JAKUB SKRZYNECKI

Junior Cybersecurity Analyst | SOC Trainee | Blue Team

Rzeszów, Poland

sjakubskrzynecki@gmail.com | +48 662 516 512

LinkedIn: jakub-skrzynecki | Portfolio: jakubsx01.github.io | TryHackMe: CyberhelperJS

PROFESSIONAL PROFILE

Ambitious Master's student in Cybersecurity with a strong foundation in network defense, web application security, and cloud technologies. Practical experience gained through academic projects and extensive lab simulations (TryHackMe, Home Lab). Proficient in vulnerability assessment (OWASP ZAP, OpenVAS), IAM implementation (Authentik, Azure AD), and incident response basics. Passionate about Blue Teaming and eager to contribute to a SOC or Security Engineering team.

PROFESSIONAL EXPERIENCE

IT/Network Intern **July 2023 – Aug 2023**

ELTEL NETWORKS ENERGETYKA S.A. *Widełka, Poland*

- **Network Security Support**: Assisted in the secure configuration of network infrastructure (routers, switches, APs), ensuring compliance with internal security policies.
- **Asset Management**: Conducted comprehensive inventory and enumeration of IT assets to support risk assessment and vulnerability management processes.
- **Infrastructure Reliability**: Verified UPS systems and emergency power solutions to guarantee business continuity during power outages.
- **Technical Support**: Resolved hardware and software issues for end-users, maintaining high availability of workstations and VoIP systems.

KEY PROJECTS

Identity & Access Management Implementation *Academic Project*

Authentik, Microsoft Azure, Docker

- **SSO Deployment**: Deployed Authentik as an Identity Provider (IdP) in Azure, enabling Single Sign-On (SSO) for multiple applications.
- **Integration**: Configured SAML 2.0 and OAuth2 protocols to integrate with Active Directory (LDAP), centralizing user management.
- **Security Hardening**: Implemented MFA and strict access policies to prevent unauthorized access.

Web Application Security Audit (PlantCare) *Academic Project*

OWASP ZAP, Burp Suite, Python

- **Vulnerability Assessment**: Performed a comprehensive security audit based on OWASP Top 10, identifying critical vulnerabilities (XSS, SQLi).
- **Automated Scanning**: Utilized OWASP ZAP for automated scanning and GitHub Dependabot for software composition analysis (SCA).
- **Remediation**: Provided detailed remediation reports and fixed identified CVEs in the application code.

Network Attack & Defense Simulation *Home Lab*

Bettercap, Wireshark, Snort

- **Traffic Analysis**: Simulated MitM attacks (ARP Spoofing, DNS Spoofing) to understand attack vectors and detection signatures.
- **Packet Inspection**: Analyzed captured traffic using Wireshark to identify anomalies and cleartext credentials.
- **Defense**: Configured IDS rules (Snort) to detect and alert on suspicious network patterns.

TECHNICAL SKILLS

Security Operations: SIEM (ELK Stack), Vulnerability Management (OpenVAS, Nessus), IDS/IPS (Snort), Honeypots (T-Pot).
Web Security: OWASP Top 10, Burp Suite, OWASP ZAP, Security Headers, WAF concepts.
Networking: TCP/IP, OSI Model, Wireshark, Nmap, VPN, DNS, DHCP, Routing (BGP basics).
Cloud & IAM: Microsoft Azure, Active Directory, Authentik, OAuth 2.0, SAML, Docker, Linux (Kali, Ubuntu).
Programming: Python (Scripting, Automation), SQL, Bash, JavaScript (Basic).

EDUCATION

M.Sc. in Computer Science (Cybersecurity) Rzeszów University of Technology
2025 – Present
Thesis: Advanced Cloud Security Architectures

B.Eng. in Electronics and Telecommunications Rzeszów University of Technology
2019 – 2025
Specialization: Telecommunications Systems

CERTIFICATIONS & TRAINING

- **CompTIA Security+** (SY0-701) – *In Progress/Completed*
- **Google Cloud Digital Leader** – Google Cloud Skills Boost
- **TryHackMe Paths**: Pre-Security, Web Fundamentals, Jr. Penetration Tester, SOC Level 1
- **Network Security** – Course Completion Certificate