

Программа курса

# ОНЛАЙН-КУРС ПО ЭТИЧНОМУ ХАКИНГУ



# ПРОГРАММА КУРСА

## ► Блок 1

### Введение в пентест

#### Содержимое блока:

- Введение в курс
- Методологии пентеста
- Виртуальный полигон

#### Научишься:

- Основам тестирования на проникновение
- Методологиям пентеста
- Работе с виртуальным полигоном для практики

#### 🔧 Практика в блоке:

- Методология пентеста
- Видеоразбор

#### 📖 Методические материалы:

- Методический материал блока "Введение в пентест" 📄
- Методический материал по установке и настройке виртуальной лаборатории 🖥️

#### ✅ Тестирование по блоку Введение в пентест

## 🕸 Блок 2

### Сети

#### Содержимое блока:

- Основы сетевого взаимодействия
- Настройка стенда в GNS3
- Атака DHCP Starvation, Yersinia
- Wireshark. Основы анализа
- Протокол ARP
- Атаки MITM

#### Научишься:

- Основам сетевого взаимодействия
- Настройке стенда в GNS3 для практики
- Анализу сетевого трафика с помощью Wireshark
- Проведению атак DHCP Starvation и MITM

#### 🔧 Практика в блоке:

- Проведение атаки MITM
- Видеоразбор

#### 📖 Методические материалы:

- Методический материал по сетям 🌐
- Методические материалы по настройке GNS3 📡

#### ✅ Тестирование по блоку Сети

## Веб-пентест

### Содержимое блока:

- Введение в SQLi
- Настройка и использование Burp Suite
- SQLi. Продолжение
- Автоматизация инъекций с sqlmap
- Серверные уязвимости: Path Traversal, Information Disclosure, SSRF, Command Injection
- Клиентские уязвимости: XSS (Stored, Reflected, DOM-based), CSRF
- Основы Web Application Firewall (WAF)
- Мануал по Docker
- Итоговая работа: полигон DVWA и Juice Shop

### Научишься:

- Базам данных и основам SQL-инъекций
- Работе с Burp Suite для анализа и тестирования веб-приложений
- Использованию sqlmap для автоматизации атак
- Поиску серверных и клиентских уязвимостей (Path Traversal, SSRF, XSS, CSRF)
- защите веб-приложений от атак с использованием Web Application Firewall (WAF)
- Развёртыванию стендов DVWA и Juice Shop через Docker

### Практика в блоке:

- Проведение SQL-инъекций
- Проведение XSS-атак
- Итоговая работа: DVWA и Juice Shop
- Видеоразбор

### Методические материалы:

- Методический материал по веб-пентесту 
- Методический материал по Docker 

**Тестирование по блоку Веб-пентест**

## Эксплуатация Linux и постэксплуатация

### Содержимое блока:

- Введение, теория, cyberkillchain
- Мануал по nmap
- Эскалация через sudo misc
- Эскалация через capabilities
- Эскалация через уязвимость ядра
- Эксплуатация и эскалация Linux (kernel)
- Эскалация через crontab
- Безопасность Linux: iptables
- Итоговая практика Linux
- Мануал по mfsconsole
- Мануал по searchsploit expdb

### Научишься:

- Основам эксплуатации Linux-систем
- Методу эскалации привилегий через различные векторы (sudo, capabilities, crontab)
- Работе с инструментами для поиска уязвимостей (nmap, searchsploit)
- Защите Linux-систем с использованием iptables

### Практика в блоке:

- Эскалация через sudo
- Эскалация через crontab
- Итоговая практика Linux
- Видеоразбор

### Методические материалы:

- Методический материал по Linux 
- Методический материал по утилитам 

**Тестирование по блоку Эксплуатация Linux и постэксплуатация**

 Блок 5

## Windows

### Содержимое блока:

- Введение в Windows Active Directory
- Обзор компонентов в Active Directory
- Создание и настройка полигона
- Эксплуатация Windows
- Постэксплуатация Windows
- Mimikatz
- Обеспечение безопасности Windows-систем

