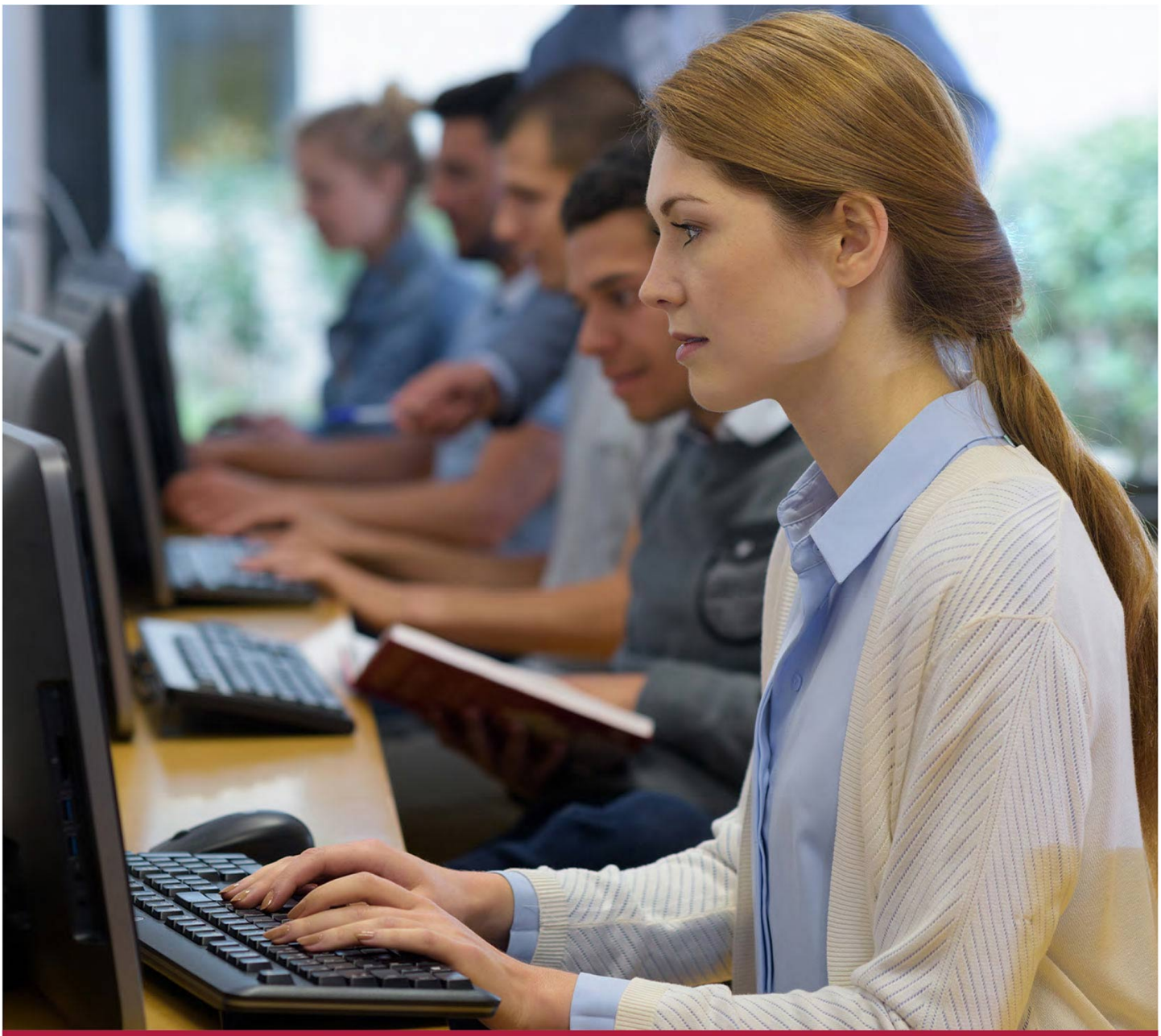
Академия АйТи
a Softline Company



Пентестер: этичный хакинг и анализ систем безопасности

Код курса: pentester

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

Пентестер: этичный хакинг и анализ систем безопасности

Код курса: pentester

Длительность	220 ак. часов
Формат	
Разработчик курса	Академия АйТи
Тип	Учебный курс
Способ обучения	Под руководством тренера

