
OTUS
ОНЛАЙН-ОБРАЗОВАНИЕ
Онлайн-образование

Не забыть включить запись!

Меня хорошо видно && слышно?

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

Тестирование на проникновение. Методика и цели

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

Общие определения. Виды пентеста

Методики пентеста

Курсы и сертификации

Рефлексия

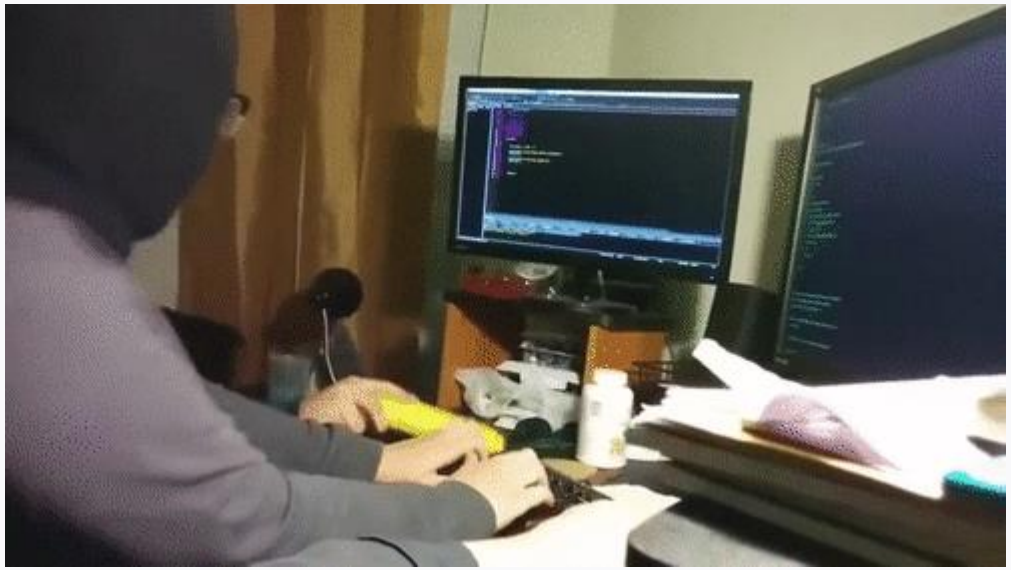
Цели вебинара

1. Познакомимся с терминологией и определениями
2. Узнаем, какие существуют виды методик тестирования на проникновение
3. Проведем обзор курсов и сертификаций по тестированию на проникновение

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Что такое pentest?

Тестирование на проникновение - метод оценки безопасности компьютерных систем и сетей посредством санкционированного моделирования атак злоумышленников.



Что такое pentest?

Часто употребляется жаргонный термин пентест/pentest, от английского
PENetration TESTing

Чем не является pentest.

Использование только лишь одних сканеров уязвимостей при проведении тестирования на проникновение не может дать надежного результата.

https://www.owasp.org/index.php/Category:Vulnerability_Scanning_Tools

Анализ защищенности

Анализ защищенности (vulnerability assessment) - проведение полного комплекса мероприятий по техническому аудиту внутренней ИТ-инфраструктуры компании.

