OTUS

Внедрение и работа в DevSecOps

Best Practice по внедрению и использованию новейших инструментов информационной безопасности в рамках DevOps CI / CD

Длительность курса: 212 академических часов

1 Базис знаний информационной безопасности

1 **Словарь, термины, стандарты, методики, источники информации, используемые в инструментах информационной безопасности**

Домашние задания

1 Ознакомиться с основными стандартами информационной безопасности

Цель: Ознакомиться со стандартами информационной безопасности:

1.NIST 800-53 для разделов:
https://nvd.nist.gov/800-53/Rev4/family/Access%20Control
https://nvd.nist.gov/800-53/Rev4/family/Configuration%20Management
https://nvd.nist.gov/800-53/Rev4/family/Identification%20and%20Authentication
https://nvd.nist.gov/800-53/Rev4/family/System%20and%20Communications%20Protection

2. CIS Benchmarsks
https://github.com/cismirror/benchmarks
2-3 документа по вашему выбору исходя из используемых на работе элементов.
или например:
https://github.com/cismirror/benchmarks/blob/master/CIS_Ubuntu_Linux_20.04_LTS_Benchmark_v1.0.0.pdf
https://github.com/cismirror/benchmarks/blob/master/CIS_Apache_HTTP_Server_2.4_Benchmark_v1.5.0.pdf

2 **Основные принципы обеспечения информационной безопасности стека приложений и инфраструктуры**

Домашние задания

1 Описать как в вашем стеке приложений используется принцип Defense In Depth

Цель: - Описать как в вашем стеке приложений (на вашем местеработы) используется принцип Defense In Depth.
- Если у вас нет собственного стека приложений (на вашем месте работы), выполнить аналогичную работу для предложенного примера

2 Обзор уязвимостей OWASP

1 **Разбор уязвимостей OWASP Top 10 Web**

Домашние задания

1 Провести симуляцию атаки по одной из предложенных уязвимостей OWASP Top 10 - Web

Цель: Провести симуляцию атаки по одной из предложенных уязвимостей OWASP Top 10 - Web на предоставленном стенде лабораторной работы

---

2 **Разбор уязвимостей OWASP Top 10 - Mobile**

Домашние задания

1 Провести симуляцию атаки по одной из предложенных уязвимостей OWASP Top 10 - Mobile

Цель: Провести симуляцию атаки по одной из предложенных уязвимостей OWASP Top 10 - Mobile на предоставленном стенде лабораторной работы

---

3 **Разбор уязвимостей OWASP Top 10 - IoT**

Домашние задания

1 Провести симуляцию атаки по одной из предложенных уязвимостей OWASP Top 10 - IoT

Цель: Провести симуляцию атаки по одной из предложенных уязвимостей OWASP Top 10 - IoT на предоставленном стенде лабораторной работы

---

4 **Разбор уязвимостей OWASP Top 10 - REST API**

Домашние задания

1 Провести симуляцию атаки по одной из предложенных уязвимостей OWASP Top 10 - REST API

Цель: Провести симуляцию атаки по одной из предложенных уязвимостей OWASP Top 10 - REST API на предоставленном стенде лабораторной работы

3 Особенности разработки безопасного кода и использования фреймворков

1 **Безопасная разработка в HTML/CSS**

Домашние задания

1 Проанализировать и устранить уязвимость в HTML/CSS коде

Цель: Проанализировать и устранить уязвимость в HTML/CSS коде из предложенного варианта, или в вашем собственном приложении

---

2 **Безопасная разработка в C/C++**

Домашние задания

1 Проанализировать и устранить уязвимость в C/C++ коде

Цель: Проанализировать и устранить уязвимость в C/C++ коде из предложенного варианта, или в вашем собственном приложении

---

3 **Безопасная разработка в Java**

Домашние задания

1 Проанализировать и устранить уязвимость в Java коде

Цель: Проанализировать и устранить уязвимость в Java коде из предложенного варианта, или в вашем собственном приложении

---

4 **Безопасная разработка в Node.js**

Домашние задания

1 Проанализировать и устранить уязвимость в Node.js коде

Цель: Проанализировать и устранить уязвимость в Node.js коде из предложенного варианта, или в вашем собственном приложении

---

5 **Безопасная разработка в Python**

Домашние задания

1 Проанализировать и устранить уязвимость в Python коде

Цель: Проанализировать и устранить уязвимость в Python коде из предложенного варианта, или в вашем собственном приложении

6 **Безопасная разработка в Go**

Домашние задания

1 Проанализировать и устранить уязвимость в Go коде

Цель: Проанализировать и устранить уязвимость в Go коде из предложенного варианта, или в вашем собственном приложении

7 **Безопасная разработка в .NET**

Домашние задания

1 Проанализировать и устранить уязвимость в .NET коде

Цель: Проанализировать и устранить уязвимость в .NET коде из предложенного варианта, или в вашем собственном приложении

8 **Безопасная разработка в Ruby**

Домашние задания

1 Проанализировать и устранить уязвимость в Ruby коде

Цель: Проанализировать и устранить уязвимость в Ruby коде из предложенного варианта, или в вашем собственном приложении

