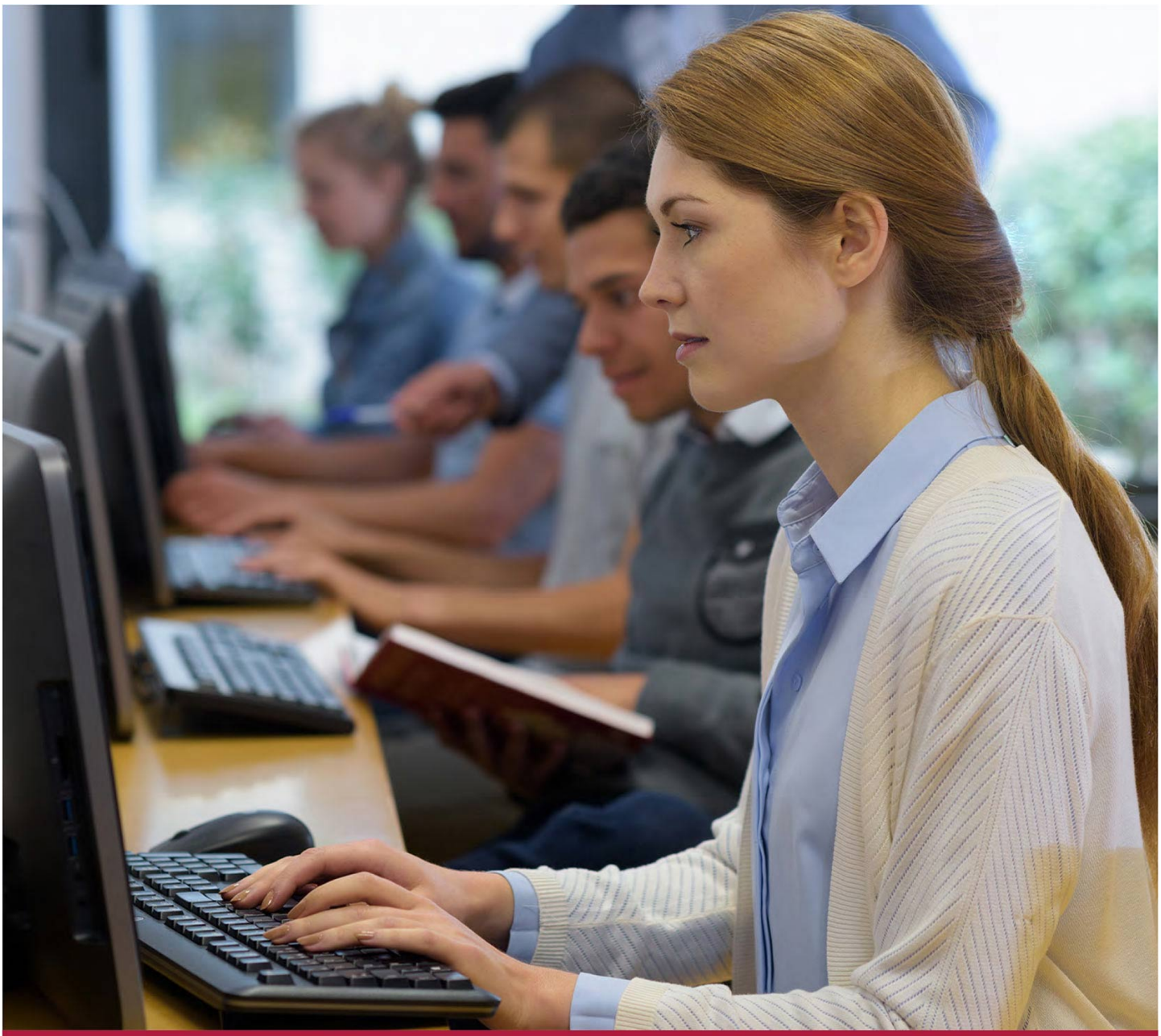
Академия АйТи
a Softline Company



Тестирование на проникновение и анализ безопасности. Базовый уровень

Код курса: EH1

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

Тестирование на проникновение и анализ безопасности. Базовый уровень

Код курса: EH1

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

О курсе

Пентест - метод оценки безопасности компьютерных систем или сетей средствами моделирования атаки злоумышленника. В ходе теста на проникновение специалист действует как настоящий хакер: находит уязвимые места, «проходит» их и получает доступ к нужной информации. В рамках курса рассматриваются шаги, используемые для взлома и защиты от него в рамках различных технологий и инструментов, применяемых PEN-тестерами (аудиторами безопасности), также слушатели получают представление о разных способах и методах атак на корпоративные сети и другие информационные ресурсы.

