариев.

Задача №5. Выделить и приоритизировать недостатки, создающие предпосылки к реализации компьютерных атак, приводящих к негативным для Объекта последствиям.

Задача №6. Предоставить рекомендации по устранению или минимизации выделенных недостатков.