Ростелеком
Солар

Программный комплекс кибертренировок «Солар Кибермир»

Описание функциональных характеристик программного обеспечения

МОСКВА, 2023

Содержание

1. Назначение и решаемые задачи

1.1. Описание назначения

Программный комплекс кибертренировок «Солар Кибермир» предназначен для повышения уровня практической подготовки специалистов в области информационной безопасности в выявлении компьютерных атак, расследовании инцидентов информационной безопасности за счет автоматизации следующих процессов:

- проведение практических занятий по информационной безопасности (далее -ИБ): обнаружение, расследование и защита от кибератак (далее - КА);
- проведение учений и соревнования по информационной безопасности и защите от КА для специалистов по ИБ;
- оценки практических навыков специалистов в области ИБ;
- проведения исследований в области информационной безопасности программного обеспечения и автоматизированных систем.

1.2. Описание функциональных возможностей и решаемых задач

Основные функции комплекса кибертренировок «Солар Кибермир»:

- развертывание и управление виртуальными инфраструктурами мероприятий;
- создание шаблона мероприятия, состоящего из сценария кибератак и эталонного отчета;
- создание модели визуализации хода мероприятия на графической карте инфраструктуры;
- обеспечение доступа пользователей к удаленным рабочим столам виртуальной инфраструктуры мероприятия;
- автоматизированная оценка практических навыков участников мероприятия.

Комплекс кибертренировок «Солар Кибермир» решает следующие задачи:

- управление пользователями и организациями;
- ролевой контроль доступа пользователей;
- проведение учебных мероприятий – практических занятий по обнаружению и расследованию компьютерных атак;
- управление учебными мероприятиями;

- отображение результатов мероприятия;
- графическая визуализация хода учебного мероприятия;
- обеспечение доступа пользователей к удаленным рабочим столам виртуальной инфраструктуры мероприятия;
- автоматизированная оценка результатов учебных мероприятий и навыков участников мероприятия;
- разработка модели визуализации хода учебного мероприятия на графической карте инфраструктуры;

1.2.1. Управление пользователями и организациями

Задача решается с помощью следующих функций:

- аутентификация и авторизация пользователей;
- просмотр списка, поиск и фильтрация учетных записей пользователей;
- создание профиля пользователя;
- редактирование профиля пользователя;
- блокировка профиля пользователя;
- массовая загрузка (регистрация) пользователей из файла внешнего формата;
- смена/восстановление пароля пользователя;
- создание профиля организации;
- удаление профиля организации;
- редактирование профиля организации;
- просмотр списка, поиск и фильтрация организаций;
- блокирование/разблокирование организации и всех пользователей, входящих в состав данной организации;
- отправка на электронную почту уведомлений о регистрации пользователя;
- отправка уведомлений о смене пароля.

1.2.2. Ролевой контроль доступа пользователей

В комплексе кибертренировок «Солар Кибермир» реализованы следующие роли:

- «Администратор» имеет полный доступ ко всем функциям Комплекса, в том числе функциям управления пользователями и организациями.

- «Преподаватель» имеет доступ к функциям, необходимым для проведения учебных мероприятий: создание мероприятия, оценка отчетов участников, просмотр и скачивание результатов мероприятия.
- «Участник» имеет доступ к функциям, необходимым для выполнения учебных задач мероприятия: формирование отчета участника, управление удаленным рабочим столом своего виртуального АРМ, просмотр табло результатов, скачивание документации к мероприятию.
- «Наблюдатель» имеет доступ только к просмотру текущих результатов мероприятия, визуализации хода мероприятия и истории событий.

