



# JAKUB SKRZYNECKI

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

## Education

(2025 - Obecnie)

**POLITECHNIKA RZESZOWSKA**

Magister Informatyka, specjalizacja:  
Cyberbezpieczeństwo i Technologie Chmurowe

(2019-2025)

**POLITECHNIKA RZESZOWSKA**

Inżynier Elektronika i Telekomunikacja,  
specjalizacja: Telekomunikacja

(2017 -2021)

**ZESPÓŁ SZKÓŁ IM. KS. STASZICA W TARNOBRZEGU**

Technik teleinformatyk

## Doświadczenie zawodowe

(Lipiec 2023 - Sierpień 2023)

**ELTEL NETWORKS ENERGETYKA S.A.**  
**(WIDEŁKA) – PRAKTYKANT**


- Wspierałem wdrażanie i konfigurację urządzeń sieciowych (routery, switchy, punkty dostępowe Wi-Fi) z naciskiem na bezpieczne ustawienia.
- Przeprowadzałem inwentaryzację i enumerację zasobów IT, wspierając ocenę ryzyka infrastruktury.
- Weryfikowałem działanie systemów UPS i gniazd awaryjnych, zapewniając ciągłość działania.
- Rozwiązywałem problemy związane z systemami VoIP i urządzeniami użytkowników końcowych.

## Kontakt


 +48 662 516 512

 [sjakubskrzynecki@gmail.com](mailto:sjakubskrzynecki@gmail.com)

 Rzeszów

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

 <https://tryhackme.com/p/CyberhelperJS>

 <https://jakubsx01.github.io/>

## O mnie

Student studiów magisterskich na kierunku Cyberbezpieczeństwo i Technologie Chmurowe z praktycznym doświadczeniem w zakresie bezpieczeństwa aplikacji webowych, testów penetracyjnych, zarządzania tożsamością i dostępem (IAM) oraz obrony sieci. Mocne podstawy techniczne w pracy z Kali Linux, narzędziami OWASP, MITRE ATT&CK oraz zabezpieczeniami chmury Microsoft Azure. Doświadczenie w realizacji praktycznych laboratoriów (TryHackMe), projektów akademickich oraz symulacji ataków i obrony. Poszukuję pracy w obszarze cyberbezpieczeństwa, aby wykorzystać umiejętności techniczne i rozwijać się w środowisku zawodowym.

## Języki

- Polish - Native
- English - C1



## Projekty

### ZARZĄDZANIE TOŻSAMOŚCIĄ – AUTHENTIK SSO W AZURE

- Implementacja i konfiguracja systemu Authentik SSO w środowisku Microsoft Azure.
- Integracja z usługami przy użyciu SAML 2.0, OAuth2, LDAP (Active Directory).
- Wzmocnienie zabezpieczeń przed nieautoryzowanym dostępem.

### AUDYT BEZPIECZEŃSTWA APLIKACJI WEBOWEJ – PLANTCARE APP

- Przeprowadzenie audytu bezpieczeństwa zgodnego z OWASP Top 10.
- Skanowanie podatności z użyciem OWASP ZAP, analiza zależności z GitHub Dependabot, manualna weryfikacja CVE.

### SYMULACJA ATAKÓW MAN-IN-THE-MIDDLE – BETTERCAP

- Praktyczne przeprowadzenie ARP Poisoning i DNS Spoofing w środowisku testowym.
- Demonstracja przechwytywania sesji HTTPS hijacking i eskalacja ataków przy pomocy BEEF i SET Toolkit.
- Opracowanie rekomendacji dotyczących zabezpieczeń.

### AUDYT PODATNOŚCI INFRASTRUKTURY – OPENVAS

- Konfiguracja i uruchomienie skanera podatności OpenVAS.
- Analiza wyników, priorytetyzacja zagrożeń i przygotowanie raportu z zaleceniami dla administratorów.



## Certyfikaty

- CompTIA Security+ (SY0-701)
- TryHackMe – ścieżki: CompTIA Pentest+, Red Teaming, Jr. Penetration Tester, Web Fundamentals
- Google Cloud Skills Boost – Cloud Digital Leader Learning Path
- Uprawnienia SEP – Eksploatacja urządzeń, instalacji i sieci elektrycznych



## Umiejętności techniczne

- Języki i skrypty: Python (średnio zaawansowany), Bash (podstawy), Java/JavaScript/TypeScript (podstawy), SQL
- Narzędzia bezpieczeństwa: Kali Linux, Nmap, Metasploit, OWASP ZAP, Burp Suite, sqlmap, ffuf, gobuster, Bettercap, OpenVAS
- Chmura: Microsoft Azure (IAM, Authentik SSO)
- Standardy i frameworki: OWASP Top 10, MITRE ATT&CK
- Umiejętności miękkie: komunikacja, planowanie projektów, szybkie uczenie się