



KaliLinux «Тестирование безопасности систем».

Код курса: SLIT-978

KaliLinux «Тестирование безопасности систем».

Код курса: SLIT-978

Длительность	32 ак. часа
Формат	Очно; Дистанционно
Разработчик курса	Softline
Тип	Учебный курс
Способ обучения	Под руководством тренера

О курсе

Настоящая программа предназначена для подготовки специалистов, отвечающих за обеспечение защиты информации в телекоммуникационных системах и сетях и администрирование программного обеспечения, входящего в состав KaliLinux. Цель курса – получить знания и навыки, необходимые для успешного выявления и устранения проблем безопасности в информационных системах предприятия. Курс посвящен методикам проведения тестирования на проникновение в контексте углубленного анализа безопасности компьютерных сетей и информационных систем. В курсе представлены подробные материалы по работе информационных систем и сетей. Описаны последовательности многочисленных атак и предложены рекомендации по укреплению защищенности информационных систем и сетей.

Подробная информация

Целевая аудитория:

- Системные администраторы безопасности, инженеры и аудиторы, работающие или предполагающие работать на средних и крупных предприятиях, вплоть до организаций корпоративного масштаба.
- К основной целевой аудитории данного курса также относятся квалифицированные специалисты в области информационных технологий, включая администраторов предприятий, желающих улучшить свои знания и навыки в области безопасности компьютерных сетей.
- К дополнительной целевой аудитории также относятся квалифицированные специалисты, желающие понять суть хакинга компьютерных систем и мер по защите от вторжений.

Требования к предварительной подготовке:

- базовая подготовка в области информационных технологий и информационной безопасности, в том числе:
- базовые навыки администрирования ОС Windows, Linux;
- знание принципов организации межсетевого взаимодействия, принципов организации и структуры кадров основных протоколов стека TCP/IP.

По окончании курса слушатели смогут:

- Интегрировать полученный опыт на своих предприятиях
- Проводить анализ и выполнять последовательное тестирование всех способов проникновения в компьютерные системы

Программа курса

Модуль 1: Введение в сетевую безопасность.

- Хакеры и инструменты взлома.
- Процесс взлома и актуальные технологии.
- События и статистика по последним атакам.
- Снижение вероятности угроз и разработки оценки.

Модуль 2: Сниффинг сети.

- Значение сниффинга сети.
- Определение операционной системы и службы.
- Форматы вывода.

Модуль 3: Взлом пароля Wi-Fi.

- Методы и требования.
- Инъекция пакета.
- Инструменты взлома Wi-Fi.
- Квитирование TCP.

Модуль 4: Трояны.

- Трояны удаленного доступа. (RAT).
- Пути внедрения.
- Защита.

Модуль 5: Veil Framework.

- Veil-Evasion, Veil-Pillage и Veil-PowerTools.
- Соккрытие атак.
- Антивирусная защита.

Модуль 6: Набор инструментов социальной инженерии и использование браузера.

- Веб-инъекции.
- Атаки XSS.
- Использование браузера с BeEF.

Модуль 7: Продвинутое сетевые атаки.

- Атака MITM.
- Инструменты для атак MITM.
- Kali Linux.

Модуль 8: Передача и взлом хэша.

- Хэш (Hash).
- Криптографические функции хэширования.
- Способы взлома.
- Защита хэша.

Модуль 9: Инъекции SQL.

- Инъекции SQL.
- Защита против инъекций SQL.
- Передача аутентификации.
- Поиск угроз.

Модуль 10: Scapy.

- Создание пакета.
- Тройное квитиование TCP.
- Деформированные пакеты.
- Сканирование ACK.
- Сканирование портов TCP.

Модуль 11: Эксплоиты веб-приложений.

- Эксплоиты веб-приложений.
- Инструменты тестирования проникновения веб-приложений.
- Autorpwn.
- Browser Exploitation Framework Project.

Модуль 12: Злой двойник и спуфинг.

- Злой двойник (Evil Twins).
- Спуфинг адресов.
- Спуфинг DNS.
- Обнаружение злого двойника (Evil Twins).

Модуль 13: Устройства для инъекций.

- USB.
- Гадкий утенок (Rubber Ducky).
- Отключение портов.
- KeyGrabber.
- Glitch.

Модуль 14: Интернет вещей (IoT).

- Интернет вещей (IoT).
- IoT и ботнеты (Botnets).

Модуль 15: Системы обнаружения.

- IDS.
- IPS.
- Информация о безопасности и управление событиями (SIEM).
- Splunk.
- Snort.

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

Обращайтесь по любым вопросам
к менеджерам Учебного центра Softline

8 (800) 505-05-07 | edusales@softline.com

Ждём вас на занятиях в Учебном центре Softline!



Почему Учебный центр Softline?

Лидер на рынке корпоративного обучения.

Более 300 тысяч подготовленных IT-специалистов.

Гибкий индивидуальный подход в обучении, скидки и акции.

Широкая сеть представительств в крупнейших городах РФ и СНГ; дистанционный формат обучение на вашей территории или в арендованном классе в любой точке мира.

Высокотехнологичное оборудование

Более **18 лет** опыта работы

Международные сертификаты для IT-специалистов и пользователей в Центрах тестирования

Сертифицированные тренеры с богатым практическим опытом работы

Авторизации от мировых производителей ПО (Microsoft, Cisco, VMware, Citrix, Лаборатория Касперского, Oracle, Autodesk, Код безопасности и других).

Разработка курсов и тестов под заказ, внедрение корпоративных систем обучения.

Подробнее об Учебном центре Softline

Вы можете узнать из [профайла](#).