BloodCode Red Team Academy

Ethical Hacking, Pentesting & Adversary Simulation

Instructor: Stefan Spasov BloodCode

Format: 12 weeks, lab-first, legal and defensive.

Contact: bloodcodehack@gmail.com | +381 63 146 0616 | akademija.elmconstruct.com

Promise

BloodCode Red Team Academy teaches the process, discipline, reporting and defensive thinking behind ethical hacking and red-team work. This is not illegal hacking. Every exercise is done in owned labs, CTFs, controlled training environments or authorized engagements.

Students learn how to think, test, document and communicate like professionals.

Who this is for

- Beginners who want a serious path into cybersecurity.
- Junior IT people who want pentesting and security fundamentals.
- Students who want practical labs, not random YouTube chaos.
- Business owners who want to understand real cyber risk.
- Future consultants who want to write professional reports.

Safety rules

- No testing public systems without written authorization.
- No credential theft.
- No malware deployment.
- No destructive actions.
- No evasion or stealth against real organizations.
- Every lab has a defensive outcome: detection, hardening, reporting or remediation.

12-week curriculum

Week 1: Law, ethics, scope and professional mindset

- Difference between hacking, pentesting and red team.
- Authorization, scope, Rules of Engagement.
- Evidence handling and reporting discipline.
- Lab: write a safe scope and test plan.

Week 2: Networking, DNS, HTTP and Linux basics

- TCP/IP, ports, protocols, DNS, TLS, HTTP.

- Linux terminal, permissions, logs, services.
- Lab: map a local lab network and document assets.

Week 3: Web security foundations

- OWASP Top 10.
- Authentication, sessions, cookies, input validation.
- Lab: safe vulnerable web app exercises.

Week 4: API and authorization testing

- IDOR/BOLA.
- Role and tenant isolation.
- API request/response reasoning.
- Lab: test access boundaries in a local API.

Week 5: OSINT and passive recon

- Legal recon boundaries.
- Public sources, DNS, certificates, documentation, GitHub hygiene.
- Lab: passive recon report on owned/lab assets.

Week 6: Vulnerability validation and severity

- Impact vs noise.
- False positives.
- CVSS basics and business impact.
- Lab: triage sample findings.

Week 7: Windows and Active Directory concepts

- Windows security model.
- AD, Kerberos, LDAP, GPO, logs.
- Lab: defensive AD mapping and hardening checklist.

Week 8: Cloud and SaaS misconfiguration

- IAM, storage, public exposure, logs, secrets.
- SaaS sharing risks.
- Lab: review intentionally misconfigured cloud-like scenarios.

Week 9: Phishing defense and awareness simulation

- How phishing works conceptually.
- Safe simulation without collecting passwords.
- Reporting process and employee training.
- Lab: build a safe awareness campaign plan.

Week 10: Blue team detection and incident response

- Logs, SIEM basics, alert quality.
- Tabletop incident exercise.
- Lab: write a detection and response plan.

Week 11: Report writing and executive communication

- Technical report structure.
- Executive one-page summary.
- Remediation roadmap.
- Lab: write a report from evidence.

Week 12: Final project

- Scope.
- Test plan.
- Lab execution.
- Findings.
- Executive report.
- Defense and debrief.

Packages

Self-study: 99 EUR

- Recorded modules.
- PDF syllabus.
- Lab tasks.
- Starter checklist.

Pro Academy: 499 EUR

- Everything in Self-study.
- Weekly group sessions.
- Report review.
- Community access.

Mentorship: 999 EUR

- Everything in Pro Academy.
- Direct mentor feedback.
- Personal learning roadmap.
- Portfolio/report review.

Elite 1-on-1: 2.500 EUR

- Private sessions.

- Custom lab roadmap.
- Career/business positioning.
- Final project review.

Corporate training: 2.500 EUR+

- Custom training for teams.
- Security awareness.
- Executive tabletop.
- Defensive red-team methodology.

Lead magnets

- Red Team Starter Checklist.
- 50 Pentesting Commands Cheatsheet for legal labs.
- Executive Cyber Risk Checklist for firm owners.
- Sample pentest report template.

CTA

Write `RED TEAM` on WhatsApp: +381 63 146 0616

Or email: bloodcodehack@gmail.com