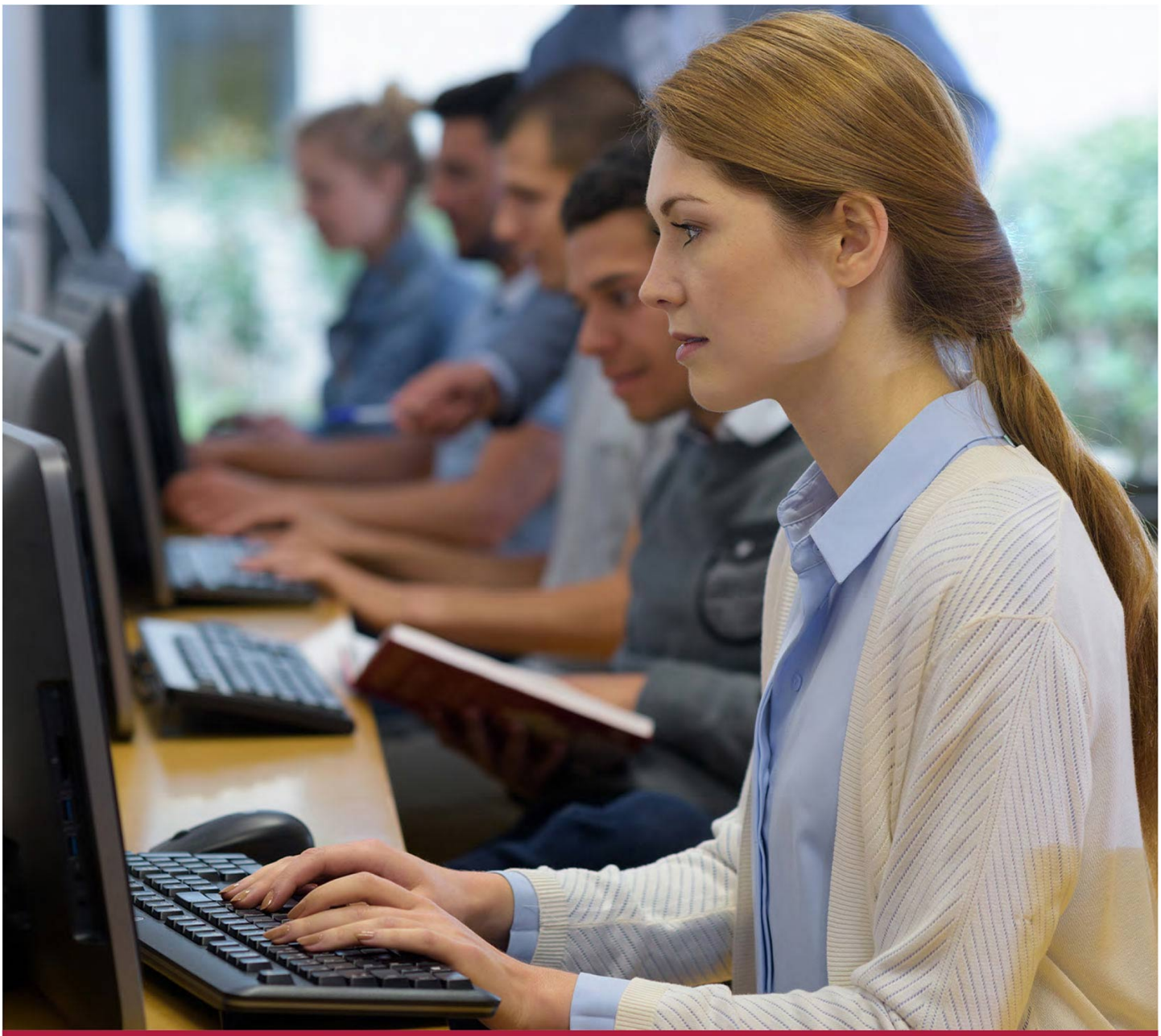
Академия АйТи
a Softline Company



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

Успешное окончание курса позволит специалистам:

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

Необходимая подготовка

Навыки системного администрирования

Навыки работы с командной строкой

Понимание основ информационной безопасности

Цель курса

Формирование знаний и навыков, необходимых для проведения тестирования на проникновение и анализа безопасности

Программа курса

Модуль 1. Введение

Компетенции аудитора безопасности

Виды хакерской активности

Эволюция хакинга

Что атакуют?