Анализ защищенности vs. Pentest

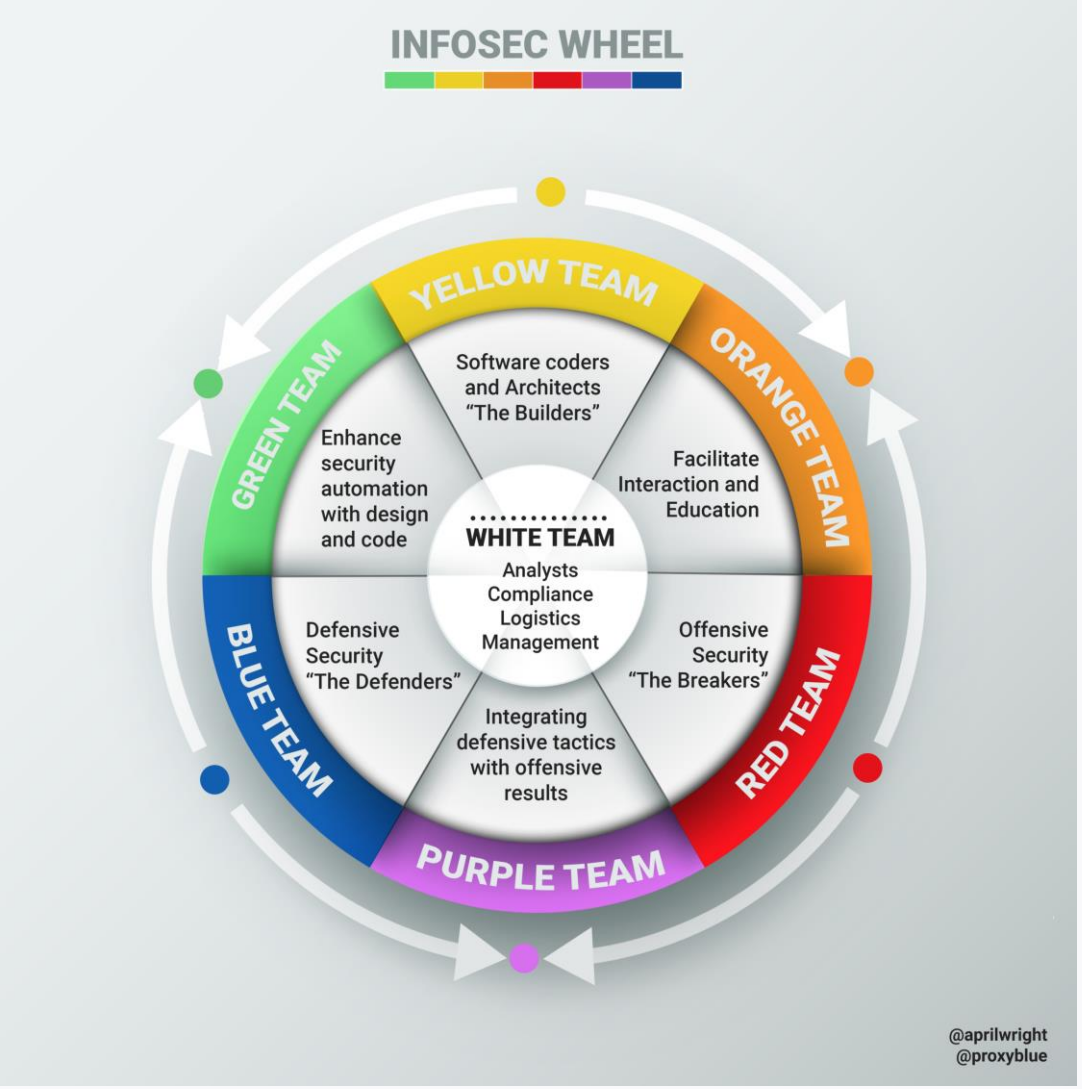
Анализ защищенности	Пентест
Поиск максимального количества уязвимостей	Достижение поставленной задачи
Использование сканеров уязвимостей	Сканеры уязвимостей + ручное тестирование
Оценка рисков безопасности	Эксплуатация уязвимостей

Red Team vs. Blue Team

Red Team	Blue Team
Атакующая сторона	Обороняющаяся сторона
Эксплуатация уязвимостей	Реагирование на инциденты
Этичный взлом	Защита периметра и внутренней инфраструктуры
Социальная инженерия, физическое проникновение на территорию заказчика,..	Охота за угрозами (threat hunting)

