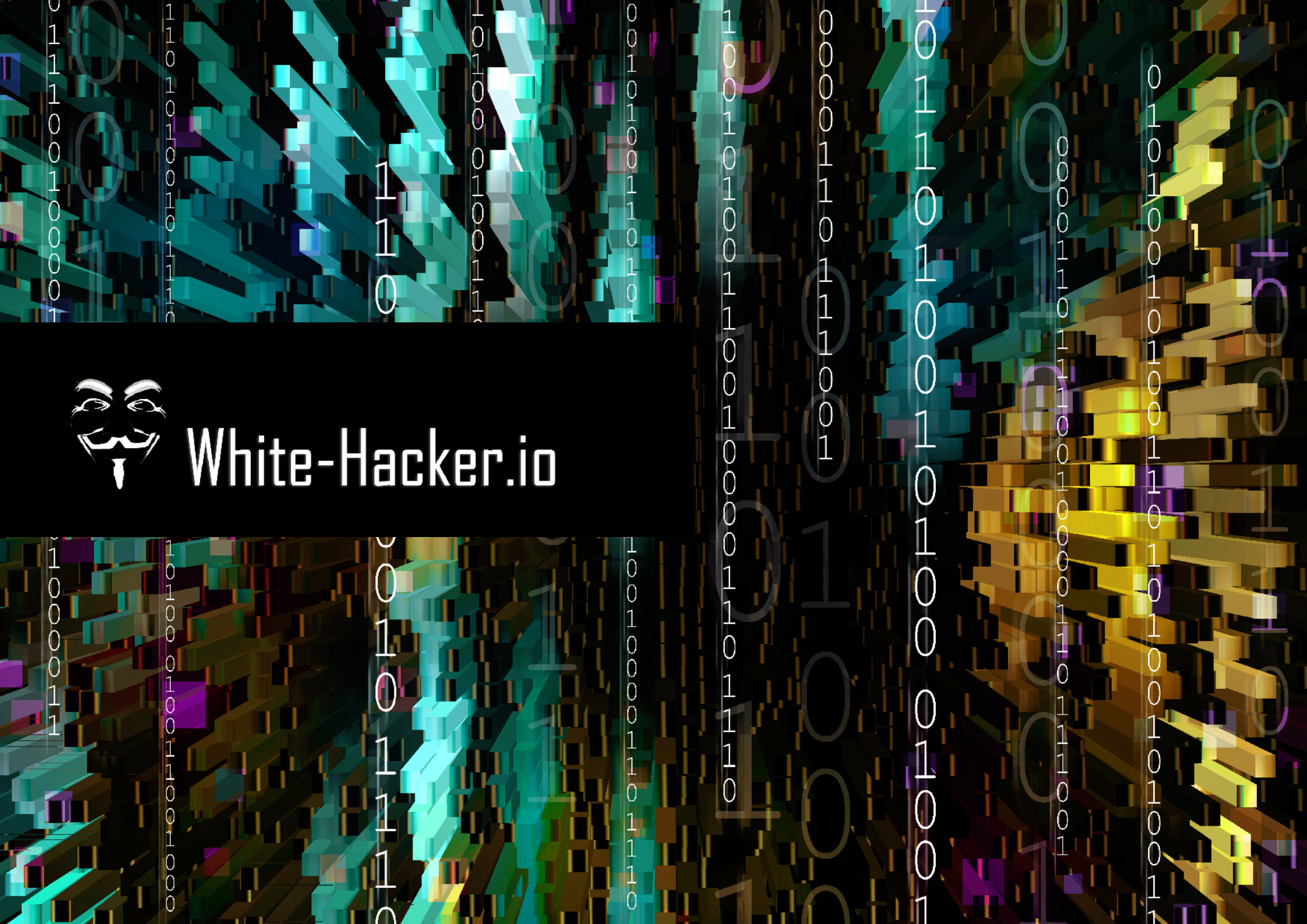

White-Hacker.io

Виды тестирований безопасности

Blackbox

Проводится по модели «черного ящика»

Заказчиком не предоставляется никакой информации о составе и конфигурации сетевого периметра, что моделирует взгляд реального внешнего злоумышленника в отношении сетевой инфраструктуры

Уровень сложности в Гайях Фоксах :)

Whitebox

Проводится по модели «серого ящика»

Заказчик предоставляет учетную запись непривилегированного пользователя и базовую информацию о конфигурации внутренней сетевой инфраструктуры целью имитации действий злоумышленника в роли нелояльного сотрудника (инсайдера).

Уровень сложности в Гайях Фоксах :)

Сбор информации о цели в рамках поставленной задачи с помощью глобальной сети, а также прибегая к другим способам подготовки логических атак.