1.2.3. Проведение и управление учебными мероприятиями

Задача решается с помощью следующих функций:

- создание мероприятия с возможностью:
  - ввода даты/времени фактического начала мероприятия;
  - автоматического формирования шаблона отчета участника о мероприятии – «включено»/«выключено»;
  - автоматического завершения мероприятия – «включено», «выключено»;
  - добавление списка пользователей участвующих в мероприятии (с указанием их роли: Участник, Наблюдатель, Преподаватель).
- просмотр перечня, поиск и фильтрация мероприятий;
- отмена/завершение мероприятия;
- автоматическое распределение виртуальных АРМ инфраструктуры между участниками;
- назначение участнику виртуального АРМ;
- просмотр журнала хода подготовки мероприятия;
- подключение участника к мероприятию;
- скачивание документации – справочных, методических и прочих материалов в виде электронных документов, приложенных к мероприятию.
- выбор шаблона мероприятия (миссии);
- включение/выключение КА;
- просмотр визуализации хода мероприятия;
- включение/выключение шумовых атак и имитации работы пользователей;
- выбор режима оценки навыков: выключен, автоматический, автоматизированный;

- автоматическое выполнение КА сценария мероприятия (миссии);
- просмотр историй событий о ходе мероприятия – содержит события о ходе выполнения сценария мероприятия: когда и какие атаки завершились, с какими результатам, какие КА выполняются в момент времени;
- ручной запуск КА из миссии текущего мероприятия;
- отображение сведений о мероприятии (цели, задачи);
- выбор режима: пауза/продолжение мероприятия (в ходе которой сценарий КА приостанавливается);
- отображение подсказок участникам об этапах КА и мероприятия.

1.2.4. Отображение результатов мероприятия

Задача решается с помощью следующих функций:

- управление отображаемым на табло результатов перечнем участников, в том числе с возможностью задавать имя и изображение участника;
- отображение текущих или финальных результатов каждого участника, выраженных в баллах;
- корректировка результатов (штрафы, премии);
- генерирование временной гиперссылки на отображения табло результатов.

В комплексе реализована функция отображения табло с текущими результатами участников мероприятия (выраженные в баллах от 0 до 100), рассчитанными в автоматическом или автоматизированном режиме скоринга.

1.2.5. Графическая визуализация хода учебного мероприятия

Задача решается с помощью следующих функций:

- отображение инфраструктуры и событий, возникающих в ходе мероприятия в графическом виде на карте инфраструктуры мероприятия в соответствии с моделью визуализации мероприятия;
- отображение событий, возникающих в ходе мероприятия (успешные атаки, отказы и аварии на узлах инфраструктуры и т. п.).

1.2.6. Обеспечение доступа пользователей к удаленным рабочим столам виртуальной инфраструктуры мероприятия

Задача решается с помощью следующих функций:

- удаленный просмотр и управление рабочим столом виртуального АРМ участника с помощью манипулятора типа «мышь» и клавиатуры;
- поддержка работы буфера обмена между виртуальным АРМ участника и его рабочим компьютером;
- ручная перезагрузка виртуального АРМ участника.

1.2.7. Автоматизированная оценка результатов учебных мероприятий и навыков участников мероприятия

Задача решается с помощью следующих функций:

- просмотр таксономии КА с описаниями и атрибутами в виде графической карты (далее – карта техник);
- заполнение отчета об обнаруженных КА и уязвимостях:
  - добавление обнаруженной в ходе мероприятия КА в отчет с помощью карты техник;
  - внесение индикаторов, обнаруженных КА фактическими данными;
  - описание методов защиты от данной КА и методов восстановления после КА с помощью графического интерфейса.
- просмотр перечня отчетов участников;
- просмотр отчета участника о мероприятии;
- выбор отчета участника для оценки;
- автоматизированная оценка отчета участника:
  - первичная автоматическая оценка правильности индикаторов КА;
  - возможность ручной проверки правильности обнаружения индикаторов компрометации КА (индикаторы компрометации) и корректировки результата;
  - ручная корректировка оценки навыков участника по каждому обнаруженному им индикатору КА;
  - ручная оценка описаний процессов защиты и восстановления после КА, заданных участником в отчете;
  - автоматический расчет оценочных баллов и оценки навыков участника за отчет;
  - публикация оценки отчета участника с отображением текущих результатов на табло;
- автоматическая оценка отчетов участника (без участия человека), при этом система не оценивает описание процесса восстановления и защиты от КА.