Физический пентест

<цвет> Team

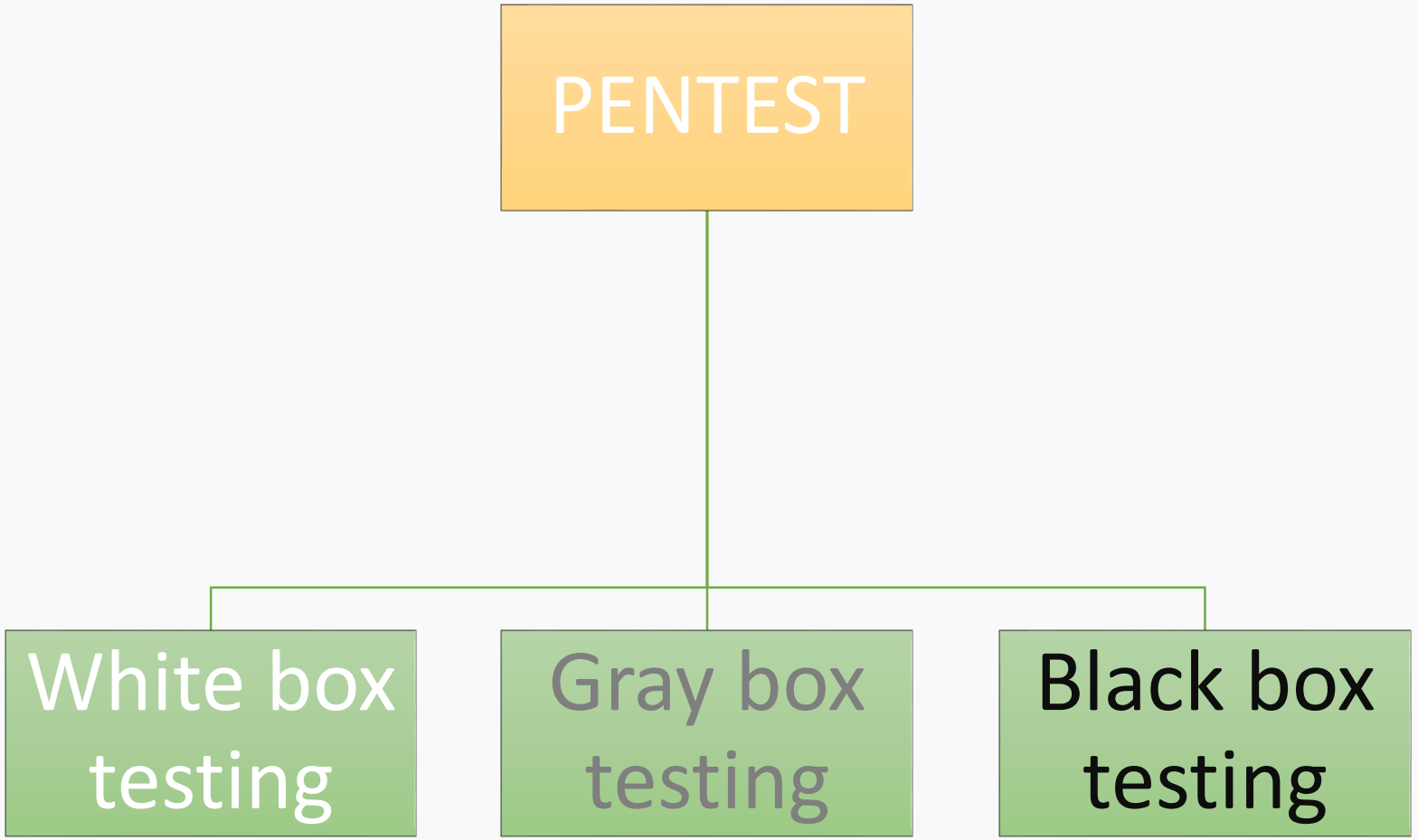

INFOSEC WHEEL
YELLOW TEAM
ORANGE TEAM
RED TEAM
PURPLE TEAM
BLUE TEAM
GREEN TEAM
Software coders and Architects "The Builders"
Facilitate Interaction and Education
Offensive Security "The Breakers"
Integrating defensive tactics with offensive results
Defensive Security "The Defenders"
Enhance security automation with design and code
WHITE TEAM
Analysts
Compliance
Logistics
Management
@aprilwright
@proxyblue

Red Team vs. Pentest

Red Team	Пентест
Команду обороняющихся не предупреждают	Команда защиты обычно предупреждена о проведении пентеста
Проведение работ 24/7	Время проведения работ, как правило, согласуется
Тестируется все, что может представлять потенциальную угрозу для защиты	Список целей согласуется с заказчиком
Часть инструментария пишется под конкретную цель	Использование готовых утилит, фреймворков и скриптов

ВИДЫ ПЕНТЕСТА.
УРОВЕНЬ ИНФОРМАЦИИ О ЦЕЛИ

Виды пентеста



White box testing

Пентестер получает в свое распоряжение всю необходимую информацию:

- IP-адреса,
- исходные коды,
- компоненты приложения,
- схему сети,..

Gray box testing

Пентестер располагает частичной или лимитированной информацией о тестируемой системе:

- роли компонентов,
- внутренние механизмы (поверхностно),
- используемые алгоритмы,..

