ТОО «INTELLA»
010000, г. Астана, р-н Есиль
ул. Д. Кунаева, 29/1, оф.1903
БИН 080840000052

+ 7(7172) 28 00 82
+7(727) 355 02 34
info@intella.kz
www.intella.pro

ПРЕДЛОЖЕНИЕ

На обучающий тренинг:

СЕН. Этичный хакинг и тестирование на проникновение v.10

- **Домен знаний:** Подготовка к сертификации (Exam Prep Course)
- **Преподаватель**: сертифицированный тренер АИС г.Москва
- **Статус:** авторизованный курс АИС г.Москва
- **Длительность обучения** 5 дней (46 ак.часов)
- **Форма обучения** аудиторные занятия с 10.00 до 18.00, обед с 13.00 до 14.00
- **Место проведения** – На базе центра повышения квалификации: «INTELLA»

г.Алматы, ул.Ауэзова, 60 БЦ “Almaty Residense” 6 этаж офис 17а тел. +7 (727) 355 02 34
г.Астана, 010000, г. Астана, р-н Есиль ул. Д. Кунаева, 29/1, оф.1903 тел. +7 (7172) 28 00 82

- **Даты проведения** - ведется набор
- **Расписание –** с 10.00 до 18.00, обед с 13.00 до 14.00.
- **В стоимость включено:** Раздаточный материал (в электронном и печатном виде) Кофе-брейки

Аннотация тренинга

ТОО «INTELLA» предлагает рассмотреть возможность пройти тренгинг: **Подготовка к сертификации СЕН. Этичный хакинг и тестирование на проникновение v.10 EC-Counsil**

Вы получите знания и навыки, необходимые для успешного выявления и устранения проблем безопасности в смешанных компьютерных сетях. Курс посвящен уникальным хакерским техникам и методам взлома в контексте применения оборонительных практик и рекомендаций, изложенных настоящими хакерами. Курс одобрен министерством обороны США и является официальной библией для сотрудников службы безопасности.

В курсе представлены подробные материалы по работе компьютерных систем и сетей. Рассмотрены типичные уязвимости сетевых протоколов, операционных систем и приложений. Описаны последовательности различных видов атак на компьютерные системы и сети, и предложены рекомендации по укреплению защищенности компьютерных систем и сетей.

Цель тренинга

Дать слушателям знания и навыки для формирования системного подхода к обеспечению компьютерной безопасности, научить методам проверки безопасности различных узлов компьютерной сети и познакомить слушателей с инструментарием злоумышленников, с их преимуществами и ограничениями.

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.

По окончании тренинга слушатели смогут:

- Понимать взаимосвязь компонентов безопасности сети, сферу ответственности и влияния каждого из узлов;
- Знать и управлять уязвимыми местами сети;
- Самостоятельно обнаруживать уязвимости;
- Работать с инструментами взлома сетей и систем;
- Знать хакерские уловки для проникновения в системы и сети;
- Проводить тестирование любых компонентов сети на предмет взлома;
- Классифицировать рабочие станции по степени риска проведения атаки;
- Понимать ход мыслей злоумышленника;
- Оценить масштаб потенциально возможных атак;
- Противодействовать несанкционированному сбору информации о сети организации;
- Понимать стратегию злоумышленника;
- Оценивать защищенность платформ виртуализации и облачных вычислений;
- Определять атаку на основе социальной инженерии;
- Изучить методы взлома беспроводной сети;
- Определить наиболее уязвимые места мобильных платформ;
- Противодействовать криптографическим атакам;
- Понимать процесс вторжения в систему;
- Проводить аудит систем безопасности;
- Противодействовать вторжению.
-

Сертификационные экзамены

Тренинг помогает подготовиться к следующим сертификационным экзаменам:

- **312-50**: Certified Ethical Hacker v10

Оплата сертификационного экзамена не входит в стоимость тренинга

Необходимая подготовка

Для эффективного обучения на тренинге слушатели должны обладать следующими знаниями и навыками:

- Опыт работы с клиентским и серверными ОС;
- Понимание работы сети и сетевых устройств;
- Понимание базовых концепций безопасности.

Рекомендуемая подготовка:

Английский язык для IT специалистов (pre — intermediate) или знание технического английского языка.

