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 00 11
info@intella.kz
www.intella.pro



**ПРИГЛАШЕНИЕ**

**На сертифицированный тренинг**

**ISTA Аудит безопасности IT-инфраструктуры и тестирование на проникновение**

- **Статус:** Авторизованный
- **Длительность обучения** – 4 дня (40 ак.часов)
- **Форма обучения** – аудиторные занятия на русском языке
- **Связанные сертификации**: CEH, CISSP
- **На базе центра повышения квалификации:** ТОО «INTELLA»
- **Место и даты проведения** – Алматы, ул.Ауэзова, 60, БЦ «Almaty Resdense» 6 этаж. Оф 17а
  г.Астана р-н Есиль ул. Д. Кунаева, 29/1, оф.1903
- **Форма обучения -** аудиторные занятия
- **Расписание -** с 10.00 до 18.00, обед с 13.00 до 14.00.
- **Преподаватель:** Ведущий специалист ПАЦИФИКА (CEH, Lead auditor)

***Аннотация тренинга***

содержание тренинга составляет *цикл практических занятий, объединенных общим сценарием тестирования* защищенности IT-инфраструктуры предприятия от наиболее вероятных внутренних и внешних угроз информационной безопасности, и *аудита* соответствия ее текущего уровня защищенности требованиям политики безопасности, проводимых *в форме практического тренинга*

1) Тренинг не привязан к какому-либо производителю
2) Материал подается в нескучном формате без лишней теории и сложной математики
3) В тренинге половина времени отводится на практику
4) Вмещает весь материал, который необходим как часть других программ обучения
5) Тренинг вмещает глубокий разбор материала доменов 2,6,9,10 CISSP; CEH
6) Основной задачей тренинга поставлено понимание материала, а не зазубривание

***Цель тренинга***

научить применять методики и программные средства, используемые хакерами, для проведения аудита безопасности IT-инфраструктуры.

***Целевая аудитория***

специалисты по информационной безопасности, ИТ-аудиторы.

***Базовые требования к участникам***

базовая подготовка в области информационных технологий и информационной безопасности, в том числе:

***Ценность обучения***

знание:

- методологий тестирования на проникновение;
- рисков, связанных с проведением активного аудита, и мер по их минимизации.

умение:

- проводить тестирование защищенности информационных систем;
- подготавливать профессионально оформленный отчет по результатам аудита.

***Пакет слушателя***

- Фирменное учебное пособие.
- Раздаточный материал (в электронном и печатном виде)
- При успешном окончании обучения слушателю выдаётся Сертификат центра повышения квалификации INTELLA

**В стоимость включено:**

- Раздаточный материал (в электронном и печатном виде)
- Кофе-брейки, обеды

Асель Муханмеджанова info@intella.kz (Астана) + 7 (7172) 28-00-82

Диана Фролова df@intella.kz (Алматы) +7 (777) 552 74 22

***ПРОГРАММА ТРЕНИНГА***

# ISTA Аудит безопасности IT-инфраструктуры и тестирование на проникновение

## *РАЗДЕЛ 1. ТЕХНОЛОГИИ АУДИТА ИТ ИНФРАСТРУКТУРЫ*

- Техническая диагностика и экспертное обследование IT-инфраструктуры, на соответствие требованиям РК в области информационной безопасности
- Выбор методики и инструментальных средств проведения аудита и тестирования защищенности
- Виды отчетов

## *РАЗДЕЛ 2. ИНСТРУМЕНТАРИЙ ТЕСТИРОВЩИКА*

- построение тестового полигона средствами виртуализации;
- установка и настройка Kali Linux и Сканер-Nessus в виртуальной лаборатории;
- основы Linux;
- Kali Linux: обзор утилит и настройка;

Практическая работа: настройка виртуальной среды.

## *РАЗДЕЛ 3. ТЕСТИРОВАНИЕ ЗАЩИЩЕННОСТИ НА ОСНОВЕ СПОСОБОВ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ*

- Техники социальной инженерии
- Предварительный сбор информации: эффективные поисковые технологии в интернет
- footprinting: определение адресов, имен ресурсов, используемых технологий. Инструменты: dig, whois, harvester;

Практическая работа: сбор данных по определенной организации методом социальной инженерии.

## *РАЗДЕЛ 4. СКАНИРОВАНИЕ СЕТИ И РУЧНОЙ ПОИСК УЯЗВИМОСТЕЙ*

- сканирование портов с помощью NMAP;
- анализ баннеров сервисов;
- ручной поиск уязвимостей: специализированные поисковики, сайты вендоров и т.п;
- Практическая работа: просканировать сервер-жертву nmap и собрать данные об уязвимостях.

## *РАЗДЕЛ 5. ИСПОЛЬЗОВАНИЕ СКАНЕРОВ УЯЗВИМОСТЕЙ*

- принципы работы сканеров уязвимостей;
- обзор сканеров уязвимостей;

Практическая работа: просканировать сервер-жертву с помощью сканера, подготовить отчет по тестированию защищенности.

***РАЗДЕЛ 6. ПОДБОР ПАРОЛЕЙ***

- какие пароли выбирают пользователи?
- пароли по умолчанию;
- методы подбора паролей;
- практика: подбор паролей.

Практическая работа: Применение техник по взлому паролей и повышению привилегий в операционных системах

***РАЗДЕЛ 7. ТЕСТИРОВАНИЕ на проникновение WEB- ПРИЛОЖЕНИЙ***

- основные уязвимости веб-приложений
- основы HTTP для этичного хакера;
- уязвимости, связанные с непроверяемыми полями ввода данных;
- применение локальных прокси-серверов;
- атаки Cross Site Scripting;
- атаки методом SQL-инъекции.

***РАЗДЕЛ 9. ЭКСПЛУАТАЦИЯ***

- проведение MITM-атаки с использованием ARP-спуфинга;
- фреймворк Metasploit: структура и возможности;
- поиск подходящих эксплойтов;
- использование консоли Metasploit для эксплуатации уязвимостей;
- использование графического интерфейса Armitage для эксплуатации уязвимостей;
- атаки на клиентское ПО: захват браузера с помощью BeeF;
- поддержание доступа: установка бэкдора и его применение;

Практическая работа: работа с Metasploit.

***Контакты:***

Диана Фролова df@intella.kz (Алматы) +7 (727) 355 02 34

(Астана) + 7 (7172) 28-00-82

Татьяна Бережная tb@intella.kz (Алматы) +7 (727) 355 02 34