1. О модуле по кибербезопасности
2. Главный инструмент белого хакера
   1. УРОК1 – Установка **OS Kali Linux** на виртуальную машину **VirtualBox**  
      **Домашнее задание:** Установить OS Kali Linux, обновить и настроить общую папку.   
      (1.5 часа)
   2. УРОК2 – Команды **bash**  
      **Домашнее задание:** С помощью команд **bash** создать папку с трема файлами в которых соответственно: список всех процессов, список файлов в текущей папке, список всех процессов начинающихся на *p.*(1 час)
   3. УРОК3 – Системное администрирование **Linux**  
      **Домашнее задание:** Изменение пароля суперпользователя через GNU GRUB   
      (1 час)
3. Стеганография
   1. Поиск скрытых данных в изображениях
      1. УРОК1 – Утилиты FILE, Strings, exiftool  
         **Домашнее задание:** Определить тип, какие строки и метаданные в файле  
         (1 час)
      2. УРОК2 – Утилиты Stegsolve, steghide, Binwalk  
         **Домашнее задание:** Найти скрытое сообщение в изображении с расширением .png  
         (1 час)
      3. УРОК3 – Web-утилиты, библиотека PIL(Python)  
         **Домашнее задание:** Произвести операцию xor с двумя изображениями при помощи библиотеки PIL  
         (1 час)
   2. Поиск скрытых данных в звуковых файлах
      1. УРОК1 – Азбука Морзе, Audacity, библиотека StegoPy(Python)  
         **Домашнее задание:** Найти скрытое послание в аудиофайле формата .mp3  
         (1 час)
   3. Поиск скрытых данных в видео файлах
      1. УРОК1 – ffmpeg, gif  
         **Домашнее задание:** Найти скрытое сообщение в видеофайле формата .mp4  
         (1 час)
   4. Поиск скрытых данных в текстовых файлах
      1. УРОК1 – Основные приемы скрытия данных в тексте, программа Shtirlitz  
         **Домашнее задание:** С помощью программы Shtirlitz определить, что скрыто в переданном сообщении  
         (1 час)
4. Web – уязвимости
   1. Основы компьютерных сетей
      1. УРОК1 – Технология Ethernet   
         **Домашнее задание:** Ответить на тест по основам компьютерных сетей  
         (1.5 часа)
      2. УРОК2 – Инструменты разработчика  
         **Домашнее задание:** С помощью инструментов разработчика посмотреть cookies на сайте  
         (1 час)
      3. УРОК3 – Протоколы, порты   
         **Домашнее задание:** Пройти тест на знание основных протоколов  
         (1.5 часа)
      4. УРОК4 – Протокол SSH   
         **Домашнее задание:** Взлом пароля SSH с помощью Hydra  
         (1 час)
      5. УРОК5– Базы данных  
         **Домашнее задание:** Создать свою БД MongoDB согласно предложенному шаблону  
         (1.5 час)
   2. Эксплуатация Web – уязвимостей
      1. УРОК1 – просмотр кода страницы, user-agent  
         **Домашнее задание:** Изменить user-agent для получения флага  
         (1 час)
      2. УРОК2 – LFI, Dirsearch, robots.txt  
         **Домашнее задание:** Просканировать все папки на сайте с помощью утилиты Dirsearch  
         (1.5 часа)
      3. УРОК3 – Command injection  
         **Домашнее задание:** Проэксплуатировать уязвимость Command injection на тестовом сайте*.*(1.5 часа)
      4. УРОК4 – Основы запросов SQL, SQL injection, sqlmap  
         **Домашнее задание:** Найти логин и пароль от администратора используя sqlmap  
         (1.5 часа)
      5. УРОК5 – Межсайтовый скриптинг  
         **Домашнее задание:** Произвести атаку XSS на тестовом сайте  
         (1.5 часа)
      6. УРОК6 – библиотека requests(Python)  
         **Домашнее задание:** С помощью библиотеки requests зайти на сайт с 10 разными user-agent  
         (1 часа)
      7. УРОК7 – Burp Suite  
         **Домашнее задание:** Используя Burp Suite зайти за Admin  
         (1.5 часа)
      8. УРОК8 – Парсинг, обход ограничений   
         **Домашнее задание:** Рассмотреть действующую уязвимость на примере FaceBook  
         (1 час)
5. Форензика
   1. УРОК1 – Форматы файлов  
      **Домашнее задание:** Взломать ключ от тестового zip-архива
   2. УРОК2 – Образы памяти  
      **Домашнее задание:** Определить что находилось на рабочем столе по время взлома
   3. УРОК3 – Анализ дисков  
      **Домашнее задание:** Найти логин и пароль от пользователя Andrey
6. Криптография
   1. УРОК1 - Кодировки и буквенные шифры  
      **Домашнее задание:** Расшифровать строку Base64
   2. УРОК2 - Симметричное шифрование  
      **Домашнее задание:** Расшифровать строку, зашифрованную алгоритмом AES
   3. УРОК3 - Асимметричное шифрование  
      **Домашнее задание:** Найти исходное сообщение, взломав алгоритм RSA
   4. УРОК4 – HashCat  
      **Домашнее задание:** Взлом “солёного” хэша на основе предложенного вордлиста
7. Reverse engineering
   1. Анализ исходного кода
      1. УРОК1 – C++  
         **Домашнее задание:** Определить, что выведет программа
      2. УРОК2 – Введение в Assembler  
         **Домашнее задание:** Найти значение регистра eax
   2. Реверсинг в Hex-Rays
      1. УРОК1 – Установка и просмотр инструментария IDA Pro  
         **Домашнее задание:** Установить IDA Pro
      2. УРОК2 – Статический анализ  
         **Домашнее задание:** Найти пароль от игры
      3. УРОК3 – Динамический анализ  
         **Домашнее задание:** С помощью динамического анализа найти лицензионный ключ
      4. УРОК4 – Патчинг  
         **Домашнее задание:** Пропатчить игру, чтобы занять 1 место
      5. УРОК5 – Автоматический анализ  
         **Домашнее задание:** Используя angr найти логин и пароль от юзера
   3. Реверс иных типов файлов
      1. УРОК1 – Реверс байткода Java
      2. УРОК2 – Реверс Androin приложений
      3. УРОК3 – Реверс .NET приложений
      4. УРОК4 – Реверс шеллы  
         **Домашнее задание:** Получить доступ к тестовому серверу с помощью Reverse Shell на python
8. Фреймворк Metasploit
   1. УРОК1 – Разбор общей методики работы с фреймворком
   2. УРОК2 – Создаём тестовую виртуальную машину на Ubuntu, проверяем на ней уязвимости  
      **Домашнее задание:** Произвести атаку на тестовую машину из предложенного списка
   3. УРОК3 – Сканируем порты серверов известных компаний на предмет уязвимостей, проводим симуляцию атаки на сервер с базой кредитных карт (Реверс шелл, уязвимость, найденная в 2017)  
      **Домашнее задание:** Закрыть «дыры» в предложенной виртуальной машине, найденные с помощью сканера в metasploit
9. Анонимность в сети
   1. УРОК1 – Изучаем TOR, VPN: что это такое и с чем едят  
      **Домашнее задание:** Создаем ветку подключения из нескольких связей TOR+VPN
   2. УРОК1 – Цифровые отпечатки  
      **Домашнее задание:** Проходим тест на знание того, что нельзя никогда оставлять о себе в сети
   3. УРОК1 – Дистрибутив TAILS  
      **Домашнее задание:** Проверить какую информацию собирает сайт о вас, в условиях работы в браузере данного дистрибутива