АННОТАЦИЯ

к рабочей программе дисциплины

«Программное обеспечение анализа защищенности информационных систем и сетей»

Специальность 10.05.03 Информационная безопасность автоматизированных систем
Специализация специализация N 7 "Анализ безопасности информационных систем"
Квалификация выпускника специалист по защите информации
Нормативный период обучения 5 лет и 6 м.
Форма обучения очная
Год начала подготовки 2021

Цель изучения дисциплины: формирование у студентов основ знаний и приёмов работы с современным программным обеспечением для практического освоения принципов и методов обеспечения информационной безопасности, а также принципов, методологий и паттернов разработки современного безопасного программного обеспечения различных уровней интеграции.

Задачи изучения дисциплины:

- формирование знаний и умений использования программных и программно-аппаратные средства для моделирования и испытания систем защиты информационных систем;
- способствование развитию навыков анализа защищенности и верификации программного обеспечения информационных систем.

Содержание дисциплины:

Методология DevOps и непрерывная интеграция. Непрерывная поставка

Инфраструктура как сервис. Непрерывная безопасность. Безопасность на основе тестирования. Мониторинг и реагирование на атаки. Оценка рисков и усиление безопасности

Защита и тестирование веб-приложений: атаки на сайты и безопасность контента;

межсайтовые сценарии и политика безопасности контента; подделка межсайтовых запросов; кликджекинг и защита плавающих фреймов; Методы аутентификации пользователей: базовая HTTP-аутентификация; обслуживание паролей; поставщики идентификации; безопасность сессий и cookie-файлов; тестирование аутентификации. Управление зависимостями: golang-вендоринг; система управления пакетами Node.js

Уровень безопасности 2: защита облачной инфраструктуры. Защита и

тестирование облачной инфраструктуры: deployer: Настройка deployer; Настройка уведомлений между Docker Hub и deployer; Тестирование инфраструктуры;

Обновление среды invoicer

Ограничение сетевого доступа: тестирование групп безопасности; налаживание доступа между группами безопасности. Создание безопасной точки доступа: Генерирование SSH-ключей; создание хоста-бастиона в EC2; Внедрение двухфакторной аутентификации с помощью SSH; Отправка уведомлений о доступе; Рассуждения о группах безопасности; Открытие доступа для групп безопасности. Управление доступом к базе данных: Анализ структуры базы данных; Роли и права доступа в PostgreSQL; Определение минимальных прав доступа для приложения invoicer

Определение прав доступа в deployer

Каналы взаимодействия: ранняя симметричная криптография; алгоритм Диффи - Хеллмана и RSA"; инфраструктуры открытых ключей; SSL и TLS. Обзор SSL/TLS: цепочка доверия; установление TLS-соединения; совершенная прямая секретность. Настройка приложений на использование HTTPS: получение сертификата AWS; получение сертификата Let's Encrypt; применение HTTP на AWS ELB. HTTPS: тестирование TLS; HSTS: строгая защита транспорта; HPKP: закрепление открытых ключей

Распределение доступа к инфраструктуре управления кодом: управление правами доступа в GitHuЬ-организации; управление правами доступа в GitHub и Circle; подпись коммитов и меток с помощью Git; Управление доступом к хранилищу контейнеров: управление правами доступа в пределах Docker Hub и CircleCI; подписание контейнеров с помощью Docker Content Trust;

Распределение прав доступа для управления инфраструктурой: Управление правами доступа с помощью ролей и политик AWS; распределение закрытых данных в системах среды эксплуатации

Выявление аномалий и защита сервисов от атак: сбор и хранение журналов; сбор данных журналов из систем и приложений; сбор журналов от систем; сбор журналов приложения; журналирование инфраструктуры; сбор журналов от GitHub. Потоковая передача событий журналов с помощью брокеров сообщений. Обработка событий потребителями журналов. Хранение и архивация журналов. Анализ журналов.

Перечень формируемых компетенций:

ОПК-7.1. - Способен использовать программные и программно-аппаратные средства для моделирования и испытания систем защиты информационных систем;

ОПК-7.3. - Способен проводить анализ защищенности и верификацию программного обеспечения информационных систем;

Общая трудоемкость дисциплины: 9 з.е.

Форма итогового контроля по дисциплине: Экзамен