Модуль 2. Сбор информации

Утечки

Поиск через сервисы Whois

Сбор данных через DNS

Использование расширенного поиска Google

Противодействие сбору данных

Лабораторная работа: Утечки

Практическое задание: Сбор данных о человеке из открытых источников

Семинар: Противодействие сбору данных

Модуль 3. Социальная инженерия

Методы социальной инженерии

Обратная социальная инженерия

Противодействие социальной инженерии

Семинар: Методы социальной инженерии

Модуль 4. 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

Лабораторная работа: Сканирование

Модуль 5. Перечисление

DNS zone transfer

SNMP

Пользователи Windows

Группы Windows

Противодействие перечислению

Модуль 6. Переполнение буфера

Stack-based Buffer Overflow

Heap-Based Buffer Overflow

Overflow using Format String

Противодействие переполнению буфера

DEP (Data Execution Preventer)

ASLR (Address Space Layout Randomization)

PAX + GRSecurity

Лабораторная работа: Переполнение буфера

Модуль 7. Отказ в обслуживании (DoS и DDoS)

Цель DoS-атаки

Как проводится DDoS-атака

Ботнеты

Признаки DoS-атаки

Обнаружение DoS-атак

Противодействие DDoS/DoS-атакам

Противодействие ботнетам

Модуль 8. Вирусы и черви

Признаки вирусной атаки

Полиморфные вирусы

Противодействие вирусам

Модуль 9. Трояны и бэкдоры

Проявления активности троянов

Определение троянов

Противодействие троянам

1

Модуль 10. Снифферы

Цели применения снифферов

Протоколы, уязвимые для прослушивания

Противодействие прослушиванию

Лабораторная работа: Снифферы

Лабораторная работа: Протоколы, уязвимые для прослушивания

Модуль 11. Перехват сеанса

Атака «Человек посередине»

Hijacking

Spoofing

Сравнение Hijacking и Spoofing

Захват сеанса

Противодействие перехвату

Модуль 12. SQL-инъекция

Как работают web-приложения

SQL-инъекция

Тестирование защиты от SQL-инъекций

Лабораторная работа: SQL-инъекция

Модуль 13. Криптография

Стандарты шифрования

Симметричные криптоалгоритмы

Ассиметричные шифры

Криптографические хэш-функции

Инфраструктура открытых ключей (PKI)

SSL/TLS

SSH

ЭЦП

Взлом шифрования

Модуль 14. Хакинг системы

«Домашняя работа» перед взломом

Проникновение в корпоративную сеть

Методы взлома паролей

Прослушивание сессии

Противодействие взлому

Лабораторная работа: Атака по словарю и перебором

Модуль 15. Хакинг web-серверов

Особенности web-серверов

Использование сообщений об ошибках

Эксплойты

Атаки на стороне клиента

Защита web-серверов

Лабораторная работа: Эксплойты

Модуль 16. Хакинг web-приложений

Специфика web-приложений

Межсайтовый скриптинг

Использование обработчиков ошибок

Некриптостойкое хранение

Управление сессией и аутентификацией

Атаки на web-сервисы

Взлом Web App

Анализ уязвимостей web-приложений

Защита web-приложений

Модуль 17. Хакинг беспроводных сетей

Стандарты беспроводной связи

Типы шифрования беспроводных соединений

Прослушивание IP-адресов

Противодействие взлому беспроводных сетей

Модуль 18. Обход IDS и Honeypot

Система обнаружения вторжений (IDS)

Определение типа брандмауэра

Техники обхода брандмауэров

Обход брандмауэра через Proxy

Honeypot

Модуль 19. Тестирование на проникновение

Оценка безопасности и уязвимостей

Тестирование на проникновение

Порядок тестирования

Методы тестирования

Что тестируется

Тестирование web-приложений

Лабораторная работа: Тестирование на проникновение

Посмотреть расписание курса и записаться на обучение

Обращайтесь по любым вопросам
к менеджерам Академии АйТи

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