Контакты:

Асель Муханмеджанова (Астана) + 7 (7172) 28-00-82
Татьяна Бережная tb@intella.kz (Алматы) +7 (727) 355 02 34
Диана Фролова tb@intella.kz (Алматы) +7 (777) 552 47 22

EPC04 Тренинг для подготовки к экзамену Certified Ethical Hacker (CEH)
CEH. Этичный хакинг и тестирование на проникновение v.10

Модуль 1. Введение в этичный хакинг
- Основные термины безопасности
- Угрозы информационной безопасности и векторы атак
- Концепции хакинга
- Этапы хакинга
- Типы хакерских атак
- Контроль информационной безопасности
- Практическая работа: Изучение концепций и подготовка лаборатории

Модуль 2. Сбор информации
- Концепции рекогносцировки
- Угрозы неавторизованного сбора информации
- Методологии сбора информации
- Инструменты сбора информации
- Меры противодействия сбору информации
- Тестирование на возможность сбора информации
- Практическая работа: Применение техник по сбору информации

Модуль 3. Сканирование
- Что такое сканирование сети
- Типы сканирования
- Методология сканирования
- Техники сканирования открытых портов
- Техника скрытого сканирования
- Инструменты сканирования
- Техники уклонения от систем обнаружения вторжений
- Сбор баннеров
- Сканирование уязвимостей
- Построение сетевых диаграмм уязвимых хостов
- Подготовка прокси
- Техники туннелирования
- Анонимайзеры
- Спуфинг IP адреса и меры противодействия
- Тестирование на возможность сканирования
- Практическая работа: Сканирование компьютеров лаборатории и идентификация сервисов

Модуль 4. Перечисление
- Концепции перечисления
- Техники перечисления
- Перечисление NetBIOS
- Перечисление SNMP
- Перечисление UNIX
- Перечисление LDAP
- Перечисление NTP
- Перечисление SMTP
- Перечисление DNS
- Меры противодействия перечислению
- Тестирование на возможность перечисления

- Практическая работа: Применение техник перечисления

Модуль 5. Хакинг системы

- Архитектура операционной системы
- Слабые точки операционной системы
- Методология хакинга системы
- Последовательность хакинга системы
- Взлом паролей
- Повышение привилегий
- Выполнение приложений
- Скрытие файлов
- Скрытие следов
- Тестирование на проникновение посредством атаки на систему
- Практическая работа: Применение техник по взлому паролей и повышению привилегий в операционных системах

Модуль 6. Трояны и бэкдоры

- Что такое троян
- Как работают трояны
- Типы троянов
- Методы обнаружения троянов
- Меры противодействия троянам
- Анти-троянское ПО
- Тестирование на проникновение с помощью трояна
- Практическая работа: Тестирование работы шелл-трояна, реверсного трояна, скрытого трояна

Модуль 7. Вирусы и черви

- Концепции вирусов и червей
- Работа вируса
- Типы вирусов
- Компьютерные черви
- Отличие червей от вирусов
- Анализ вредоносного ПО
- Меры противодействие вирусам
- Тестирование на проникновение с помощью вируса
- Практическая работа: Изучение вирусов различных типов

Модуль 8. Снифферы

- Концепции сниффинга
- Как работает сниффер?
- Типы сниффинга
- Аппаратные анализаторы протоколов
- SPAN порт
- MAC атаки
- DHCP атаки
- ARP атаки
- Спуфинг атака
- Отравление кэша DNS
- Инструменты сниффинга
- Меры противодействия сниффингу
- Практическая работа: Применение техники активного сниффинга для получения передаваемых по сети данных и подмены запросов

Модуль 9. Социальная инженерия

- Концепции социальной инженерии
- Техники социальной инженерии
- Имперсонация в социальных сетях
- Кража личности
- Меры противодействия социальной инженерии
- Тестирование на проникновение посредством социальной инженерии
- Практическая работа: Применение набора средств социальной инженерии SET из состава BackTrack

Модуль 10. Отказ в обслуживании

- Концепции Denial-of-Service
- Что такое DDoS атака
- Техники DoS/DDoS атак
- Бот сети
- Изучение примера реализация DDoS атаки
- Инструменты проведения DoS атак
- Меры противодействия DoS атакам
- Инструменты защиты от DoS
- Тестирование на подверженность DoS атакам
- Практическая работа: Применение техник проведения DoS атаки для вывода из строя сервисов учебных серверов.