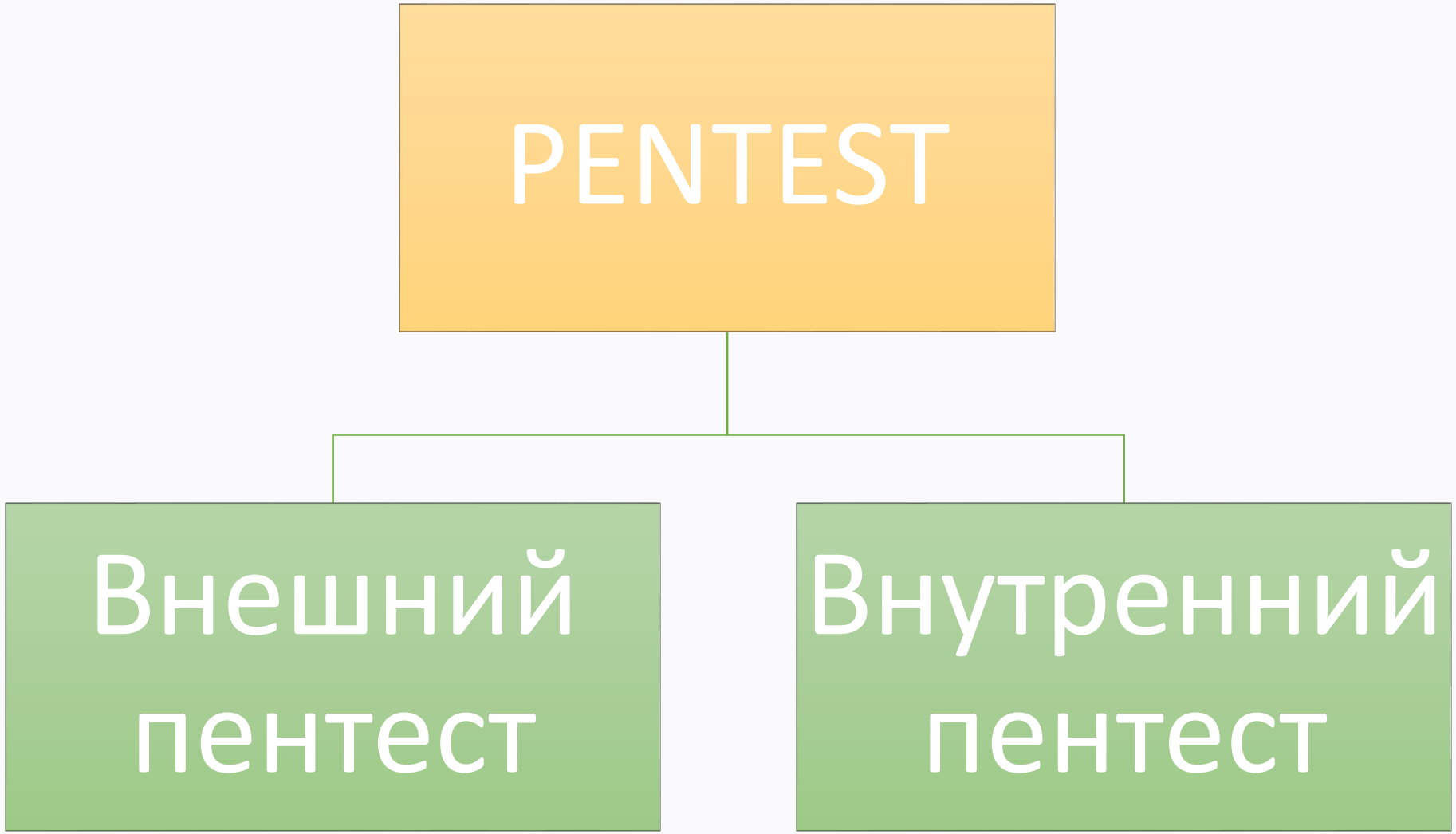
Black box testing

Изначально пентестер не располагает никакой информацией о системе:

- имитация действий злоумышленника;
- разведка;
- поиск скрытого функционала,
- поиск ошибок конфигурации,..

ВИДЫ ПЕНТЕСТА. МОДЕЛИ ЗЛОУМЫШЛЕННИКА

Виды пентеста



Тестирование внешнего периметра

- Имитация действий злоумышленника;
- Разведка (IP-адреса, поддомены, emails);
- Данные из открытых источников (OSINT);
- Поиск скрытого функционала;
- Тестирование систем, подключенных к Интернету;
- Социальная инженерия.

Цели: проникнуть во внутреннюю сеть, получить доступ к важным данным, вызвать отказ в обслуживании,..