1.2.8. Разработка модели визуализации хода учебного мероприятия на графической карте инфраструктуры

Задача решается с помощью следующих функций:

- сохранение модели визуализации мероприятия во внешний формат (для загрузки его в конструктор миссии);
- загрузка модели визуализации из внешнего формата в редактор визуализации для просмотра и редактирования;
- создание/редактирование/удаление на карте визуализации (далее – сцена) различных графических объектов (далее – объекты сцены): серверов, АРМ, маршрутизаторов и т. п.;
- создание/редактирование/удаление на сцене соединительных линий между объектами (сетевые связи);
- ввод текстовых надписей;
- перемещение объекта на сцене;
- поддержка WYSWYG-принципа («что видишь, то и получаешь») организации графического интерфейса редактора визуализации;
- настройка шрифтов, цвета и анимации объектов сцены (надписей, линий);
- ввод для объектов характеристики их состояния по умолчанию (нормальное функционирование, атакован и т. д.), которая будет отображаться в ходе визуализации мероприятия;
- указание состояния объектов графических эффектов (атакован, недоступен, авария);
- указание состояния объектов изображения, в т. ч. анимированных из библиотеки визуализации;
- управление библиотекой накладываемых на объекты изображений, в т. ч. анимированных изображений;
- поддержка групповых операций над объектами сцены (удаление, перемещение);
- создание и управление триггерами объектов визуализации – описание изменений отображения объекта (наложение графических эффектов) на момент текущего состояния мероприятия и результатов выполнения КА; триггер задается на языке JavaScript;
- отладка визуализации сцены – просмотр отображения сцены при заданной пользователем характеристике состояния мероприятия.

1.3. Условия эксплуатации

1.3.1. Требования к серверу приложения

Минимальные требования к аппаратному обеспечению сервера приложений:

- процессор не менее 12 ядер с тактовой частотой не менее 3 ГГц и поддержкой архитектуры x64;
- объем оперативной памяти не менее 32 ГБ;
- объем жесткого диска не менее 250 ГБ;
- сетевой адаптер Ethernet с пропускной способностью не ниже 100 Мбит/с.

Требования к программному обеспечению сервера:

- операционная система Linux x64 без графического интерфейса с установленными средствами защиты информации.

1.3.2. Требования к автоматизированному рабочему месту пользователя

Требования к аппаратному обеспечению:

- процессор не менее 4 ядер с тактовой частотой не менее 2,8 ГГц;
- объем оперативной памяти не менее 4 ГБ;
- объем жесткого диска не менее 128 ГБ;
- разрешение экрана при работе с интерфейсом не менее 1024x768 (интерфейс оптимизирован для разрешения 1920x1080);
- сетевой адаптер Ethernet с пропускной способностью не ниже 10 Мбит/с.

Требования к программному обеспечению:

- операционная система Linux x64 с установленным графическим интерфейсом;

Перечень принятых сокращений

АРМ	Автоматизированное рабочее место
ИБ	Информационная безопасность
КА	Кибератака

Перечень принятых определений

Мероприятие	Практическое занятие (в любой форме: лабораторная работа, контрольная работа, исследовательская работа, соревнование) по информационной безопасности, для которого задействуются функции Комплекса, в т. ч. разворачивается виртуальная инфраструктура.
Миссия	Шаблон мероприятия, который включает в себя сценарий и реализацию компьютерных атак, модели визуализации, учебные материалы, данные для оценки результатов учебных мероприятий и навыков участников.
Триггер визуализации	Блок программного кода на JavaScript (как правило, это набор условных операторов), привязанный к объекту на сцене визуализации, который служит для обнаружения изменения состояния объекта на основании данных о состоянии мероприятия (текущий этап, успешность выполнения КА и т. п.) и при успешном выполнении условий изменяет графическое отображение (внешний вид) объекта на сцене.