Модуль 11. Перехват сеанса

- Концепции перехвата сеанса
- Ключевые техники перехвата сеанса
- Процесс перехвата сеанса
- Типы перехвата сеанса
- Перехват на прикладном уровне
- Перехват на сетевом уровне
- Инструменты для перехвата сеанса
- Меры противодействия перехвату сеанса
- Тестирование на перехват сеанса
- Практическая работа: Применение техник перехвата сеанса для получения доступа к ресурсам учебных серверов

Модуль 12. Хакинг веб-серверов

- Концепции веб-серверов
- Типы атак на веб-серверы
- Методология атаки на веб-сервер
- Инструменты взлома веб-серверов
- Меры противодействия взлому веб-серверов
- Управление исправлениями
- Повышение безопасности веб-серверов
- Тестирование на возможность взлома веб-сервера

Практическая работа: Дефейс учебного веб-сервера посредством эксплуатации уязвимости с помощью Metasploit Framework

Модуль 13. Хакинг веб-приложени

- Концепции веб-приложений
- Угрозы веб-приложениям
- Методология атаки на веб-приложения
- Инструменты взлома веб-приложений
- Меры противодействия взлому веб-приложений
- Инструменты защиты веб-приложений
- Тестирование на возможность взлома

- Практическая работа: Выполнение отраженной и сохраненной XSS атаки

Модуль 14. SQL инъекции

- Концепции SQL инъекции
- Тестирование на SQL возможность инъекции
- Типы SQL инъекций
- Слепая SQL инъекция
- Методология SQL инъекции
- Примеры применения SQL инъекции
- Средства для выполнения SQL инъекции
- Скрытие SQL инъекции от IDS
- Меры противодействия SQL инъекции
- Практическая работа: Взлом учебного веб-сервера с помощью SQL инъекций

Модуль 15. Хакинг беспроводных сетей

- Концепции беспроводных сетей
- Шифрование в беспроводных сетях
- Угрозы беспроводным сетям
- Методология взлома беспроводных сетей
- Обнаружение беспроводных устройств
- Анализ трафика беспроводных сетей
- Проведение атаки на беспроводную сеть
- Взлом шифрования беспроводных сетей
- Инструменты хакинга беспроводных сетей
- Атаки на Bluetooth
- Меры противодействия атакам на беспроводные сети
- Инструменты защиты беспроводных сетей
- Тестирование на проникновение в беспроводных сетях
- Практическая работа: Нахождение точек доступа, сниффинг, де-аутентификация, взлом ключей WEP, WPA, WPA2 и расшифровывание Wi-Fi трафика

Модуль 16. Хакинг мобильных платформ

- Векторы атаки на мобильные платформы
- Взлом Android OS
- Техники и инструменты получения прав администратора Android
- Взлом iOS
- Техники и инструменты джейлбрейка
- Взлом Windows Phone OS
- Уязвимости Windows Phone 8
- Взлом BlackBerry
- Атаки на телефоны BlackBerry
- Управление мобильными устройствами
- Инструменты и рекомендации по защите мобильных устройств
- Тестирование на проникновение в мобильные платформы
- Практическая работа: Изучение инструментов для проведения атак на мобильные устройства

Модуль 17. Обход систем обнаружения вторжений, фаерволлов и Honey Pot

- Концепции IDS, фаерволлов и Honey Pot
- Системы IDS, фаерволлов и Honey Pot
- Уклонение от IDS
- Обход фаерволлов
- Обнаружение Honey Pot
- Инструменты обхода фаерволлов
- Противодействие обходу систем обнаружения
- Тестирование на проникновения сквозь системы обнаружения вторжений и фаерволлы

- Практическая работа: Изучение возможностей уклонения от систем обнаружения

Модуль 18. Переполнение буфера

- Концепции переполнения буфера
- Методология переполнения буфера
- Примеры переполнения буфера
- Обнаружение переполнения буфера
- Инструменты обнаружения переполнения буфера
- Меры противодействия переполнению буфера
- Инструменты защиты от переполнения буфера
- Тестирование на проникновение с помощью переполнения буфера
- Практическая работа: Создание программы, уязвимой к переполнению буфера и повышение привилегий с использованием переполнения буфера

Модуль 19. Криптография

- Концепции криптографии
- Алгоритмы шифрования
- Криптографические средства
- Инфраструктура открытых ключей
- Шифрование почты
- Шифрование диска
- Инструменты шифрования диска
- Криптографические атаки
- Средства криптоанализа
- Практическая работа: Изучение алгоритмов шифрования и средств стеганографии

Модуль 20. Тестирование на проникновение

- Концепции тестирования на проникновение
- Типы тестирования на проникновение
- Техники тестирования на проникновение
- Фазы тестирования на проникновение
- Дорожная карта тестирования на проникновение
- Сервисы тестирования на проникновение
- Инструменты тестирования на проникновение

Материалы слушателя

- Слушателям предоставляется фирменное учебное пособие и руководство по проведению лабораторных работ (в электронном виде) а так же прочие материалы и программное обеспечение, необходимые для выполнения этих работ.

Дополнительно

- Точное место и способ проведения тренинга уточняйте у менеджера по обучению
- При группах от 3 человек стоимость и место проведения тренинга по согласованию с Заказчиком
- Тренинги могут проводиться в г. Алматы, г. Астана, г. Москва или дистанционно