George Muscat

⊙ Sydney, Australia

✉ george@muscat.sh   ⦿ @georgemuscat   in George Muscat   ⊘ https://muscat.sh/

Experience

Security Engineer
Asontu

📅 July 2024. — Current   ⊙ Sydney, AUS

Security Engineering Consultant
- Prototyped, pitched and developed testing and deployment infrastructure using Rust, Python, Kubernetes and Git.
- Built vulnerability reporting tools, combining and cleaning multiple data sources using MySQL, Pandas and PowerBI.
- Architected, rolled out, maintained and used EDR and logging solutions including CrowdStrike, SentinelOne, NxLog and Google Chronicle in both Windows and Linux environments.
- Designed, reviewed and implemented secure networks. Diagnosed and fixed issues throughout the networking stack.
- Managed client relationships, enabling large organisations to complete new initiatives, while introducing security and reliability considerations to new design processes without added friction.

Casual Academic
UNSW

📅 Sep. 2022 — Dec. 2024   ⊙ Sydney, AUS

Course Administrator for ENGG1811 (Computing for Engineers)
- Managed 15 academic staff and coordinate over 350 undergraduate students per term.
- Responsible for setting up and maintaining course infrastructure, with technologies such as Linux (Debian Server), Bash, Python, PHP, Docker and CGI.
- Sole individual responsible for setting up and running exams in an in-house virtual exam environment.

Tutor for COMP6443 (Web Application Security)
- Taught students to discover, report and remediate discovered vulnerabilities.
- Vulnerabilities exploited and remediated include SQLi, XSS, LFI and SSRF.

Tutor for COMP1531 (SWE Fundamentals)
- Taught TypeScript, ExpressJS, CI/CD, Git Version Control, Docker Containerisation and Agile Development.

Education

Undergraduate
University of New South Wales

📅 2021 — 2024   ⊙ Sydney, AUS

B.Sc. Computer Science (Security Engineering) - Distinction

Projects

FuzzyWuzzy - An in memory resetting binary fuzzer

Designed for modularity and speed. Speed was achieved by creating a harness that hooks libc calls to provide coverage based mutations of inputs, as well as being able to reset the process being fuzzed without having to create new processes (reducing major overhead). This assignment received full marks. Source code can be found here https://github.com/GeorgeMuscat/fuzzywuzzy

sshnoop - A SSH hijacking tool

Written in Rust, sshnoop uses ptrace to intercept all data transmitted to an ssh session. Sshnoop also writes data to the ssh session using IOCTL. Source code can be found here https://github.com/GeorgeMuscat/sshnoop

Locked Shields 2024 & 2025 - NATO CCDCOE Wargames

Lead the Australian incident response team in a simulated cyberwarfare exercise organised by the NATO CCDCOE. Wrote custom bash/python scripts and EDR detections to manage and monitor over 150 endpoints running various versions of Linux and Windows. Other responsibilities included liaising with non-technical members and maintaining clear communication in a fast and stressful environment. https://ccdcoe.org/exercises/locked-shields/