Бауманский учебный центр «Специалист»

Программа курса Тестирование на проникновение хакера и анализ безопасности

Код курса: **CEH2**

Тема	Ак. часов
Модуль 1. Введение в тестирование на проникновение • Концепции тестирования на проникновение • Методология LPT • Руководства и рекомендации по проведению тестирования	**2**
Модуль 2. Область тестирования на проникновение • Подготовка к тестированию на проникновение • Запрос коммерческого предложения • Установление правил проведения тестирования на проникновение • Установление каналов связи • Временные рамки • Решение юридических вопросов • **Лабораторная работа.** Подготовка к тестированию на проникновение в сеть учебной лаборатории	**2**
Модуль 3. Методология разведки OSINT • Что такое сбор информации • Чек-лист по сбору информации • Автоматизация процесса сбора информации с помощью инструментов • **Лабораторная работа.** Использование средств для сбора информации	**1**
Модуль 4. Социальная инженерия • Концепции социальной инженерии • Навыки, необходимые для проведения социальной инженерии • Социальная инженерия посредством E-Mail • Вектор телефонной атаки • Вектор физической атаки • Подготовка отчета о проведенной атаке социальной инженерии • **Лабораторная работа.** Подготовка фишинговой кампании	**2**
Модуль 5. Внешнее тестирование на проникновение • Тестирование и анализ внешних вторжений • Обнаружение систем и сервисов • Атака на системы извне • **Лабораторная работа.** Выполнение внешнего тестирования	**1**
Модуль 6. Внутреннее тестирование на проникновение • Тестирование и анализ внутренних вторжений • Сетевое сканирование • Сетевое перечисление • Анализ уязвимостей • Нахождение эксплойтов • Эксплуатация систем Windows • Эксплуатация систем Linux • Методы эксплуатации внутренней сети • Продвинутые техники эксплуатации • **Лабораторная работа.** Выполнение внутреннего тестирования	**2**

Модуль 7. Тестирование на проникновение через периметр • Обход межсетевых экранов • Обход систем обнаружения вторжений • Оценка безопасности маршрутизаторов • Оценка безопасности коммутаторов • **Лабораторная работа.** Обход запрещающих правил фаерволла	**2**
Модуль 8. Тестирование веб-приложений • Обнаружение содержимого веб-приложения • Обнаружение скрытого содержимого • Сканирование веб-уязвимостей • Тест на внедрение SQL-кода • Тест на уязвимости XSS • Тест на уязвимости слабой криптографии • Тесты на уязвимости неправильной конфигурации безопасности • Тест на атаку на стороне клиента • Атаки на аутентификацию и авторизацию • Атаки на управление сеансом • Тест на безопасность веб-служб • Тест на недостатки бизнес-логики • Тест на уязвимости веб-сервера • Тест на уязвимости толстых клиентов • Тестирование Wordpress • **Лабораторная работа.** Выявление и эксплуатация уязвимостей веб-приложения	**1**
Модуль 9. Тестирование на проникновение в беспроводные сети • Тестирование беспроводных сетей • Тестирование RFID • Тестирование NFC • **Лабораторная работа.** Исследование методов взлома беспроводных сетей.	**1**
Модуль 10. Тестирование на проникновение в Интернет Вещей (IoT) • Тестирование IoT ◦ Введение в тестирование IoT ◦ Чек-лист по проведению тестирования IoT ◦ Инструмент для выполнения тестирования IoT ◦ Рекомендации по защите IoT • **Лабораторная работа.** Исследование методов взлома Интернета Вещей.	**1**
Модуль 11. Тестирование на проникновение операционных технологий (OT) • Концепции OT и SCADA • Шина Modbus • Тестирование на проникновение ICS и SCADA • **Лабораторная работа.** Исследование безопасности операционных технологий	**1**
Модуль 12. Тестирование на проникновение облачных вычислений • Тестирование на проникновение в облаке • Область тестирования на проникновение в облаке • Специфика тестирования AWS • Специфика тестирования Azure • Специфика тестирования Google Cloud • **Лабораторная работа.** Исследование безопасности облачных технологий	**1**

Модуль 13. Бинарная эксплуатация • Концепции двоичного кодирования • Бинарный анализ • Бинарный анализ архитектуры x64 • Методология бинарного анализа • Обход запрета на выполнение в стеке • Возвратно-ориентированное программирование • **Лабораторная работа.** Атака на переполнение буфера в уязвимом приложении	**2**
Модуль 14. Отчеты и действия после тестирования на проникновение • Результаты тестирования и заключение • Написание отчета по тестированию на проникновение • Формат отчета по тестированию • Анализ результатов • Хранение отчета	**1**
Модуль 15. Финальная Лабораторная работа. Выполнение тестирования на проникновение в сеть учебной лаборатории • Планирование проведения тестирования на проникновение • Выполнение тестирования на проникновение • Анализ результатов • Написание отчета	**20**
Аудиторная нагрузка в классе с преподавателем	**40 ак.ч. + 40 ак.ч. самостоятельно**

По окончании обучения на курсе проводится итоговая аттестация. Аттестация проводится в виде теста на последнем занятии или на основании оценок практических работ, выполняемых во время обучения на курсе.

Контакты центра

Для частных лиц
+7 (495) 232-32-16

Для организаций
+7 (495) 780-48-44

E-mail
info@specialist.ru