О курсе

Пентестер – это специалист по кибербезопасности, который моделирует хакерские атаки, проводит глобальный аудит безопасности компьютерных систем и сетей ищет в них уязвимости. Главная задача пентестера – пройти уязвимые места, получить доступ к закрытой информации, проанализировать каждый смоделированный шаг «злоумышленника» и минимизировать риски взлома цифровых систем. Пентестер – это белый хакер, одна из самых востребованных профессий в области информационной безопасности. Чтобы защититься от преступников, компании активно ищут специалистов по компьютерной кибербезопасности. В рамках курса Вы получите практические навыки в технологиях и инструментах, применяемых PEN-тестерами (аудиторами безопасности), а также представление о разных способах и методах атак на корпоративные сети и другие информационные ресурсы.

Подробная информация

Цель:

Формирование знаний и навыков, необходимых для проведения тестирования на проникновение и анализа безопасности, повышение экспертности и ценности как специалиста по борьбе с киберугрозами.

Целевая аудитория:

- 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,
- тестировщики digital-систем, специалисты по кибербезопасности.

О курсе:

Задачами курса является подготовка специалистов по кибербезопасности. Каждое четвертое преступление в России происходит с использованием высоких технологий, за год в России зафиксировано 510 тысяч IT-преступлений. Киберпреступники используют искусственный интеллект

для создания фишинговых сайтов, для генерации теста, который может выглядеть как сообщение от конкретной компании или организации. 98% мировых компаний признают, что их системы безопасности не отвечают потребностям в полной мере.

Законодательство требует обеспечивать сохранность данных клиентов. На рынке труда очевиден дефицит специалистов.

Курс поможет прокачать знания и навыки в борьбе с кибератаками, научит находить и предотвращать уязвимые места в различных ИТ-системах.

Программа курса состоит из 20 модулей, полный учебный цикл включает лекционные и лабораторные работы. Освоение программы завершается обязательной ИТОГОВОЙ РАБОТОЙ НА КИБЕРПОЛИГОНЕ.

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

Модуль 1. Введение в специальность

- Компетенции аудитора безопасности
- Методология тестирования на проникновение

Модуль 2. Арсенал злоумышленников

- Знакомство с инструментами злоумышленников
- Источники уязвимостей в программном обеспечении
- Схема проникновения в корпоративную сеть
- Защита информации
- Средства и методы выполнения атак
- Методы поиска уязвимостей к атакам
- OWASP (Открытый проект по обеспечению безопасности веб-приложений)
- OWASP Top 10 2021
- OWASP Mobile Top 10 2016
- CWE Top 25 2022 (Common Weakness Enumeration)

Модуль 3. Сбор информации

- Утечки данных
- Использование методов OSINT
- **Лабораторная работа:** Поиск через сервисы Whois
- **Лабораторная работа:** Сбор данных через DNS
- **Лабораторная работа:** Использование Maltego
- Использование расширенного поиска Google
- **Практическое задание:** Сбор данных о человеке из открытых источников
- Противодействие сбору данных

Модуль 4. Социальная инженерия

- Методы социальной инженерии
- Обратная социальная инженерия
- Противодействие социальной инженерии
- Семинар: Применение социальной инженерии

Модуль 5. Сканирование

- Цели сканирования сети
- Методы сканирования
- Определение топологии сети
- Определение доступных хостов и получение списка сервисов для каждого из них
- **Лабораторная работа:** Определение доступных хостов
- **Лабораторная работа:** Получение списка сервисов для найденных хостов
- **Лабораторная работа:** Определение операционной системы для каждого из доступных узлов сети
- **Лабораторная работа:** Автоматизированный поиск потенциально уязвимых сервисов
- **Лабораторная работа:** Внедрение бэкдора в качестве системной службы
- **Лабораторная работа:** Ручной поиск внедренных бэкдоров
- Противодействие сканированию
- Техники туннелирования
- **Лабораторная работа:** Использование TOR

Модуль 6. Перечисление

- Цели и задачи перечисления
- Протоколы: DNS, SNMP, NetBIOS, SMB/CIFS, LDAP и пр.
- **Лабораторная работа:** DNS zone transfer
- **Лабораторная работа:** Применение enum4linux
- **Лабораторная работа:** Использование Active Directory Explorer
- Противодействие перечислению

