
OTUS
ОНЛАЙН-ОБРАЗОВАНИЕ
Онлайн-образование

Не забыть включить запись!

Меня хорошо видно && слышно?

Ставьте + , если все хорошо
Напишите в чат, если есть проблемы

МОДУЛЬ #1
Знакомство со структурой курса, используемое программное обеспечение

Казанцев Анатолий
преподаватель
+7 (499) 110-61-65

Преподаватель

Александр Колесников

- Специалист по комплексной защите объектов информатизации с большим опытом в реверс-инжиниринге, исследовании вредоносного кода и анализе уязвимостей
- Сертификаты: BEC II Advanced (2013 г.), CEH (2016 г.)

Преподаватель

Анатолий Казанцев

- Около 3х лет опыта работы вирусным аналитиком
- Международный сертификат по тестированию на проникновение (pentest) Offensive Security Certified Professional

Правила вебинара

Активно участвуем

Задаем вопрос в чат или голосом

Off-topic обсуждаем в Slack #general или #pentest-2019-09

Вопросы вижу в чате, могу ответить не сразу

Маршрут вебинара

Структура и содержание курса

Рекомендации для саморазвития

Необходимое ПО

Рефлексия

Цели вебинара

1. Познакомимся со структурой курса, темами в модулях.
2. Узнаем, какое ПО необходимо в первую очередь для настройки рабочего окружения.
3. Рассмотрим дополнительные источники информации по теме курса, тренировочные площадки.

СТРУКТУРА КУРСА

Модули курса

Модуль 1: Введение. Основы, которые пригодятся на курсе

Модуль 2: Сетевая безопасность

Модуль 3: Повышение привилегий

Модуль 4: Web pentest

Модуль 5: Консультации по выпускной работе

МОДУЛЬ 1

Модуль №1

Часть курса, которая расскажет об основных инструментах, которые будут использоваться на протяжении всего курса

Основные темы модуля №1

- Знакомство со структурой курса
- Общее понимание тестирования на проникновение
- Online-сервисы для пассивного сбора информации
- Изучение наборов инструментов (Kali Linux, Metasploit Framework)
- Повторение основ сетевого взаимодействия (стэк TCP/IP)
- Сканирование и идентификация сервисов

Цели модуля №1

- Узнаем минимальные основы для дальнейшего изучения материалов курса
- Сформируем навыки работы с инструментарием
- Наладим взаимодействие по курсу в целом
- Настроим рабочее окружение для практических работ

МОДУЛЬ 2

Модуль №2

Описание основных механизмов сетевого взаимодействия на «пальцах»

Основные темы модуля №2

- Основные сетевые протоколы на примере записанного трафика
- Работа с сетевыми пакетами на «низком» уровне (Scapy)
- Сетевые подсистемы популярных операционных систем
- Обзор атак на сетевое взаимодействие

Цели модуля №2

- Научимся работать с популярными утилитами мониторинга сетевого трафика
- Подробнее ознакомимся с форматами сетевых пакетов
- Изучим подходы к анализу сетевого взаимодействия
- Рассмотрим как производятся атаки на сетевое взаимодействие

МОДУЛЬ 3

Модуль №3

Безопасность операционных систем. Штатные механизмы разграничения доступа

Основные темы модуля №3

- Методы разграничения доступа в ОС Windows
- Методы разграничения доступа в ОС Linux
- Как подсистемы ОС противодействуют выполнению вредоносного кода
- Практические занятия по теме

Цели модуля №3

- Изучим механизмы и подходы разграничения доступа в ОС Windows и Linux
- Познакомимся с основными инструментами
- Узнаем, как это все заставить работать на пользователя
- Узнаем основные преграды со стороны ОС на пути вредоносного кода

МОДУЛЬ 4

Модуль №4

Безопасность Web-приложений. Виды атак и уязвимостей

Основные темы модуля №4

- Классификация веб-уязвимостей
- Разбор некоторых Proof-Of-Concept (PoC) для эксплуатации ПО
- Подробный разбор каждого типа уязвимости
- Практические занятия по теме

Цели модуля №4

- Познакомимся с наиболее популярными типами веб-атак и уязвимостей
- Получим навыки работы с основными инструментами
- Применим методики поиска веб-уязвимостей
- Наконец-то выясним, куда подставлять кавычку! ☺

