

## LYUBEN PETROV

Highly motivated and disciplined, I'm a quick learner with a thirst for knowledge. A critical thinker with great attention to detail, I excel in teamwork, possess tech-savvy skills, and manage time effectively. As a communicator, I actively listen and respond. In my free time I like participating in CTFs and writing about them in my blog.

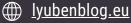
 $\sim$ 

lyubenlp.work@gmail.com



0887212955

**?** Sofia, Bulgaria



## PERSONAL INFORMATION

Name: Lyuben Petrov, born 04/03/1999

• From: Sofia, Bulgaria

• LinkedIn profile

# **EDUCATIONAL HISTORY**

# BACHELOR COMPUTER SCIENCE AND ENGINEERING

Eindhoven University of Technology (Sep 2018 - Apr 2022)

- Focus on Cybersecurity (and AI) through elective courses
- Above 7 grade point average (out of 10)
- Experience with wide variety of technologies: Java, Python, Ruby (on Rails), Bash, SQL

# SECONDARY EDUCATION

73rd High school of foreign languages "Vladislav Gramatik", Sofia (2013 - 2018)

- Mathematics- and informatics-oriented curriculum
- · C1 Level in German with DSD certificate
- Overall grade 5.91/6 (excellent)

#### **ENGLISH SKILLS**

C2 level with CPE certificate

## **EXPERIENCE**

### STAFF CONSULTANT

A-LIGN | July 2022 - October 2023

- Performed SOC 1 and 2 audits, as well as HIPAA, for international clients.
- Reviewed penetration tests, risk assessments and security controls.
- Gained deep understanding of technologies that clients use for protection - firewalls, AVs, IDS/IPS, ISMS, FIM, Active Directory.
- Developed an impeccable work ethic necessitated by meeting tight deadlines and working on simultaneous engagements.

### **CERTIFIED PENETRATION TESTING SPECIALIST**

Certificate by HackTheBox | November 2023 - January 2024

- Passed with 100 points and excellent report feedback.
- Mastered crucial tools like Nmap, Metasploit, BurpSuite,
  Nessus, Kali Linux tools, Impacket (and many others)
- Learned key concepts like:
  - Information gathering and reconnaissance techniques.
  - Attacking Windows and Linux targets.
  - Windows and Linux Privilege escalation.
  - Active Directory penetration testing.
  - Web application penetration testing.
  - Vulnerability assessment.
  - Pivoting and Lateral Movement.
  - Post-exploitation enumeration.
  - Vulnerability/Risk communication and reporting.