9 **Безопасная разработка в PHP**

Домашние задания

1 Проанализировать и устранить уязвимость в PHP коде

Цель: Проанализировать и устранить уязвимость в PHP коде из предложенного варианта, или в вашем собственном приложении

4 Моделирование и анализ возможных угроз и атак (Threat Modelling)

1 **Базовое моделирование угроз с использованием OWASP Top 10**

Домашние задания

1 Разработать модель угроз на основе OWASP Top 10

Цель: Разработать модель угроз на основе OWASP Top 10 для предложенного или вашего собственного приложения

---

2 **Продвинутое моделирование угроз с использованием ATP MITRE ATT&CK**

5 Разработка безопасных контейнерных и serverless приложений

1 **Обеспечение безопасности в Docker контейнерах**

Домашние задания

1 Протестировать Docker контейнер на предмет возможных уязвимостей

Цель: Протестировать Docker контейнер на предмет возможных уязвимостей на предоставленном стенде лабораторной работы, или ваш собственный Docker контейнер

---

2 **Обеспечение безопасности в Kubernetes**

Домашние задания

1 Протестировать Kubernetes приложение на предмет возможных уязвимостей

Цель: Протестировать Kubernetes приложение на предмет возможных уязвимостей на предоставленном стенде лабораторной работы, или ваш собственное Kubernetes приложение

---

3 **Обеспечение безопасности в Red Hat OpenShift**

6 Интеграция и работа с инструментами ИБ в рамках DevSecOps

1 **Обеспечение безопасности CI/CD тулчейна и DevOps процесса**

Домашние задания

1 Изучить существующие CI/CD с точки зрения доступных инструментов ИБ

Цель: Изучить существующие Managed Cloud SaaS для CI/CD (GitLab, CircleCI и др) на предмет наличия в них инструментов ИБ и подготовить сравнительную таблицу (написать статью в корпоративный Security Knowledge Base Portal)

---

2 **Обзор DevSecOps инструментария - часть 1 (Dev)**

Домашние задания

1 Собрать требования, которые определяют DevSecOps тулчейн

Цель: Собрать требования, которые определяют DevSecOps, написать статью в корпоративный Security Knowledge Base Portal

---

3 **Обзор DevSecOps инструментария - часть 2 (Ops)**

---

4 **Статический анализ исходного кода на безопасность (SAST)**

Домашние задания

1 Провести SAST тестирование

Цель: Провести SAST тестирование для предложенного или вашего собственного приложения

---

5 **Динамический анализ приложений на безопасность (DAST/IAST)**

Домашние задания

1 Провести IAST/DAST тестирование

Цель: Провести IAST/DAST тестирование для предложенного или вашего собственного приложения

---

6 **Анализ использования**

Домашние задания

	стороннего и открытого программного обеспечения (SCA) и Тестирование конфигурации на соответствие стандартам безопасности (CIS, NIST, PCI-DSS)	1 Провести SCA тестирование Цель: Провести SCA тестирование для предложенного или вашего собственного приложения
7	**Усиление конфигурации и патчинг (Configuration Hardening, Patching)**	
8	**Применение менеджмента секретов и сертификатов (Secrets and Certificates Management)**	
9	**Применение защиты для REST-API внутри микро-сервисных приложений и на back-end**	Домашние задания 1 Провести REST API тестирование Цель: Провести REST API тестирование для предложенного или вашего собственного приложения
10	**Применение Web-Application Firewall (WAF) для защиты Web, REST API, Bot protection**	Домашние задания 1 Подготовить конфигурацию WAF для REST API Цель: Подготовить конфигурацию WAF для REST API для предложенного или вашего собственного приложения
11	**Система обнаружения / предотвращений вторжений (IDS/IPS)**	Домашние задания 1 Подготовить конфигурацию IDS/IPS Цель: - Подготовить конфигурацию IDS/IPS для предложенного или вашего собственного приложения - Провести симуляцию атаки - Проанализировать результаты обнаружения и предотвращения атаки

12	**Ручное и автоматизированное тестирование на проникновение (Penetration Testing)**	Домашние задания 1 Провести Pen-Test тестирование Цель: Провести Pen-Test тестирование для предложенного или вашего собственного приложения	
13	**Мониторинг безопасности и реакция на события в ИБ (SIEM/SOAR)**		
14	**Криминалистическая экспертиза (Forensic Analysis)**	Домашние задания 1 Провести криминалистическую экспертизу (Forensic Analysis) Цель: - Выполнить атаку на предложенном стенде лабораторной работы или для вашего собственного приложения - Провести криминалистическую экспертизу (Forensic Analysis)	
15	**План проекта и методика трансформации организации в DevSecOps**		

7 Проектный модуль

1 **Выбор темы**

Домашние задания

1 Выбрать тему проектной работы

Цель: Выбрать тему проектной работы из предложенных или по вашему усмотрению

---

2 **Консультации и обсуждения проектной работы**

Домашние задания

1 Консультация по выполнению проектной работы

Цель: При необходимости запросить и получить консультацию по выполнению проектной работы

---

3 **Защита проектов**

Домашние задания

1 Защита проектной работы

Цель: Выполнить проектную работу
Сдать на проверку проектную работу
Получить результат проверки проектной работы