infotecs

Тестовое задание для стажера на позицию «Аналитик ИБ»

Минимальное требование – выполнение любого одного из двух заданий. Максимальное – выполнение обеих заданий.

Задание №1

Прочитать:

- Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах (https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17).
- Требования по безопасности информации к многофункциональным межсетевым экранам уровня сети (https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/trebovaniya-po-bezopasnosti-informatsii-utverzhdeny-prikazom-fstek-rossii-ot-7-marta-2023-g-n-44).
- Меры защиты информации в государственных информационных системах (https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-11-fevralya-2014-g).

На основании прочитанного написать требования к механизмам идентификации и аутентификации Межсетевого экрана для применения в государственной информационной системе 2 класса защищенности.

Требование к присылаемым решениям

Требования должны быть кратко сформулированы, иметь явную структуру и трассировку на выполнение нормативных документов.

Цель документа – иметь обоснованный перечень необходимого функционала для разработки в продукте.

Задание №2

Моделирование угроз – процесс аналитического поиска угроз безопасности информационной системы или её части путём рассмотрения модели этой системы (или её части).

Вы аналитик по информационной безопасности, вам требуется промоделировать угрозы для разрабатываемого продукта на основании следующих требований к продукту:

Требуется разработать увлажнитель воздуха с датчиком влажности в оранжерее с экзотическими растениями и возможностью управления через браузер. Должна быть возможность включения / выключения, определения минимальной и максимальной влажности (чтобы растения не погибли), просмотра текущего количества воды в бачке.

Требования безопасности:

- должны быть доступны три учётные записи (которые создаются только в момент развёртывания):

  - администратор, отвечающий за настройку параметров подключения,
  - специалист по уходу за растениями, отвечающий за настройку параметров увлажнения,
  - техник, отвечающий за пополнение запасов воды в бачке;
- однофакторной аутентификации достаточно;
- администратор – не нарушитель.

- нарисуйте диаграмму продукта в соответствии с представленными требованиями;
- осуществите поиск угроз, зафиксируйте их; при фиксации угроз желательно описать сценарий тестирования;
- отранжируйте найденные угрозы (определите порядок, в котором они должны быть исправлены).*****

  *Опционально

Требование к присылаемым решениям

Рекомендуем для моделирования угроз использовать диаграмму потоков данных (Data Flow Diagram, DFD), на которой изображаются внешние по отношению к системе участники (например, администратор), части моделируемой системы (например, веб-сервер), хранилища (например, лог доступа), потоки данных (передаваемая информация) и границы доверия, показывающие изменение требуемых для доступа прав.

Для поиска угроз предпочтительнее использовать методику STRIDE, предполагающую последовательное применение типов угроз:

- Spoofing – подмена; например, кто-то выдаёт себя за администратора;
- Tampering – искажение; например, передача неправильного значения заполненности бачка;
- Repudiation – отказ от действия; например, кто-то меняет параметры влажности и отрицает это;
- Information disclosure – раскрытие информации; например, пароль администратора становится известен нарушителю;
- Denial of service – отказ в обслуживании; например, ситуация, когда техник не сможет получить доступ к информации о заполненности бачка с водой;
- Elevation of privilege – превышение полномочий; например, техник сможет изменить параметры влажности

к каждому элементу диаграммы (кроме границ доверия) или к каждому потоку данных.

Для ранжирования можно применить, например, Mitre CVSSv3, Microsoft DREAD или оценку потенциала нападения из ГОСТ 18045-2013 (Common Criteria).

Максимальное время на выполнение задания: 1 неделя.