LEVI GEERT HEKMAN

ETHICAL HACKER

CONTACT

- 06-53373321
- Levihekman21@gmail.com
- Sassenheim, Zuid-Holland
- Levihekman.nl

SKILLS

- Governance, Risk & Compliance
- Network Security
- Penetration Testing Fundamentals
- Security Awareness
- ISO 27001
- Incident Response
- Threat Intelligence
- Vulnerability Assessment

LANGUAGES

- Dutch
- English

PROFILE

Cybersecurity student at NOVI University of Applied Sciences, currently completing an intensive Ethical Hacker Bootcamp focused on offensive security, network security, and organizational risk management. Experienced in conducting ISO 27001 audits, threat landscape analysis (Cyber Kill Chain, MITRE ATT&CK), and developing practical security improvement plans. Analytical and detail-oriented, with a background in digital strategy that supports structured, evidence-based work. Looking to bring these skills into a first role within a security or pentesting team.

WORK EXPERIENCE

Bright Work Wear 2023 - 2025
Marketing Specialist

- SEO optimization • Website improvements • Content strategy • Online marketing • Brand positioning • Technical SEO analysis • Performance optimization • Improved website visibility • Optimized content structure • Supported digital marketing strategy

Bright Work Wear 2022 - 2023
Production employee

- Process-oriented working • Quality control • Precision • Team collaboration

Mika Distribution
Marketing & Communication intern 2022 - 2022

- Supported marketing campaigns • communication activities and digital content creation

L.J. Sport 2019 - 2020
Sales associate

- Customer advice • Product knowledge application • Sales performance • Visual merchandising

EDUCATION

NOVI Hogeschool 2026 - 2026
Ethical Hacker BootCamp (HBO)

Codam Coding College 2025 - 2025
Piscine Programming Bootcamp

Roc Top 2020 - 2023
Marketing & Communication

PROJECTS

Organisation Security Risk Assessment — Fictional FinTech SaaS Case Study

- Conducted a full ISO/IEC 27001:2022 compliance audit for a simulated B2B FinTech SaaS organization, identifying control gaps in vulnerability management, network segmentation, and incident detection
- Modeled a hypothetical data breach scenario (based on the 2017 Equifax incident) using the Cyber Kill Chain and MITRE ATT&CK frameworks to map attacker behavior and technical impact
- Performed qualitative and quantitative risk analysis (Annual Loss Expectancy method), quantifying financial exposure at €610K/year
- Designed an 18-month remediation roadmap (SANS Maturity Model level 2 → 3), including automated vulnerability management, SIEM/UEBA monitoring, and Zero Trust network segmentation, projected to reduce annual risk exposure by €381K

NovaTech CTF — Self-Designed Docker-Based Capture The Flag Challenge

- Designed, built, and containerized a full Capture The Flag challenge (Docker/docker-compose) for the Systems Security bootcamp end-of-year assignment, simulating a vulnerable web application environment
- Engineered and validated a complete multi-stage exploit chain: Local File Inclusion (LFI) via path traversal, SSH log poisoning (Apache/rsyslog), and Remote Code Execution (RCE) through malicious payload injection
- Designed a privilege escalation path via a misconfigured world-writable cronjob to escalate from web-shell access to root
- Authored comprehensive setup documentation for Windows, Linux, and macOS, enabling fellow students to independently deploy and solve the challenge
- Ensured cross-platform reproducibility through full Docker containerization of all services (Apache, PHP, SSH, rsyslog)