Подробная информация

Профиль аудитории:

- Квалифицированные специалисты, желающие понять суть хакинга компьютерных систем и мер по защите от вторжений,
- Специалисты в области информационных технологий, желающие улучшить свои знания и навыки в области безопасности компьютерных сетей,
- Системные администраторы, администраторы безопасности, сетевые инженеры и аудиторы ИБ.

Предварительные требования:

- Навыки системного администрирования
- Навыки работы с командной строкой
- Понимание основ информационной безопасности

По окончании курса слушатели смогут:

- Проводить тестирование на проникновение
- Минимизировать риски незащищённости цифровых систем
- Обнаруживать и эксплуатировать уязвимости систем
- Отражать кибератаки и поддерживать безопасность IT-систем
- Прогнозировать риски

- Тестировать уровень защиты ИС
- Готовить отчетность по результатам проверки

Программа курса

Вводный модуль

- Компьютерные сети и основы их защиты

Модуль 1 «Введение в специальность»

- Введение в специальность
- Управление сетевыми рисками и уязвимостями
- Что такое VLAN и Trunk. Как они работают и для чего созданы

Модуль 2 «Арсенал злоумышленников»

- Доступные мишени
- Четыре этапа теста на проникновение в сеть
- Защита информации
- Источники уязвимостей в ПО
- Фазы атаки

Модуль 3 «Сбор информации»

- OSINT (open-source intelligence), разведка на основе открытых данных
- Процесс поиска по открытым данным
- Google hacking. Продвинутые операторы. Методы защиты от Google Dorking
- Руководство по подготовке специалиста по тестированию на проникновение
- Metasploitable 2. Руководство по использованию уязвимостей
- Операторы и параметры поиска Google

Модуль 4 «Социальная инженерия»

- Методы социальной инженерии
- Обратная социальная инженерия
- Противодействие социальной инженерии

Модуль 5 «Сканирование»

- Цели сканирования сети
- Методы сканирования
- Определение топологии сети
- Определение доступных хостов и получение списка сервисов для каждого из них
- Определение операционной системы для каждого из доступных узлов сети
- Поиск потенциально уязвимых сервисов
- Противодействие сканированию
- Использование TOR
- Другие техники туннелирования

- Как попасть в «Даркнет»
- Путешествие по даркнету

Модуль 6 «Перечисление»

- Перечисление (enumeration). Шаги для компрометации системы
- Основы NetBIOS
- Инструменты командной строки.
- SNMP-перечисление
- Обнаружение хостов. Использование Cain
- Контрмеры

Модуль 7 «Эксплойты и методы защиты от них»

- Эксплуатация уязвимостей и получение доступа
- Защита на уровне ядра системы
- Защита на уровне ядра ОС Linux Файл

Модуль 8 «Отказ в обслуживании»

- Отказ в обслуживании DoS и DDoS
- Контрмеры
- Примеры уязвимостей. Решения по их устранению

Модуль 9 «Вредоносное ПО (Malware)»

- Вредоносное ПО (Malware)
- О создании Payload для разных платформ с помощью MSFVenom

Модуль 10 «Снифферы»

- Цели применения снифферов
- Протоколы, уязвимые для прослушивания
- Противодействие прослушиванию
- Использование сниффера Wireshark

Модуль 11 «Перехват сеанса»

- Атака «Человек посередине»
- Spoofing. Их сравнение
- Захват сеанса. Перехват сеанса
- Противодействие перехвату
- Принципы, лежащие в основе перехвата сеанса
- Демонстрация атак с использованием перехвата сеанса

Модуль 12 «Атаки с использованием Web-уязвимостей»

- XSS (межсайтовый скриптинг). BB-коды (Bulletin Board)
- XSS и HTML. XSS и UTF-7

Модуль 13 «Криптография»

- История создания. Концепции.
- Типы шифров. Методы шифрования.
- Типы симметричных и ассиметричных систем.
- Целостность сообщения. Инфраструктура открытых ключей. Управление ключами.
- Канальное и сквозное шифрование. Безопасность в сети Интернет. Атаки
- Как устроена машина "Энигма"

Модуль 14 «Хакинг беспроводных сетей»

- Защита беспроводной сети
- Взломать WPA-WPA2 с помощью Hashcat
- Взломать Wi-Fi за 10 часов
- Защита беспроводной сети
- Простой способ взлома Wi-Fi-сетей

Модуль 15 «Обход IDS и Honeypot»

- Обход IDS и Honeypot
- Установка Snort и его настройка на выявление нужных видов трафика.

Посмотреть расписание курса и записаться на обучение

Обращайтесь по любым вопросам
к менеджерам Академии АйТи

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