МОДУЛЬ 5
ВЫПУСКНАЯ РАБОТА

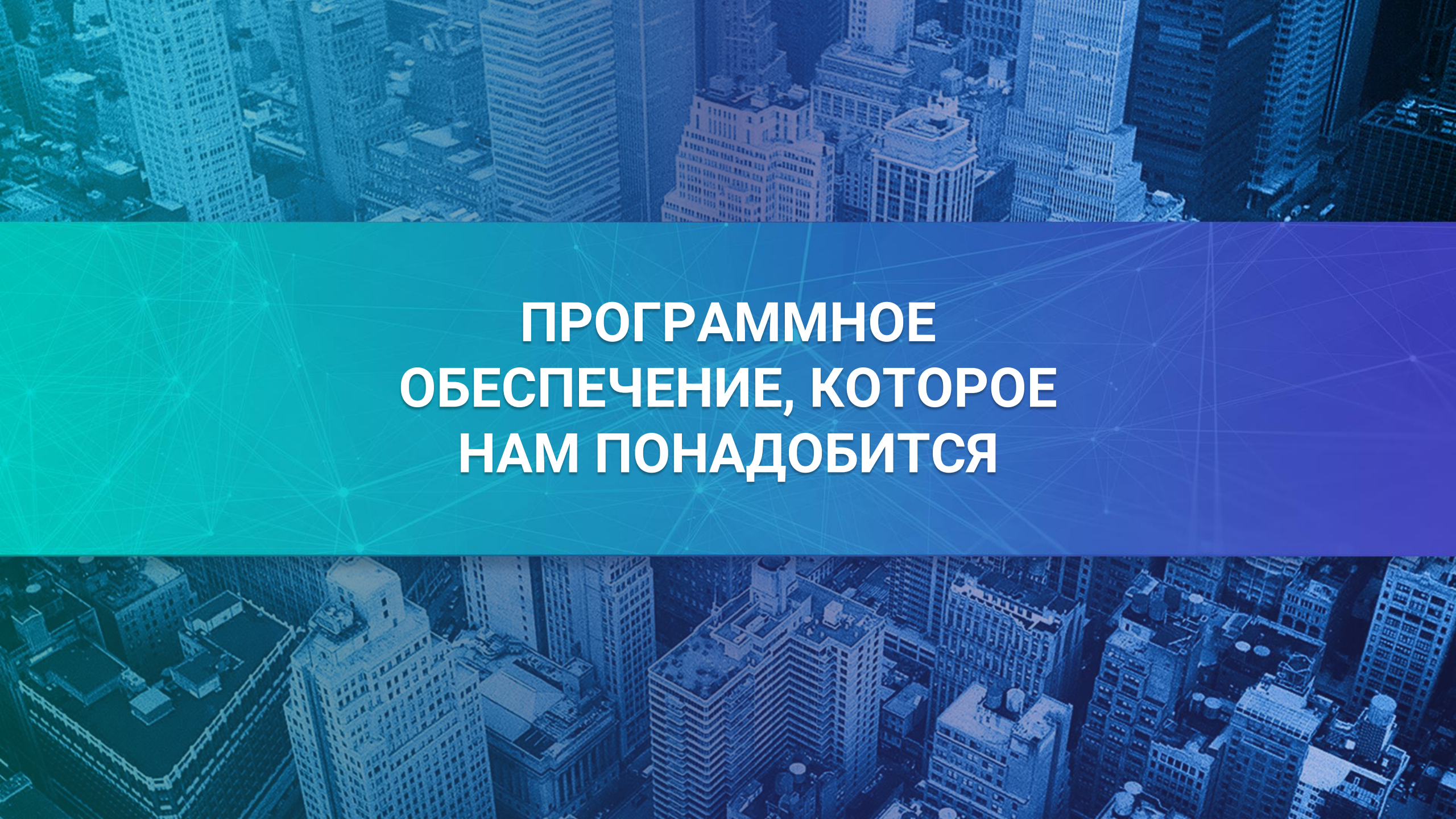
Модуль №5

Выпускная работа в формате соревнований
Capture The Flag (CTF)

РЕКОМЕНДАЦИИ ПО ОСВОЕНИЮ ТЕМ КУРСА

Список рекомендуемых ресурсов

ТЕМА	РЕСУРС
Reverse Engineering	https://beginners.re/
CTF соревнования	https://ctftime.org/
Wargame (Linux basics)	http://overthewire.org/wargames/bandit
Wargame (Web)	http://overthewire.org/wargames/natas/
Соревнования (Web, Forensic, Network)	https://www.root-me.org/en/Challenges/
Web	https://hack.me/s/
Blog Portswigger	https://portswigger.net/blog
∞	∞



ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ, КОТОРОЕ НАМ ПОНАДОБИТСЯ

Список необходимого софта

НАЗВАНИЕ	РЕСУРС
Virtual Box	https://www.virtualbox.org/wiki/Downloads
Kali Linux (Kali Linux 32-Bit или 64-Bit)	https://www.kali.org/downloads/
Ubuntu Desktop	https://ubuntu.com/download/desktop
Docker	https://www.docker.com/
Windows VMs	https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/

Домашнее задание

1. Самостоятельно ознакомиться с дополнительными материалами, тренировочными площадками.

