

ƏLİƏKBƏR BABAYEV

ETHICAL HACKER

CONTACT

☎ +994-55-533-5253

✉ eliekberbabayev23082007@gmail.com

📍 Baku city, Bineqedi Dist.
Khutor Str, No 52

EDUCATION

2024 - 2028

AZERBAIJAN STATE OIL AND
INDUSTRIAL UNIVERSITY

- Information Security in English

SKILLS

- Network Forensics
- Windows/Linux Manager
- Scripting
- Exploitation
- Privilege Escalation
- CTF Player
- Red Teaming
- Web Exploitation

SUMMARY

A highly motivated and passionate Cybersecurity enthusiast with a strong foundation in ethical hacking principles, network security, and system administration. Proven practical skills through active participation in Capture The Flag (CTF) competitions, development of security tools, and completion of multiple industry-recognized certifications. Eager to apply technical knowledge in Linux, Windows, and networking to an entry-level SOC Analyst, Vulnerability Management, or Penetration Testing role. A fast learner committed to continuous professional development.

PROJECTS

CTF Walkthroughs

2025 - PRESENT

Vulnhub Machines

- documented my learning process through hands-on labs, vulnerable machines, and capture-the-flag challenges.

My Tools

- **ARPKill** - Python-based tool that demonstrates ARP spoofing/poisoning attacks to disconnect devices from a local network.
- **DirSeeker** - Python-based directory brute-force tool for discovering hidden files and folders on web servers.
- **SSHield** - Python-based real-time brute-force attack detection tool. It monitors SSH login attempts from system logs and helps identify suspicious activity such as repeated failed login attempts that may indicate a brute-force attack.

I shared these in my github repositories : www.github.com/ali-ctf-player

CERTIFICATIONS

- [Ethical Hacker] | [Cisco Networking Academy]
- [Multi Cloud Red Team Analyst] | [CyberWarfare Labs]
- [Python/C++ Essentials] | [Cisco Networking Academy]
- [Cyber Security Analyst] | [Cisco Networking Academy]
- [Certified Red Teaming Infra-Dev] | [CyberWarfare Labs]