ZACHARY ZHI

IT GRADUATE - Nov 2023

jczhi@hotmail.com ✉
0291247658 📱
zachary-zhi in

OBJECTIVE

A dedicated cybersecurity enthusiast. I am seeking an entry-level role as a **security analyst** or **penetration tester**.

EDUCATION

Cybersecurity Training and Certifications

- ISC2 Certified in Cybersecurity (CC)	*(Completed)*
- Google Cybersecurity Professional Certificate	*(Completed)*
- Splunk Security Operation and Defense Analyst	*(Completed)*
- Microsoft Security Operations Analyst Associate	*(Ongoing - Nov 2023)*
- INE Security Junior Penetration Tester (eJPT)	*(Ongoing - Dec 2023)*

Graduate Diploma (Computer and Information Sciences)

Auckland University of Technology (AUT)

Software Development / Network and Cybersecurity *Feb 2023 - Nov 2023*

(**GPA** 9.0/9.0 as of Aug 2023)

EXPERIENCE

Cybersecurity Projects

- Configuring and updating Microsoft Defender; Enabling and configuring Microsoft Firewall.
- Microsoft Active Directory: Configured groups and performed basic administrative tasks.
- Used Sysmon and Event Logs to detect and analyze malicious activities on Windows Server including identifying DLL hijacking. Used Event Tracing for Windows (ETW) to identify unusual parent-child relationships and malicious .NET assembly loading.
- Utilized TCPDump to capture and analyze TCP traffic. Used shell script for packets capture, and log PCAPs with filter expressions.
- Used Wireshark on Ubuntu to analyze HTTP/S and RDP traffic. Applied filters to detect a certain packet type, detect IP address related tasks.
- Splunk: Used Splunk to detect and analyze threats, perform continual monitoring like a SOC analyst. Finished the Splunk training course.
- VirusTotal: Investigated an email attachment by firstly retrieved the malicious file and create a SHA256 hash. Then used VirusTotal to uncover additional IoCs(indicators of compromise) that are associated with the file.
- Suricata: Used this open-source IDS, IPS and network analysis tool examined a rule which trigger alerts on network traffic and analyzed the log outputs.
- Python Automation: Used Python algorithm to automate updating the "allowlist.txt" file and remove IP addresses that should no longer have access.
- Capture The Flag (CTF): Challenges on ‘OverTheWire’ and CTF on ‘TryHackMe’ while update notes and writeups on Github.
- PortSwigger Web Security Academy labs: SQL injection, Authentication, Directory traversal, Command injection, XSS injection.

Branch Manager

Sichuan Airlines - New Zealand Branch *Feb 2017 - Dec 2022*

- Main Achievement and Problem-Solving skill:
  Demonstrated as facing the challenge of establishing and operating the new international route and New Zealand branch office from the ground up. I navigated issues such as regulatory hurdles, logistical challenges, route scheduling, human resources, airfare pricing and agencies cooperation etc.

Fleet Administrator

Sichuan Airlines - Head Office *Sep 2011 - Jun 2016*

- Main achievement: Managed and coordinated a fleet of 160+ aircraft, ensuring optimal utilization and compliance with all relevant regulations.

SKILLS

Programming:

- Java
- Python
- SQL
- Web Development - MERN stack (MongoDB/Express.js/React.js/Node.js)

Network:

- Basic knowledge (Protocols/IP Addressing/Ports/Routing/Switching)
- CCNA-3-v7 - Enterprise Networking, Security, and Automation

Windows:

- Defender/Firewall
- Active Directory

Linux:

- Basic commands and system administration

SIEM and other tools:

- Splunk
- Chronicle
- Sentinel
- VirusTotal
- Suricata

Network analysis:

- TCPDump/Wireshark

Pen-testing:

- Kali Linux/Recon/OSINT/Nmap/DirBuster/Enum4Linux/Metasploit
  Burp Suite/JohnTheRipper/Hydra etc.

INTEREST

Magic Performance

- A skilled magician, used to perform professionally on stage and close-up.

Video Editing

- Former paid video editor, possess a keen eye for detail and a creative flair.

Guitar Playing

- A campfire guitarist, enjoy playing guitar and sharing the joy of music.

VISA

NZ Resident Visa

Reference upon request