



Академия АйТи
a Softline Company



Тестирование на проникновение и анализ безопасности. Профессиональный уровень

Код курса: EH2

Тестирование на проникновение и анализ безопасности. Профессиональный уровень

Код курса: EH2

Длительность	72 ак. часа
Формат	Очно; Дистанционно
Разработчик курса	Академия АйТи
Тип	Учебный курс
Способ обучения	Под руководством тренера

О курсе

Курс является логическим продолжением курса «Тестирование на проникновение и анализ безопасности. Базовый уровень» и предназначен для практического закрепления полученных навыков и уверенного их применения в работе.

Подробная информация

Успешное окончание курса позволит специалистам:

Подготавливать и настраивать виртуальные машины

Осуществлять взлом хоста на платформе Linux

Осуществлять защиту хоста на платформе Linux

Взламывать и защищать сетевой узел на платформе Windows

Осуществлять проникновение в локальную сеть компании

Собирать и настраивать ядра Linux с патчами безопасности

Необходимая подготовка

Успешное завершение курса «Тестирование на проникновение и анализ безопасности. Базовый уровень» или аналогичная подготовка

Цель курса

Формирование и совершенствование знаний и навыков, необходимых для проведения тестирования

на проникновение и анализа безопасности

Программа курса

Модуль 1. Подготовка и настройка виртуальных машин

Настройка Windows Server

Настройка Kali Linux

Импорт и развертывание жертвы для взлома на платформе Linux

Импорт и развертывание жертвы для взлома повышенной сложности (используется для взлома виртуальной корпоративной сети)

Модуль 2. Взлом хоста на платформе Linux

Сканирование

Проверка на наличие web-приложений

Проверка на возможность взлома web-приложений

Выявление потенциально уязвимых сервисов

Использование Metasploit для проверки существующих уязвимостей

Подготовка отчета о результатах тестирования

Подготовка рекомендаций по устранению найденных недостатков

Модуль 3. Защита хоста на платформе Linux

Применение сетевого суперсервера для ограничения доступа к сервисам

Использование политик безопасности SELinux/AppArmor в Linux, MAC во FreeBSD

Виртуализация серверов с использованием технологий OpenVZ/LXC в Linux и Jail во FreeBSD

Виртуализация приложений путем совмещения помещения сервисов в Chroot и применения к ним политик безопасности

Модуль 4. Взлом сетевого узла на платформе Windows

Сканирование

Выявление потенциально уязвимых сервисов

Использование Metasploit для проверки существующих уязвимостей

Подготовка отчета о результатах тестирования

Подготовка рекомендаций по устранению найденных недостатков

Модуль 5. Защита сетевого узла на платформе Windows

Усиление политик безопасности там, где не требуется совместимость с предыдущими версиями Windows

Виртуализация серверов с использованием технологии Hyper-V

Виртуализация приложений с использованием технологии App-V (ранее SoftGrid)

Использование службы управления правами (AD RMS)

Модуль 6. Проникновение в локальную сеть компании

Сбор данных с сайта компании

Проверка корпоративного сайта на подверженность web-уязвимостям

Тестирование на возможность раскрытия данных с сайта компании

Сканирование доступных ресурсов компании

Выявление потенциально уязвимых сервисов

Проверка потенциально уязвимых сервисов на предмет возможности эксплуатации уязвимостей

Проникновение через найденные уязвимости

Использование полученного доступа для дальнейшего проникновения

Повторение этого списка шагов, пока не будет получен полный доступ ко всем сетевым узлам корпоративной сети

Подготовка отчета о результатах тестирования

Подготовка рекомендаций по устранению найденных недостатков

Установка и настройка EMET (Enhanced Mitigation Experience Toolkit) на Windows Server

Модуль 7. Сборка и настройка ядра Linux с патчами безопасности

Сборка и настройка ядра Linux с патчами GRSecurity и PaX

[Посмотреть расписание курса и записаться на обучение](#)

Обращайтесь по любым вопросам
к менеджерам Академии АйТи

+7 (495) 150 96 00 | academy@academyit.ru