Тестирование внутренней сети

- Имитация инсайдерских атак;
- Создание дополнительного слоя защиты в случае «пробива» внешнего периметра;
- Сбор данных о топологии сети;
- Сбор данных о пользователях;
- Атаки Man in the Middle (MitM);
- Атаки на домен.

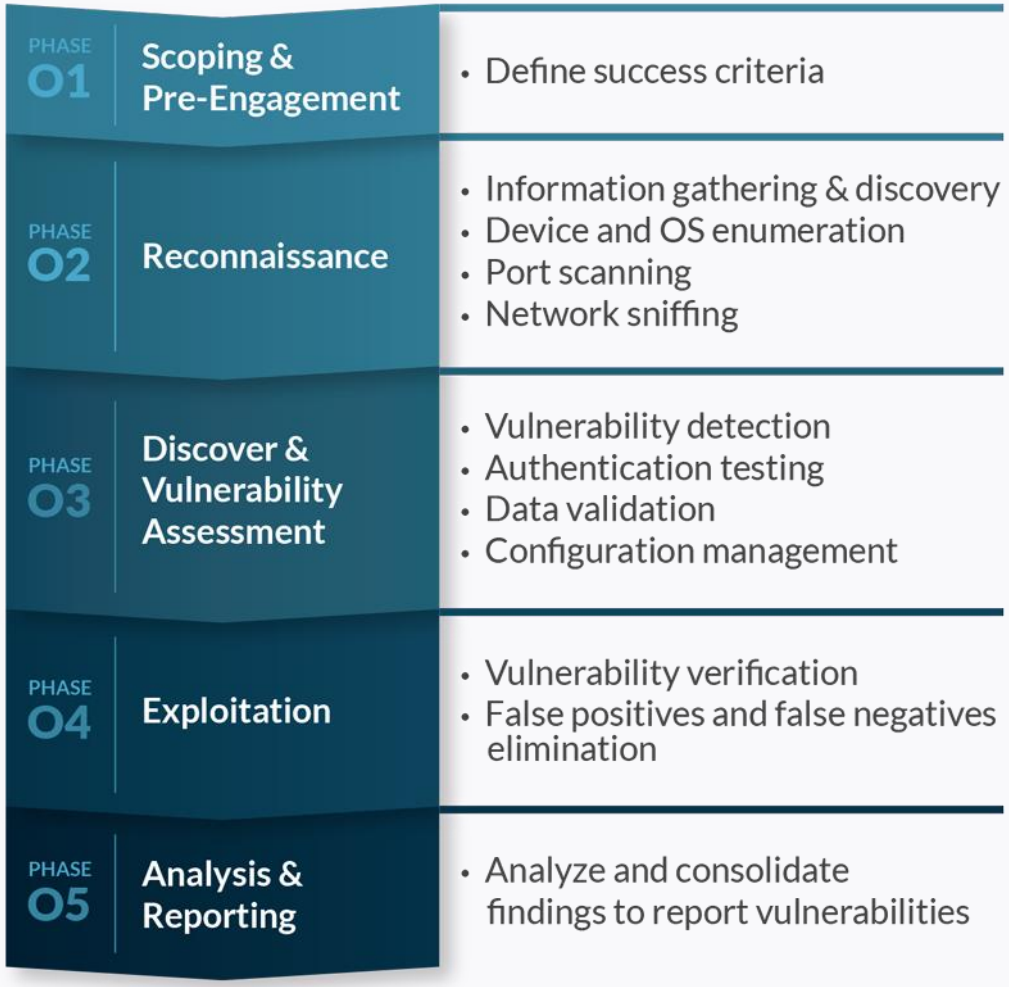
Цели: проникнуть и закрепиться во внутренней сети, получить доступ к важным данным,..

МЕТОДИКИ ПРОВЕДЕНИЯ ПЕНТЕСТА

Cyber Kill Chain

https://lukatsky.blogspot.com/2016/10/kill-chain.html

Методология пентеста



https://www.pratum.com/images/content/penetration-testing-methodology.png

Penetration Testing Execution Standard (PTES)

Вместо простого описания методологии или процесса PTES предоставляет практические руководства о том что и как тестировать, рекомендации по инструментам (утилиты, сервисы) и их использованию.

www.pentest-standard.org/index.php/PTES_Technical_Guidelines

Open Source Security Testing Methodology Manual (OSSTMM)

Структурированный, систематизированный подход, но мало информации по конкретным действиям и инструментам

https://www.isecom.org/OSSTMM.3.pdf

MITRE ATT&CK

ATT&CK™

База знаний методик и тактик, основанная на реальных атаках. Призвана послужить базой для разработки собственной модели угроз в частных компаниях, государственных учреждениях, защитных решениях.

https://attack.mitre.org

Open Web Application Security Project (OWASP)

Методика поиска уязвимостей в веб-приложениях

https://www.owasp.org/index.php/OWASP_Testing_Project

PCI DSS

Payment Card Industry Data Security Standard.