Модуль 7. Эксплойты и методы защиты от них

- Stack-based Buffer Overflow
- Heap-Based Buffer Overflow
- Overflow using Format String
- **Лабораторная работа:** Переполнение буфера

- Противодействие переполнению буфера
- Технологии защиты от эксплойтов в ядре Windows
- **Лабораторная работа:** Настройка EMET
- Защита от эксплойтов на уровне ядра Linux
    - Обзор патчей GRSecurity/PAX и Linux Hardened
    - **Лабораторная работа:** Сборка ядра с патчем GRSecurity/PAX
    - **Лабораторная работа:** Использование ASTRA Linux с hardened-ядром
    - Обзор модулей ядра LKRG и Tyton
    - **Лабораторная работа:** Использование модуля ядра LKRG
    - **Лабораторная работа:** Применение модуля ядра Tyton

Модуль 8. Отказ в обслуживании (DoS и DDoS)

- Цель DoS-атаки
- Как проводится DDoS-атака
- **Лабораторная работа:** Проведение DoS-атаки с использованием протоколов: UDP, TCP и HTTP
- Ботнеты
- Признаки DoS-атаки
- Обнаружение DoS-атак
- **Лабораторная работа:** Обнаружение DoS-атаки
- Противодействие DDoS/DoS-атакам
- Противодействие ботнетам

Модуль 9. Вредоносное ПО (Malware)

- Классификация вредоносного ПО: вирусы, черви, трояны, бэкдоры и пр.
- Способы применения вредоносного ПО
- Remote Access Trojans (RAT)
- **Лабораторная работа:** Подготовка, установка и использование Remote Access Trojan
- Backdoors и Rootkits
- **Лабораторная работа:** Подготовка backdoor средствами msfvenom
- **Лабораторная работа:** Установка backdoor’а и его применение
- Вирусы и черви
- Классификация вирусов
- **Лабораторная работа:** Практическая проверка эффективности антивирусных сканеров
- Противодействие вирусам и червям

Модуль 10. Снифферы

- Цели применения снифферов
- Протоколы, уязвимые для прослушивания
- Противодействие прослушиванию
- **Лабораторная работа:** Использование сниффера Wireshark
- Протоколы, уязвимые для прослушивания

Модуль 11. Перехват сеанса

- Атака «Человек посередине»
- Hijacking
- Spoofing

- Сравнение Hijacking и Spoofing
- **Лабораторная работа:** Перехват сеанса
- Противодействие перехвату

Модуль 12. Атаки с использованием Web-уязвимостей

- Как работают web-приложения
- **Лабораторная работа:** Использование утилит: whatweb, nikto, dirb и OWASP ZAP
- Атаки на клиентов: HTML-инъекции, XSS, iFrame-инъекции и пр.
- **Лабораторная работа:** Тестирование различных типов HTML-инъекций
- **Лабораторная работа:** Тестирование на уязвимость к XSS
- **Лабораторная работа:** Тестирование на возможность iFrame-инъекций
- Атаки на серверную часть: OS Command Injection, PHP Code Injection, Server Side Includes (SSI), SQL-инъекции
- **Лабораторная работа:** Тестирование на возможность OS Command Injection
- **Лабораторная работа:** Тестирование защиты от PHP Code Injection
- **Лабораторная работа:** Тестирование на уязвимость к Server Side Includes (SSI)
- **Лабораторная работа:** Тестирование на уязвимость к SQL-инъекции

Модуль 13. Криптография

- Введение и история криптографии
- **Демонстрация:** Работа шифровальной машины Энигма
- **Лабораторная работа:** Знакомство с инструментом CryptTool (на примере шифра Вернама)
- Симметричные криптоалгоритмы
- Потоковые и блочные криптоалгоритмы
- **Демонстрация:** Визуализация RC4
- **Демонстрация:** Визуализация DES
- **Демонстрация:** Визуализация AES
- **Лабораторная работа:** Шифрование AES с неявным преобразованием
- **Лабораторная работа:** Использование VeraCrypt для создания криптоконтейнера
- Ассиметричные шифры
- **Демонстрация:** Алгоритм безопасного обмена ключами Диффи-Хеллмана
- **Демонстрация:** Визуализация RSA
- Криптографические хэш-функции
- **Демонстрация:** Визуализация SHA-256
- Инфраструктура открытых ключей (PKI)
- Протокол SSH
- Логика работы ЭЦП
- Взлом шифрования
- Требования нормативной документации по криптографической защите информации
    - ФЗ №63 Об электронной подписи
    - Приказ ФАПСИ №152
    - Приказ ФСБ №66 (ПКЗ-2005)

