JAKUB SKRZYNECKI

Junior Cybersecurity Analyst | SOC Trainee | Blue Team |Vulnerability Management

Contact

☎ +48 662 516 512

sjakubskrzynecki@gmail.com

Rzeszów

https://linkedin.com/in/jakub-skrzynecki-f0r-vv0rk

https://tryhackme.com/p/CyberhelperJS

https://jakubsx01.github.io/

About Me

Motivated M.Sc. student in Cybersecurity & Cloud Technologies with hands-on experience in web application security, penetration testing, identity & access management (IAM), and network defense. Strong technical foundation in Kali Linux, OWASP tools, MITRE ATT&CK, and Microsoft Azure security. Skilled in executing real-world labs (TryHackMe), academic projects, and proof-of-concept attacks/defenses. Seeking an cybersecurity role to apply technical expertise and grow in professional security environments.

Language

- Polish - Native
- English - C1

Education

(2025 - Currently)

RZESZÓW UNIVERSITY OF TECHNOLOGY

M.Sc. Computer Science, Cybersecurity & Cloud Technologies (in progress)

(2019-2025)

RZESZÓW UNIVERSITY OF TECHNOLOGY

B.Sc. Electronics & Telecommunications, specialization: Telecommunications

(2017 -2021)

STASZIC SECONDARY SCHOOL, TARNOBRZEG

Technical Diploma in Teleinformatics

Professional Experience

(Jul 2023 - Aug 2023)

ELTEL NETWORKS ENERGETYKA S.A. (WIDEŁKA) – INTERN

- Assisted in deployment and configuration of network devices (routers, switches, Wi-Fi access points) with focus on secure setup.
- Performed asset inventory and enumeration to support infrastructure risk assessment.
- Verified reliability of UPS systems and emergency power outlets ensuring business continuity.
- Troubleshooted and restored VoIP communication systems and user devices.

Projects

ENTERPRISE IDENTITY MANAGEMENT – AUTHENTIK SSO IN AZURE

- Implemented and configured Authentik SSO in a Microsoft Azure environment.
- Integrated services with SAML 2.0, OAuth2, LDAP (Active Directory).
- Strengthened security to prevent unauthorized access.

WEB APPLICATION SECURITY ASSESSMENT – PLANTCARE APP

- Conducted security audit aligned with OWASP Top 10.
- Performed scans using OWASP ZAP, dependency analysis with GitHub Dependabot, and manual CVE verification.

MAN-IN-THE-MIDDLE ATTACKS – BETTERCAP

- Simulated ARP Poisoning and DNS Spoofing in a lab environment.
- Demonstrated HTTPS hijacking and extended attacks using BEEF and SET Toolkit.
- Delivered mitigation recommendations.

VULNERABILITY AUDIT – OPENVAS

- Configured and ran a vulnerability scan on a test infrastructure.
- Analyzed results, prioritized risks, and prepared a full remediation report.

Certifications

- CompTIA Security+ (SY0-701)
- TryHackMe Learning Paths: CompTIA Pentest+, Red Teaming, Jr. Penetration Tester, Web Fundamentals
- Google Cloud Skills Boost – Cloud Digital Leader Learning Path
- SEP Certification – Operation of electrical devices, installations, and networks

Technical Skills (Highlights)

- Languages & Scripting: Python (intermediate), Bash (basic), Java/JavaScript/TypeScript (basic), SQL
- Security Tools: Kali Linux, Nmap, Metasploit, OWASP ZAP, Burp Suite, sqlmap, ffuf, gobuster, Bettercap, OpenVAS
- Cloud Platforms: Microsoft Azure (IAM, Authentik SSO)
- Frameworks & Standards: OWASP Top 10, MITRE ATT&CK
- Soft Skills: Effective communication, project planning, fast learning