### Научишься:

- Основам работы с Windows Active Directory
- Настройке и эксплуатации Windows-систем
- Использованию Mimikatz для получения учетных данных
- Защите Windows-систем от атак

### Практика в блоке:

- Атака SMB Relay
- Использование msfconsole для получения шелла
- Использование Mimikatz
- Видеоразбор

### Методические материалы:

- Методический материал по Windows 
- Методический материал для полигона Active Directory 

**Тестирование по блоку Windows**

 Bonus level

## Программирование для хакинга

### Содержимое блока:

- Intro
- Bash
- Python basics pycharm
- Python fuzz
- Python bruteforce
- Python for nmap
- Hack the box

### Научишься:

- Основам программирования на Bash и Python для хакинга
- Разработке скриптов для фуззинга и брутфорса
- Работе с nmap через Python

### Практика в блоке:

- Написание скриптов на Bash и Python
- Использование Python для автоматизации атак
- Hack the box
- Видеоразбор

### Методические материалы:

- Методический материал по Python для хакинга 
- Методический материал по Hack the box 

**Тестирование по блоку Программирование для хакинга**

## Что дальше

### Содержимое блока:

- Как развиваться после прохождения курса?
- Материалы к шестой теме
- Финальный проект: Текст задания
- Финальный проект: Итоговый кибер-полигон

### Научишься:

- Как развивать свои навыки в области этичного хакинга после завершения курса

### 🔧 Практика в блоке:

- Финальный проект: Кибер-полигон
- Видеоразбор

### 📖 Методические материалы:

- Методический материал по развитию в сфере пентеста 🚀
- Методический материал для итогового проекта 🏆

## 🏁 Финальное тестирование

### ✅ Обобщающее тестирование по всем блокам курса

- Проверь свои знания, закрепи ключевые темы и убедись, что готов применять новые навыки на практике

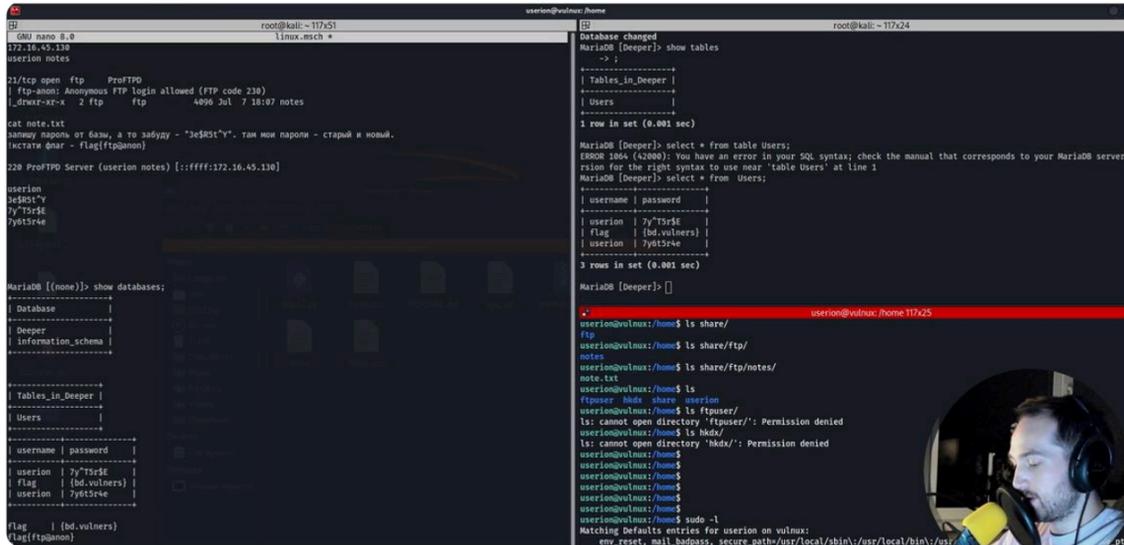
## Изучишь технологии и инструменты:

