Compstyle
TECHNOLOGY

Программа обучения



Кибербезопасность

Red Team

Наступательная безопасность и пентест

Kali Linux | Nmap | Burp Suite | Metasploit | BloodHound

Уровень	Программа	Формат	Занятия	Язык
С нуля	8 модулей	Онлайн	Группа или индивидуально	Азербайджанский

О курсе

Чтобы защитить систему, нужно увидеть её глазами атакующего. Вы начинаете с основ сетей и сами проводите полный цикл пентеста на реальной цели – от разведки до отчёта.

Для кого этот курс

01 **Новички**

Технические знания не нужны. Первый модуль начинается с основ сетей, Linux и Windows.

02 **IT-специалисты**

Если вы системный администратор, сетевой инженер или программист, вы надстраиваете наступательную сторону над тем, что уже знаете.

03 **Студенты**

Ещё до диплома в вашем портфолио появятся реальные отчёты о пентесте и решённые лаборатории.

Как проходит неделя

01

Онлайн-занятие

Ментор объясняет тему в реальном времени, вопросы вы задаёте прямо на занятии.

02

Лаборатория

Ту же тему вы повторяете своими руками в лаборатории в браузере.

03

Еженедельное задание

Задание на основе реального сценария проверяет, что вы усвоили.

04

Проверка ментором

Ментор проверяет вашу работу, показывает ошибки и подсказывает следующий шаг.

Это не видеокурс: занятия проходят онлайн, вживую с ментором. В группе до 5 человек или индивидуально – ментор видит работу каждого. Обучение на азербайджанском языке.

Программа обучения

8 модулей – от основ до профессии

Каждый модуль закрепляется онлайн-занятием, лабораторией и еженедельным заданием. К следующему модулю вы переходите, когда освоили предыдущий на практике.

01

Основы: сети, Linux и Windows

Язык атаки: как идут пакеты и как устроена система.

OSI и TCP/IP · Терминал Linux · Внутреннее устройство Windows · Скрипты на Bash и Python

02

Разведка и OSINT

Изучение цели – без касания и с касанием.

Пассивная и активная разведка · Nmap · Поиск поддоменов · Перечисление сервисов

03

Атаки на веб-приложения

Самая частая цель – веб-приложения.

OWASP Top 10 · Burp Suite · SQL injection · XSS · SSRF · Ошибки аутентификации

04

Эксплуатация сетей и сервисов

От открытого порта до первоначального доступа.

Metasploit · Публичные эксплойты · Атаки на пароли · Reverse shell

05

Повышение привилегий

От обычного пользователя до root и SYSTEM.

Повышение привилегий в Linux · Повышение привилегий в Windows · Ошибки конфигурации

06

Атаки на Active Directory

Сердце корпоративной сети – домен.

Kerberoasting · BloodHound · Pass-the-hash · Lateral movement

07

Пост-эксплуатация

Закрепление доступа и продвижение по сети.

Persistence · Pivoting · Туннелирование · Основы C2

08

Отчёт о пентесте и карьера

Перевести находки на язык, понятный заказчику.

Структура отчёта · Оценка рисков · Портфолио · Подготовка к собеседованию

По итогам курса вы сможете

- Самостоятельно проводить полный цикл пентеста целевой системы
- Находить и доказывать уязвимости OWASP Top 10 в веб-приложениях
- Повышать привилегии в Linux и Windows
- Выстраивать цепочку атаки в среде Active Directory
- Писать профессиональный отчёт о пентесте для заказчика
- Решать машины HackTheBox и TryHackMe без подсказок

Инструменты, с которыми вы будете работать

Kali Linux · Nmap · Burp Suite · Metasploit · BloodHound · Impacket · Hydra · Gobuster · Wireshark · Python

Где работают наши выпускники

Kapital Bank · Rabitəbank · birmarket · RISK COMPANY · BMU Bakı Mühəndislik Universiteti · AZTU

Следующий шаг

Приходите на бесплатный онлайн-урок – познакомьтесь с ментором, а потом решайте.

Группа или индивидуально - выбор за вами. Цену, расписание и дату старта следующей группы пришлём в WhatsApp. Обучение на азербайджанском языке.

WhatsApp и звонки	+994 70 639 33 09
Сайт	compstyle.tech/ru/kursy/red-team
Instagram	@compstyle.az
Telegram	@compstylekanal
YouTube	@Compstyle



Compstyle TECHNOLOGY

Учись сам, создавай сам.

© Compstyle Technology