Kia ora, I'm
Tomais Williamson

hello@tomais.nz
+64 27 901 5179
https://tomais.nz/
SoftPoison

I'm a security consultant in Wellington, New Zealand.

I enjoy learning about both old and new technologies, and finding novel ways of exploiting them.

I am active in the Capture The Flag scene, representing Oceania at the International Cybersecurity Competition in 2023 where we placed second of seven. I am also an active and published security researcher with four credited CVEs and multiple vendor disclosures for a range of high and critical vulnerabilities.

I'm looking for a role where I can continue to upskill my offensive capabilities and perform security research into both emerging and well established technologies, and work to improve the security posture of organisations.

Education

2018 - 2020

Victoria University Wellington

B.Sc Computer Science and Mathematics

Research

Multiple issues in Kramer VIA GO2

- CVE-2023-33507
- CVE-2023-33508
- CVE-2023-33509

Privilege escalation in Accellion kiteworks

- CVE-2021-31585

Experience

NOV 2019 – PRESENT

ZX Security

Senior Security Consultant,
Research and Training Manager - ZX Security

This is my first excursion into the security industry, being hired as an intern, and working my way to becoming a senior consultant. In this role, I am able to work unaided on a wide range of pentesting engagements, as well as quickly upskill on any technologies and types of engagements. As a senior consultant I am capable of managing an engagement from start to finish, including scoping, writing the final report, and readout meetings.

As part of the Research and Training Manager role, I am responsible for the professional development and research plans of the staff in the pentest division, as well as tracking training budgets across the whole company. I also coach and mentor junior and intermediate staff to ensure that they are appropriately upskilling and supported through their career.

2019

Victoria University Wellington

Cyber Security Tutor

This was a part-time role as I studied at university. It involved tutoring first year students in cyber security (CYBR171) and marking assignments.

2017 – 2018

HiveTech

Developer

Between 2017 and 2018 I developed two proof of concept mobile applications for HiveTech which helped them garner a spot as a finalist in the 2018 Hi-Tech NZ awards

2017 – 2018

PortL Computer Services

Work Experience

In my final year of high school, I worked here part-time. I provided technical support for customers, such as installing new computer hardware and software, and I also developed custom websites and software.

References available on request

Kia ora, I'm
Tomais Williamson

hello@tomais.nz
+64 27 901 5179
https://tomais.nz/
SoftPoison

Key skills and competencies

Good communication

Whether it be meeting with clients and writing a representative statement of work, delivering the report to the client, or presenting findings to an audience, communication is a cornerstone of the work I do. Ensuring that my communication is clear and appropriate is a necessity.

Wide scope of knowledge

As part of being a senior, I have good working knowledge of many different areas of pentesting. This lets me perform a variety of tasks, from pentesting internal networks, segmentation scanning, physical device compromise and embedded systems, web applications, and some cloud engagements.

Able to manage others while getting work done

A large part of my work involves managing others, including helping them with their research and training plans, as well assisting with any technical questions. Being able to balance these things with my regular work is a strong point of mine.

High technical capability

As can be seen in my published research, my play as a member of CTF teams, and in my day-to-day work, I have high technical capability. I am able to understand subjects to a great depth, and crucially, explain issues to a large, technically varied, audience.

Programming languages and frameworks

I have good working knowledge of most popular programming languages, including C, C#, Rust, Go, Java, Javascript, and PHP, as well as many of their associated web application frameworks. I can both write and review code with a variety of static and manual analysis techniques, including CodeQL and SemGrep. I am extremely familiar with the OWASP Top Ten, as well as the MITRE frameworks.

Custom tooling

I have created and contributed on the following tools, out of curiosity and professional necessity:

- *Rustdump* – a tool for dumping the LSASS process, built in Rust, which successfully evades multiple AV implementations.
- *GoSnaff* – a fast multiplatform SMB looter built in GoLang to assist with finding sensitive files and documents in accessible SMB shares in an Active Directory environment.
- *Flaming Penguin* – an internet scanner for New Zealand's IP space, similar to Shodan, which collates details about each host such as open services, possible vulnerabilities, and HTTP screenshots.
- *Snazzy* – a speedy tool for pulling hidden credentials and interesting data out of Microsoft Azure.

References available on request