Тренинг по тестированию на проникновение

Длительность тренинга – 2 дня.

1. Программа тренинга

День 1.

1. Вводная часть
    a. Основы этичного хакинга
    b. «Черные шляпы», «Серые шляпы», «Белые шляпы»
    c. Законодательство по противодействию киберпреступлениям
    d. OWASP TOP 10
2. Футпринтинг
    a. Предварительный сбор информации
    b. Практическая работа с NIKTO
    c. Практическая работа с Harvester
    d. Практическая работа с Shodan
    e. Практическая работа с Google Hacking
3. Сканирование и получения информации о компьютерной системе в сети и сервисах, работающих на ее открытых портах
    a. Трёхсторонний TCP Handshake
    b. Метод «захвата баннеров»
    c. Практическая работа по исследованию систем
    d. Практическая работа по проверке портов
    e. Практическая работа по технологиям сканирования
    f. Практическая работа по идентификации операционных систем
    g. Практическая работа по моделированию сети
    h. Практическая работа по методу «захвата баннеров»
4. Сниффинг
    a. Введение в сниффинг
    b. Инструменты, используемые для сниффинга
    c. Практическая работа с Wireshark
    d. Практическая работа по подмене MAC-адресов

5. Веб-серверы и веб-приложения
    a. Введение в веб-серверы и веб-приложения
    b. Практическая работа с Burp Suite
6. Атаки типа SQL Injection
    a. Основы работы с базами данных
    b. Виды атак SQL Injection
    c. Практическая работа по ручной атаке SQL Injection
    d. Практическая работа по автоматизированному сканированию на уязвимости к атакам типа SQL Injection
7. Перехват сессий
    a. Введение в перехват сессий
    b. Практическая работа по перехвату сессий на уровне приложения
    c. Практическая работа по перехвату сессий на уровне сети
8. Зловредные программы
    a. Вирусы, троянские программы и черви
    b. Практическая работа по защите от троянской программы
    c. Практическая работа по внедрению бэкдора
    d. Взлом системы с помощью бэкдора
9. Отказ в обслуживании
    a. Введение в атаки на отказ в обслуживании
    b. Виды атак на отказ в обслуживании
    c. Способы имитации атак и проверки отказоустойчивости систем
10. Взлом беспроводных сетей
    a. Способы взлома WiFi
    b. Способы взлома Bluetooth

День 2.

11. Взлом и безопасность мобильных устройств
    a. Устройства на ОС Android
    b. Архитектура и джейлбрейк устройств на iOS
    c. Управление устройствами на iOS
    d. Использование Smartphone Pentest Framework

12. Межсетевые экраны, IDS и ханипоты
    a. Системы обнаружения вторжений
    b. Межсетевые экраны
    c. Ханипоты
    d. Практическая работа по конфигурированию IDS и ханипота
13. IoT
    a. Основы IoT
    b. IoT и основы OWASP
    c. Инструменты для анализа IoT
14. Облачные технологии
    a. Введение в облачные технологии
    b. Атаки в облаках
15. Криптография
    a. Введение в криптографию и криптоанализ
    b. Алгоритмы криптографии
    c. Хэши
    d. PKI, шифрование дисков, шифрование электронной почты
    e. Стеганография и стеганоанализ
    f. Практическая работа по криптографии
16. Социальная инженерия
    a. Введение в социальную инженерию
    b. Сбор данных для социальной инженерии
    c. Практическая работа по Google Hacking
    d. Практическая работа по Maltego
    e. Практическая работа по Recon-ng
    f. Практическая работа по Social-Engineer Toolkit (SET)
    g. Практическая работа по Cupp
    h. Практическая работа по Cewl
    i. Практическая работа по Scythe
    j. Практическая работа по Creepy
17. Отчёты
    a. Executive Summary

b. Принципы классификации и оценки
c. Детальное описание обнаруженных уязвимостей с подтверждениями
d. Метрики
e. Common Vulnerability Scoring System (CVSS)
f. Примеры оформления отчётов

Для заказа тренинга напишите нам info@h-xtech.com или позвоните +380958860891.