2. Загрузить необходимое ПО, которое мы рассмотрели на занятии.

Срок: 2 дня

Рефлексия

Отметьте 3 пункта, которые вам запомнились с вебинара

Следующий вебинар

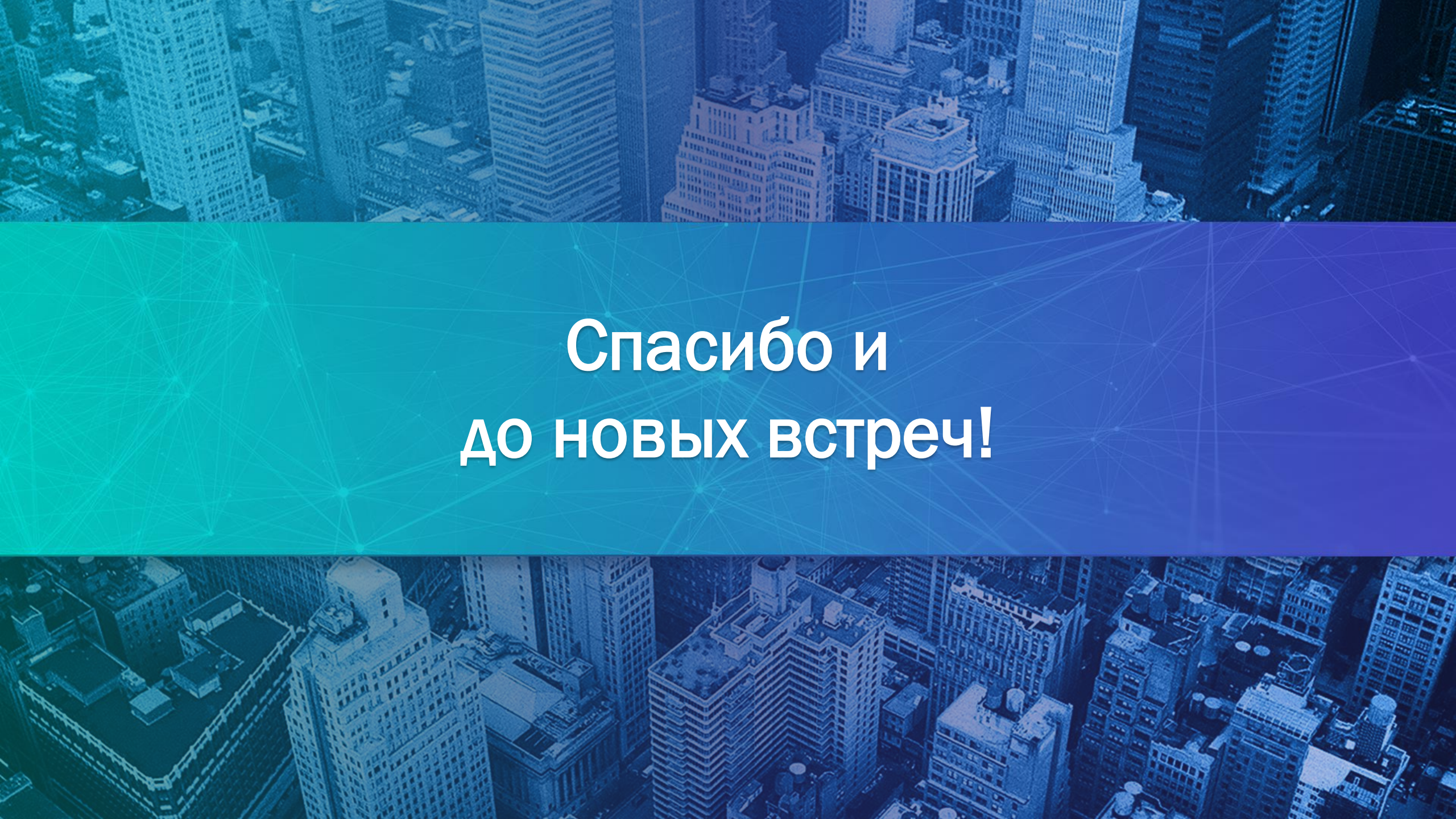
Тема: «Что такое тестирование на проникновение и зачем оно нужно»

3 октября 2019 г. в 20:00

Ссылка на вебинар будет в личном кабинете за 15 минут до начала

Материалы к занятию в ЛК — можно изучать

Обязательный материал обозначен красной лентой


Спасибо и
до новых встреч!