Jihun Baek

Cyber Security Analyst

bjhbrian916@gmail.com | 0490 326 502 | Sydney, NSW
LinkedIn: https://www.linkedin.com/in/jihun-baek-505544270 | Portfolio: jihun.me

Core Competencies

- Splunk
- Burp Suite
- Wireshark
- OWASP Top 10
- Python scripting
- AWS WAF
- AWS GuardDuty
- Docker

Education

Macquarie University

Major in Cyber Security

2024 - 2025

Handong Global University

Major in Computer Science

2021 - 2022

Certifications

AWS Certified Solutions Architect – **Professional**

Feb 2025

AWS Certified Solutions Architect – **Associate**

Jan 2025

Profile

AWS Certified Solutions Architect – Professional with hands-on experience in cloud infrastructure hardening, penetration testing, and SIEM log analysis. Track record across systems administration, offensive security CTF development, and ML-based threat detection.

Work Experience

Junior IT Systems Administrator at Gomaps Trading

Nov 2025 – Present

- Administered network and cloud infrastructure for a trading company, enforcing access control via Active Directory Group Policies and maintaining high service availability.
- Architected scalable cloud email delivery infrastructure, reducing monthly costs by 15% and hardening sending domains with SPF/DKIM/DMARC.

Challenge Developer & Technical Mentor at KnockOn

Feb – Oct 2025

- Engineered 10+ CTF challenges modelled on real-world CVEs (OWASP Top 10, privilege escalation, SSRF) for 3 cohorts of security trainees — averaging a 73% solve rate, indicating well-calibrated difficulty and real-world applicability.
- Delivered weekly technical mentoring on web exploitation, network traffic analysis, and vulnerability remediation.

Projects

Hack MAC 2025 — CTF Challenge Development & Infrastructure

Jul – Oct 2025

- Co-developed 38 CTF challenges across web, crypto, forensics, OSINT, and reverse engineering categories for a university-wide competition hosted by **Macquarie University**.
- Containerised all web challenges using Docker; wrote Python tooling to auto-scan the repo and generate JSON/Markdown challenge inventories tracking paths, categories, difficulty, and deployment status.

Penetration Test — LAMP Bulletin Board System Web App

Jan – Feb 2025

- Conducted black-box pentest of a LAMP web app identifying 8 critical vulnerabilities including SQLi, stored XSS, RCE via file upload, IDOR, and session fixation.
- Produced a structured pentest report with CVSS-style severity ratings, reproduction steps, and remediation recommendations for each finding.

AI-Based Network Attack Classifier

Nov– Dec 2024

- Built a multi-class attack classifier in Python using Random Forest, XGBoost, and Logistic Regression on network security logs which classified attack types including brute-force, SQL injection, XSS, and system command execution — best model (Random Forest) achieved 92.6% accuracy evaluated based on precision, recall, and F1-score.