1-2 недели

1

Поиск и подготовка опорной платформы для старта атаки и закрепления результата

1 неделя

2

Подготовка ПО собственного производства, а также сторонних производителей (настройка и подготовка программного обеспечения для решения поставленных задач)

2 недели

3

Запуск тестирования, выявление уязвимых узлов, сбор данных о сетевой инфраструктуре цели

2 недели

4

Подготовка отчета о результатах тестирования, рекомендации по исправлению уязвимостей и усилению защиты

1 неделя

5

Уровень сложности в Гайях Фоксах :)

White-Hacker.io

Сбор информации о цели в рамках поставленной задачи с помощью глобальной сети, а также прибегая к другим способам подготовки логических атак.

1-2 недели

1

Поиск и подготовка опорной платформы для старта атаки и закрепления результата

1 неделя

2

Подготовка ПО собственного производства, а также сторонних производителей (настройка и подготовка программного обеспечения для решения поставленных задач)

2 недели

3

Подготовка структуры, сценариев атак для тестирования на базе стандартов OWASP, OSSTMM, NIST

1 неделя

4

Запуск тестирования, выявление уязвимых узлов, сбор данных о сетевой инфраструктуре цели

2 недели

5

Подготовка отчета о результатах тестирования, рекомендации по исправлению уязвимостей и усилению защиты

1 неделя

6

Уровень сложности в Гайях Фоксах :)

White-Hacker.io

КОМПЛЕКСНОЕ ТЕСТИРОВАНИЕ

1. Сбор информации о цели в рамках поставленной задачи с помощью глобальной сети, а также прибегая к другим способам подготовки логических атак.
   1-2 недели
2. Поиск и подготовка опорной платформы для старта атаки и закрепления результата
   1 неделя
3. Подготовка ПО собственного производства, а также сторонних производителей (настройка и подготовка программного обеспечения для решения поставленных задач)
   2 недели
4. Подготовка структуры, сценариев атак для тестирования на базе стандартов OWASP, OSSTMM, NIST
   1 неделя
5. Запуск тестирования, выявление уязвимых узлов, сбор данных о сетевой инфраструктуре цели
   2 недели
6. Подготовка отчета о результатах тестирования, рекомендации по исправлению уязвимостей и усилению защиты
   1 неделя
7. Использование техник, отступающих от стандартов OWASP, OSSTMM, NIST (собственные методики, а также топовые практики Blackhat)
   1-3 недели
8. Закрепление в информационной системе заказчика поиск возможных систем для безопасной эксплуатации уязвимостей
   1 неделя
9. Показательная эксплуатация найденных уязвимостей в рамках, согласованных с заказчиком (не нарушая работу информационных систем заказчика)
   2 недели
10. Социальная инженерия
    2 недели
11. Тестирование WEB приложений
    2 недели
12. Тестирование Мобильных приложений
    2 недели

White-Hacker.io

Уровень сложности в Гайях Фоксах :)

ДОПОЛНЕНИЯ К ТЕСТИРОВАНИЮ

13

Использование техник, отступающих от стандартов OWASP, OSSTMM, NIST (собственные методики, а также топовые практики Blackhat)

1-3 недели

14

Закрепление в информационной системе заказчика поиск возможных систем для безопасной эксплуатации уязвимостей

1 неделя

15

Показательная эксплуатация найденных уязвимостей в рамках, согласованных с заказчиком (не нарушая работу информационных систем заказчика)

3 недели

16

Социальная инженерия

3 недели

17

Тестирование WEB приложений

3 недели

18

Тестирование Мобильных приложений

3 недели

White-Hacker.io

ДОПОЛНЕНИЯ К ТЕСТИРОВАНИЮ

Тестирование проводных корпоративных сетей

2 недели

19

Тестирование корпоративных Wifi сетей

2 недели

20

Тестирование систем видео наблюдения.

1-2 недели

21

Тестирование на устойчивость к DDos атакам

1-2 недели

22

Тестирование исходного кода программных продуктов

1-2 недели

23

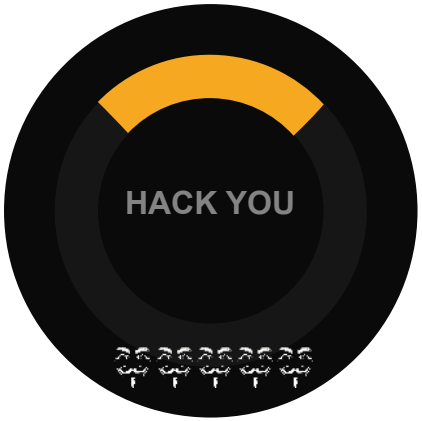
Выявление не лояльных сотрудников в компании

2-4 недели

24

White-Hacker.io

Сроки проведения мероприятий по тестированию безопасности зависят от объема выбранных тестов.



Наши контакты:
https://white-hacker.io
https://olit.su
Почта: info@olit.su
Телефоны: +7 495 940 72 72 | +7 985 227 38 16
UK +44 2038079431