Стандарт представляет собой совокупность 12 детализированных требований по обеспечению безопасности данных о держателях платёжных карт, которые передаются, хранятся и обрабатываются в информационных инфраструктурах организаций. Принятие соответствующих мер по обеспечению соответствия требованиям стандарта подразумевает комплексный подход к обеспечению информационной безопасности данных платёжных карт.

https://www.pcisecuritystandards.org

КУРСЫ, СЕРТИФИКАЦИИ И ЛАБОРАТОРИИ

PWK/OSCP

Название курса - **Penetration Testing with Kali Linux**

Сертификация - **Offensive Security Certified Professional**

Один из немногих курсов практической направленности. Призван сформировать базовые навыки, подходы и методики в области пентеста.

Минусы: анализ безопасности Active Directory практически не рассматривается.

https://www.offensive-security.com/

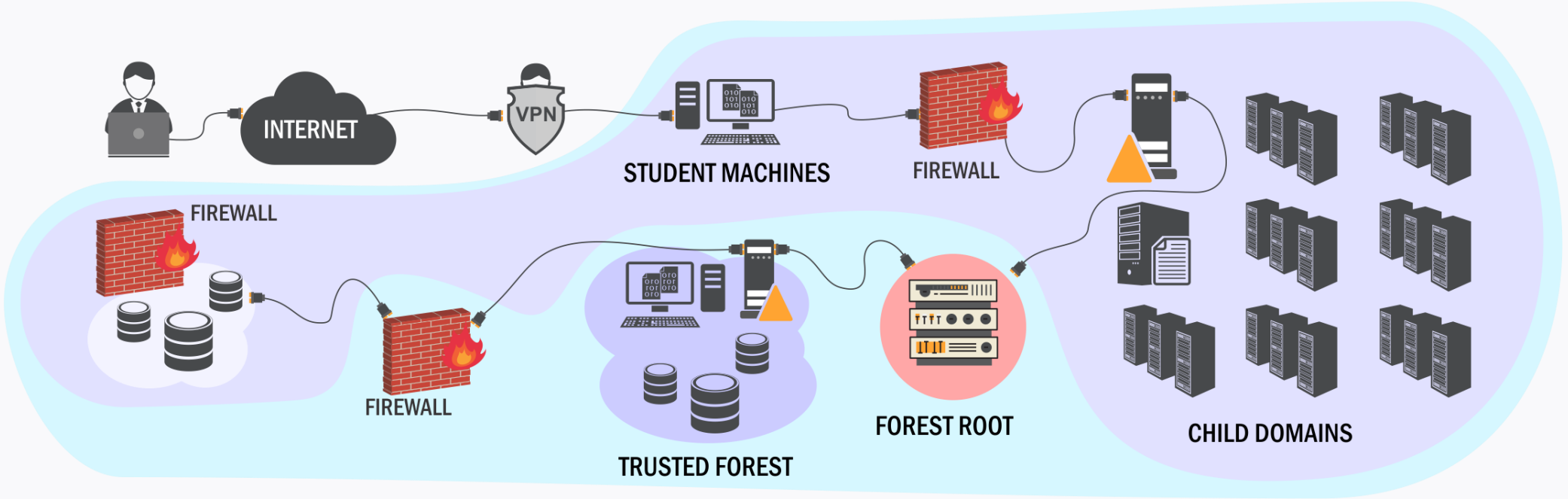
CEH

Одна из самых популярных сертификаций.

Международный уровень.

https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/

Pentester Academy



https://www.pentesteracademy.com/activedirectorylab

Список курсов и сертификаций

Название курса/сертификации	Ссылка
Cracking The Perimeter (CTP) Offensive Security Certified Expert (OSCE)	link
SANS SEC542 - GWAPT	link
SANS SEC560 - GPEN	link
SANS SEC575 - GMOB	link
SANS SEC660 - GXPN	link
CompTIA Security+	link
Pentestit. Курсы этичного хакинга	link

Домашнее задание

Самостоятельно ознакомиться с материалами по предоставленным ссылкам.