Модуль 14. Хакинг системы

- «Домашняя работа» перед взломом
- Проникновение в корпоративную сеть

- **Лабораторная работа:** Построение SSH-туннеля для обхода межсетевого экрана
- **Лабораторная работа:** Взлом сетевого узла с использованием существующих уязвимостей
- Методы взлома паролей
- **Лабораторная работа:** Атака по словарю с помощью hydra и medusa
- **Лабораторная работа:** Использование утилит hashcat, john the ripper и ophcrack для взлома хэшей паролей
- **Лабораторная работа:** Использование online-ресурсов для взлома хэшей паролей
- Прослушивание перехват ввода пароля пользователя
- **Лабораторная работа:** Использование возможностей meterpreter для перехвата ввода пароля пользователя
- Противодействие взлому паролей

Модуль 15. Хакинг с использованием web-уязвимостей

- Специфика web-приложений
- Использование сообщений об ошибках
- Веб-уязвимости и их использование
- Управление сессией и аутентификацией
- **Лабораторная работа:** Взлом сетевого узла с использованием Web-уязвимостей
- Защита web-приложений

Модуль 16. Анализ безопасности узла на примере metasploitable3

- **Лабораторная работа:** Определение ip-адреса и открытых портов
- **Лабораторная работа:** Определение сервисов и их версий
- **Лабораторная работа:** Поиск уязвимостей средствами nmap и nessus
- **Лабораторная работа:** Использование searchsploit и/или metasploit framework
- **Лабораторная работа:** Подбор паролей средствами Hydra/Medusa
- **Лабораторная работа:** Ручной поиск эксплойтов
- **Практика:** Подготовка отчета по итогам анализа безопасности

Модуль 17. Практикум по взлому

- **Лабораторная работа:** Взлом виртуальной машины BeeBug
- **Лабораторная работа:** Взлом виртуальной машины Lab26
- **Лабораторная работа:** Взлом виртуальной машины Hackxor2
- **Лабораторная работа:** Взлом виртуальной машины DoNot5Top
- **Лабораторная работа:** Взлом виртуальной машины Kioptrix4
- **Лабораторная работа:** Capture The Flags (необходимо собрать не менее 30 флагов)

Модуль 18. Хакинг беспроводных сетей

- Стандарты беспроводной связи
- Типы шифрования беспроводных соединений
- Прослушивание IP-адресов
- Методология взлома беспроводных сетей
- Противодействие взлому беспроводных сетей

Модуль 19. Обход IDS и Honeypot

- Система обнаружения вторжений (IDS)
- Определение типа брандмауэра
- **Лабораторная работа:** Определение брандмауэра
- Техники обхода брандмауэров
- **Лабораторная работа:** Использование техник обхода брандмауэра
- Возможности Honeypot по выявлению сканирования
- **Лабораторная работа:** Выявление сканирования средствами Honeypot
- **Лабораторная работа:** Использование техники скрытого сканирования

Модуль 20. Дополнительные механизмы защиты

- Защитные механизмы в Windows
  - Обзор локальных политик безопасности
  - Шифрование дисков BitLocker
  - **Лабораторная работа:** Использование BitLocker
- Защитные механизмы Linux
  - Основные возможности SELinux
  - **Лабораторная работа:** Применение SELinux для защиты Web-сервера
  - Защита приложений средствами AppArmor
  - **Лабораторная работа:** Создание профиля AppArmor
  - Шифрование LUKS
  - **Лабораторная работа:** Создание криптоконтейнера средствами LUKS

ИТОГОВАЯ РАБОТА НА КИБЕРПОЛИГОНЕ

Посмотреть расписание курса и записаться на обучение

Обращайтесь по любым вопросам
к менеджерам Академии АйТи

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