Kali Linux    BurpSuite    Metasploit    Docker

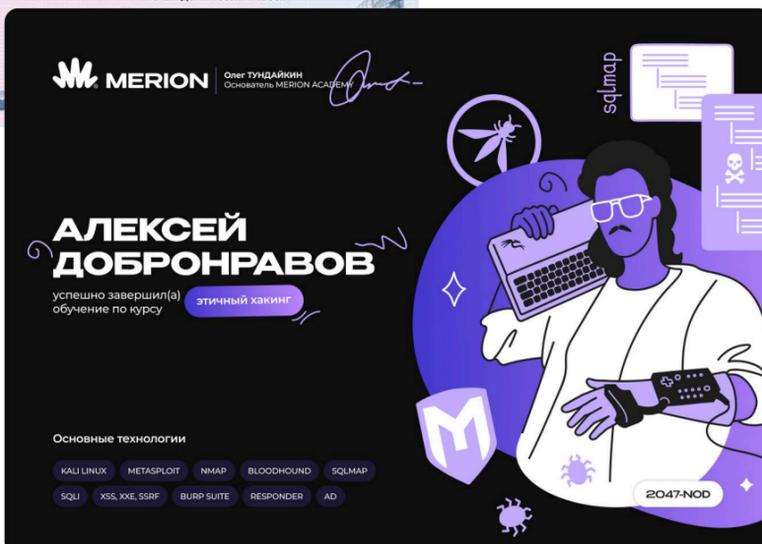
Command-line    Nmap    Hashcat    Sqlmap

GNS3    Python

## Научишься работать с хакерской операционной системой Kali Linux



## Получишь сертификаты:



# ОБ АВТОРЕ



## Гамид Джафаров

Ведущий специалист по кибербезопасности, независимый исследователь (Red Team Lead, White hat)

- Преподаватель курсов Ethical Hacking, "Белый хакер", Основы реверс-инжиниринга, Бинарные уязвимости
- Спикер Accenture «New IT fest»
- Skills: Ethical Hacking, Reverse Engineering, Vulnerability Reverse, Assembler, Python, Bash
- Products: BurpSuite (PortSwigger), Metasploit (Rapid7), Nessus (Tenable), BloodHound, Cobalt Strike, PS Empire, IDA Pro

# ЧТО ГОВОРЯТ НАШИ СТУДЕНТЫ



**Mr B.**

11 марта 2025



Все курсы сделаны профессионально и с душой)) Ёмко, интересно, современно. Уже являюсь обладателем трех курсов, и это только начало, т.к. курсы обновляются по реальным потребностям рынка обучения. Спасибо вам за ваш неповторимый стиль обучения



**Tamer Kastor**

30 января 2025



Классный сайт, для изучения профессий в сфере IT, всегда хотел влиться в эту сферу деятельности, и этот сайт надеюсь даст мне возможность 🍷



**Khizri Tataev**

26 декабря 2024



Спасибо академии Merion, которая делает образование в сфере ИТ и ИБ доступным. Множество студентов получает практические навыки в странах СНГ благодаря ей. Это большой вклад в развитие ИТ сообщества. Практические кейсы, теория в доступной визуализированной форме, удобство формата обучения от профессионалов своего дела. Везде одни плюсы, рекомендую!

# ЗДЕСЬ РАБОТАЮТ НАШИ ВЫПУСКНИКИ

Для нас это не просто логотипы, а истории повышения зарплаты, получения новой должности и масштабирования бизнеса.



## ЗАПИСАТЬСЯ

Перейди по ссылке, или отсканируй QR-код,  
чтобы записаться на курс

[Перейти по ссылке](#) >

