Jaydon Quek

IT & Cybersecurity Graduate | Passionate About Networking & Ethical Hacking

✉ qjaydon@gmail.com ☎ +60 16 220 8997 My Website in jaydon-quek Jayd0n2

Summary

Computer Science graduate majoring in Cybersecurity with hands-on experience in system deployment, troubleshooting, and security tools. Eager to apply technical skills in network infrastructure, security tools, and proactive support mindset in an IT operations environment.

Education

University of Wollongong, B.Sc. in Computer Science *Jan 2022 – Oct 2024*

- **Major**: Cyber Security
- **Coursework:** Ethical Hacking, Cybersecurity, Networks and Communications
- **Clubs and societies**: CF Worship Coordinator/Exco Member, Malaysian Community, Dragonboat Team

Singapore Institute of Management, Diploma in Information Technology *Oct 2020 - Sep 2021*

- **Noteworthy Courses:** Database Management and Security, Business Statistics with Python

Experience

Valeo Marketing Sdn Bhd, Digital Content Specialist *Mar 2020 – Oct 2021*

- **Produced engaging articles** that enhanced the brand's online presence and attracted a wider audience**.**
- **Increased user interaction and sales** by populating content and managing promotions on E-commerce platforms (Shopee, Lazada) and social media accounts
- Assisted in **managing assets** and maintained **tracking** spreadsheets.
- Collaborated with team leads to support e-commerce and **system setup**

Projects

Carpooling Application *GitHub Repo*

- Implemented end-to-end app deployment using Flask and Heroku, simulating real-world web-based system usage and support, allowing university staff and students to book rides efficiently.
- Team lead for deployment and development of web app, database integration.
- Responsible for troubleshooting deployment and functionality issues for the app (server errors,UI/UX bugs)
- **Tech Stack**: Flask, Heroku, GitHub, SQL, HTML5, CSS

Cybersecurity Writeups *GitHub Repo*

- A personal repository documenting my hands-on learning in ethical hacking, penetration testing, and blue team techniques. It includes structured writeups and notes from platforms like TryHackMe and Hack The Box.
- Documented technical walk-throughs for TryHackMe rooms and CTF-style labs including recon, exploitation, privilege escalation, and post-exploitation.

Penetration Testing Report *GitHub Repo*

- Conducted end-to-end penetration testing on a remote machine by exploiting a web vulnerability and gaining reverse shell as part of a technical assessment for a cybersecurity company.
- Performed enumeration, vulnerability discovery, exploitation, and wrote a formal report documenting findings.
- Practiced technical documentation, risk communication, and reporting in line with industry expectations.
- **Tools used:** Nmap, Burp Suite, Netcat, LinEnum, SearchSploit

Skills

Languages: Python, C++, Java, HTML, SQL, CSS, LaTeX, JavaScript

Technologies: React, Flask, MySQL, Node.js, Microsoft Visual Studio, Git/GitHub, Microsoft 365 (Excel,etc.)

Operating Systems: Linux, Windows

Cybersecurity Proficiency

GRC & Compliance: Familiar with ISO/IEC 27001, NIST CSF, risk assessments

Penetration Testing: Metasploit, Burp Suite, Hydra, John the Ripper, Gobuster

Reconnaissance & Scanning : Nmap, Whois

Vulnerability Analysis : Burp Suite, Nikto, CVE research

Audit & Risk Tools : Nessus, Excel (audit logs), OpenVAS

Network Traffic Analysis : Wireshark, tcpdump

Security Frameworks : Familiar with MITRE ATT&CK, defense-in-depth principles, least privilege, and CIA triad

Cybersecurity Certifications & Competitions

Google Cloud Cybersecurity

- Completed foundational training in cloud security principles, including risk management, identity and access control, and securing cloud workloads on Google Cloud.

TryHackMe Advent of Cyber 2024

- Gained hands-on experience in ethical hacking and cybersecurity by completing daily practical challenges, covering topics like web exploitation, privilege escalation, and malware analysis.

Industrial Intrusion CTF Competition 2025

- Participated in a 48-hour red team Capture The Flag (CTF) competition simulating a real-world cyberattack on an industrial water control facility.
  - Engaged in offensive security tasks and digital forensics investigations to identify and neutralize advanced persistent threats in an OT (Operational Technology) environment
  - Solved practical challenges involving threat hunting, lateral movement, privilege escalation, and web portal exploitation
  - Collaborated in a team environment under time constraints, mimicking real-world incident response scenarios

ISC2 Certified in Cybersecurity (CC)

In Progress

- Preparing for foundational certification in security principles and access controls