Срок: нет

Рефлексия

Отметьте 3 пункта, которые вам запомнились с вебинара

Следующий вебинар

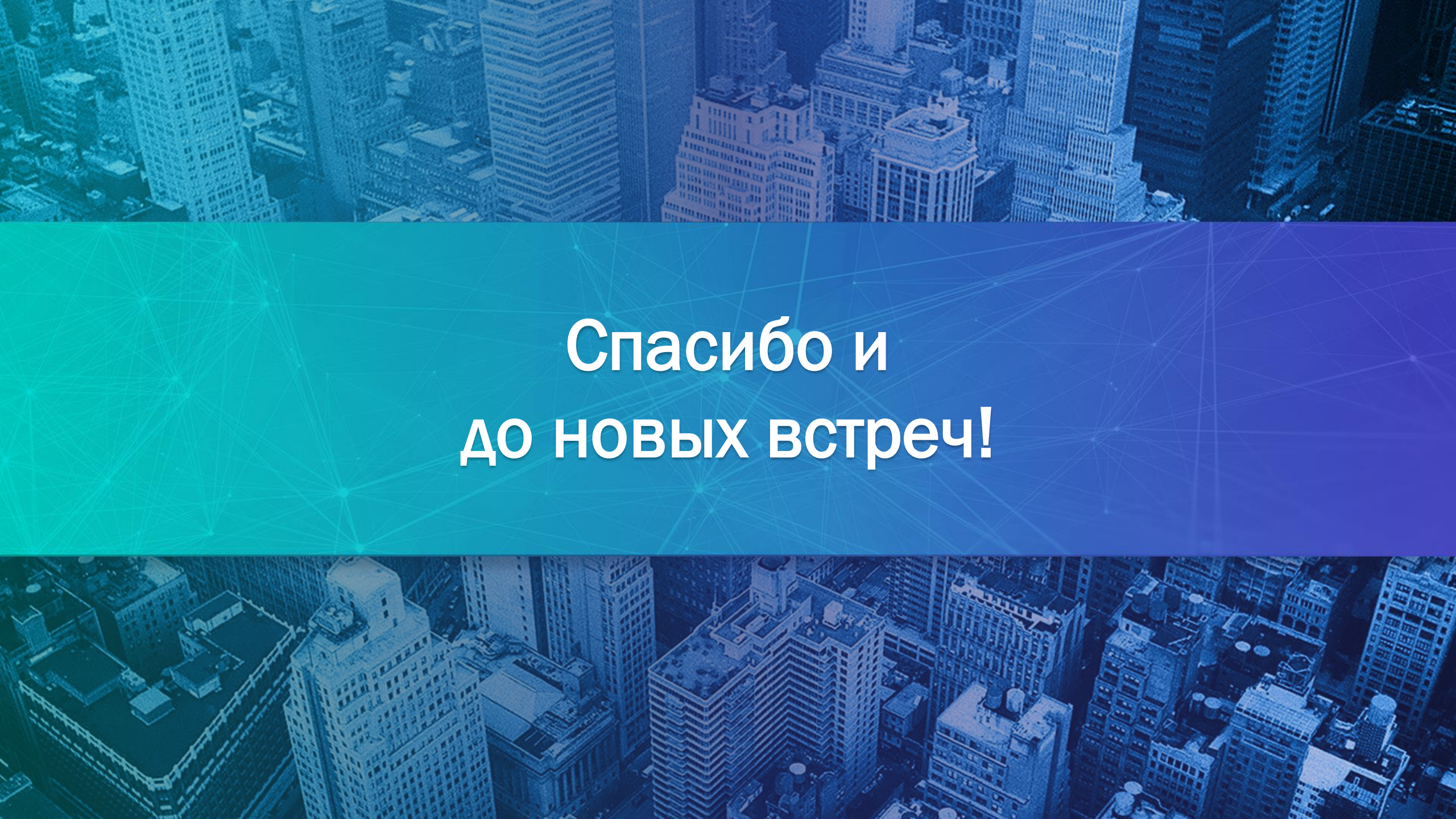
Тема: «Полезные online сервисы для пассивного сбора информации»

Вторник 8 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!