Пентест. Базовый курс

Длительность курса: 64 академических часа

1 Операционные системы

1	**Общие принципы работы операционной системы Windows с точки зрения безопасности. Механизмы разграничения доступа.**	занятие описывает общие подходы к построению подсистем защиты операционных систем. Будут рассмотрены следующие понятия: менеджер памяти, исполняющая подсистема, монитор безопасности, работа пользователей в операционной системе, разграничение доступа
2	**Windows основные механизмы, затрагиваемые при атаках**	занятие посвящено локальным и удаленным атакам. Будут разобраны основные структуры и механизмы которые задействуется при: эскалации привелегий, эксплуатации уязвимостей, связанных с работой с памятью.
3	**MacOS, iOS**	занятие описывает основные подсистемы операционных систем, которые отвечают за безопасность. Будут рассмотрены основные механизмы и архитектура операционных систем.
4	**MacOS, iOS**	занятие описывает основные атаки, которые существуют для указанных операционных систем. Эскалации привилегий и удаленные атаки. Для проведения тестирования и исследования почему работает та или иная атака будет проведен анализ подсистем ОС или/и уязвимых приложени
5	**Linux**	занятие рассматривает основные механизмы разграничения доступа в операционной системе, подсистему выполнения

		команд.
6	**Linux**	занятие рассказывает об основных методах атак на операционную систему. Будут описаны атаки: Эскалация привилегий, атаки с использованием бинарной эксплуатации узявимостей.
7	**Android**	занятие содержит в себе информацию по основным механизмам операционной системы, которые используются при компроментации. Рассматриваются архитектурные особенности.
8	**Android**	рассматриваются основные атаки, возможные в операционной системе.

2 Фреймворки для тестирования на проникновение

1	**Что такое FrameWork: общие понятия, принципы работы**	занятие рассказывает о базовых проблемах связанных с организацией доступа к различным тестируемых системам. Рассматриваются проблемы с открытием доступа по сети, выполнением команд, детектированием подсистемами защиты. В качестве завершающего этапа приводится пример реализации требуемого функционала во Framework`е Metasploit.
2	**Архитектура Metasploit: основные данные.**	занятие содержит информацию по популярному фреймворку, который позволяет автоматизировать работу по доступу к тестируемых операционным системам. Рассматриваются следующие вопросы: архитектура, основные сценарии использования.
3	**Metasploit Payloads**	чем может помочь фреймворк если: ограничена среда выполнения команд, нет возможности для запуска нативных приложений, нужно протестировать систему с включенной подсистемой защиты.
4	**Empire, как, только и когда?**	особенности фреймворка, основные методы, которыми он пользуется, проведения тестирования систем с его использованием.
5	**dropengine**	занятие затрагивает темы работы с фреймворками, что они не позволяют сделать из коробки? Почему 100 раз закодированный файл все равно не работает в тестируемый системе? Рассматривается кастомизация на основе нового фреймворка с Defcon 2020.
6	**koadic**	занятие рассказывает о том как можно воспользоваться внутренними механизмами операционной системы, чтобы получить доступ и выполнить команды.
7	**Сценарии тестирования операционных систем с использованием изученных фреймворков. Часть 1**	занятия подразумевают, что для закрепления информации о всех фреймворках, необходимо провести тестирование систем с использованием какого-то заданного фреймворка или фрагментов всех изученных.
8	**Сценарии тестирования операционных систем с использованием изученных**	занятия подразумевают, что для закрепления информации о всех фреймворках, необходимо провести тестирование систем с использованием какого-то заданного фреймворка или фрагментов всех изученных

фреймворков.
Часть 2

3 Reverse для пентеста

1	**Windows**	как исследовать поведение эксплойта, найденного в сети? Какие есть инструменты?
2	**Windows**	как разобраться что делает приложение в операционной системе? Какие сетевые и локальные ресурсы использует?
3	**MacOs**	как исследовать поведение эксплойта, найденного в сети? Какие есть инструменты?
4	**MacOS**	как разобраться что делает приложение в операционной системе? Какие сетевые и локальные ресурсы использует?
5	**Android**	как разобраться что делает приложение в операционной системе? Какие сетевые и локальные ресурсы использует?
6	**Анализ приложений. Ч.1**	поиск скрытого функционала приложений, обнаружение небезопасного использования ресурсов.
7	**Анализ приложений. Ч.2**	поиск простых уязвимостей, которые ведут к отказу в обслуживании приложения.
8	**Анализ приложений. Ч.3**	поиск «уязвимостей» архитектуры приложения

4 Web технологии

1	**Как работает современный Web?**	занятия рассказывает об основных архитектурах, которые применяются в web-приложениях. Рассказывается об основных отличиях frontend и backend.
2	**Что такое реляционные базы данных и какие они бывают? Исследование основных функций**	занятие знакомит с популярными базами данных, а так же демонстрирует их основной функционал. Особый упор делается на функционал «полезный» для проведения тестирования на проникновение.
3	**Что такое нереляционные базы данных и какие они бывают? Исследование основных функций**	занятие знакомит с популярными базами данных, а так же демонстрирует их основной функционал. Особый упор делается на функционал «полезный» для проведения тестирования на проникновение.
4	**Языки программирования frontend. Особенности и узявимости. Часть 1**	занятие показывает основные особенности языков программирования. Типы ошибок и уязвимостей, которые им присущи.
5	**Языки программирования frontend. Особенности и узявимости. Часть 2**	занятие показывает основные особенности языков программирования. Типы ошибок и уязвимостей, которые им присущи.
6	**Языки программирования backend. Особенности и узявимости. Часть 1**	занятие показывает основные особенности языков программирования. Типы ошибок и уязвимостей, которые им присущи.
7	**Языки программирования backend. Особенности и узявимости. Часть 2**	занятие показывает основные особенности языков программирования. Типы ошибок и уязвимостей, которые им присущи.
8	**Атаки на web-приложения**	занятие содердит информацию по основным методикам и подходам для проведения тестирования на проникновения web-приложений.