

Cybersecurity

Red Team

Offensive security and pentesting

Kali Linux | Nmap | Burp Suite | Metasploit | BloodHound

Level	Program	Format	Lessons	Language
From zero	8 modules	Online	Group or one-to-one	Azerbaijani

To protect a system, you have to see it through an attacker’s eyes. You start from networking fundamentals and run a full pentest cycle on a real target yourself – from reconnaissance to the report.

Who this course is for

01 **Complete beginners**

No technical knowledge required. The first module starts with networking, Linux and Windows fundamentals.

02 **IT professionals**

If you are a system administrator, network engineer or developer, you build the offensive side on top of what you already know.

03 **Students**

Before you graduate, your portfolio fills up with real pentest reports and labs you have solved.

What a week looks like

01

Online lesson

The mentor explains the topic live; you ask your questions right in the lesson.

02

Lab

You repeat the same topic hands-on in a browser-based lab.

03

Weekly assignment

You test what you know with an assignment based on a real scenario.

04

Mentor review

The mentor reviews your work, points out mistakes and tells you the next step.

This isn’t a video course: lessons are online and live with a mentor. A group of up to 5 people or one-to-one – the mentor sees everyone’s work. Lessons are taught in Azerbaijani.

Curriculum

8 modules – from fundamentals to a profession

Every module ends with an online lesson, a lab and a weekly assignment. You move on to the next module once you have mastered the previous one in practice.

01

Fundamentals: networking, Linux and Windows

The language of attacks: how packets travel and how systems are built.

OSI and TCP/IP · Linux terminal · Windows internals · Bash and Python scripting

02

Reconnaissance and OSINT

Getting to know the target – without touching it, and by touching it.

Passive and active recon · Nmap · Subdomain discovery · Service enumeration

03

Web application attacks

The most common target – web applications.

OWASP Top 10 · Burp Suite · SQL injection · XSS · SSRF · Authentication flaws

04

Network and service exploitation

From an open port to initial access.

Metasploit · Public exploits · Password attacks · Reverse shell

05

Privilege escalation

From a regular user to root and SYSTEM.

Linux privilege escalation · Windows privilege escalation · Misconfigurations

06

Active Directory attacks

The heart of a corporate network – the domain.

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

07

Post-exploitation

Keeping access and moving through the network.

Persistence · Pivoting · Tunneling · C2 basics

08

Pentest reporting and career

Turning findings into language the client understands.

Report structure · Risk assessment · Portfolio · Interview prep

By the end of the course you will be able to

- Run a full pentest cycle on a target system on your own
- Find and prove OWASP Top 10 vulnerabilities in web applications
- Escalate privileges on Linux and Windows
- Build an attack chain in an Active Directory environment
- Write a professional pentest report ready for a client
- Solve HackTheBox and TryHackMe machines without help

Tools you'll use

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

Where our graduates work

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

Next step

Join a free online trial lesson – meet your mentor, then decide.

Group or one-to-one – the choice is yours. We'll send you the price, schedule and start date of the next group on WhatsApp. Lessons are taught in Azerbaijani.

WhatsApp and calls	+994 70 639 33 09
Website	compstyle.tech/en/courses/red-team
Instagram	@compstyle.az
Telegram	@compstylekanal
YouTube	@Compstyle

Compstyle TECHNOLOGY

Learn it yourself, build it yourself.

© Compstyle Technology