George Muscat

Sydney, Australia

george@muscat.sh https://muscat.sh/ @georgemuscat George Muscat

Aspiring Security Engineer & Incident Responder

WHOAMI

Hello! I am recent graduate from UNSW with a Bachelors of Computer Science (Security Engineering).

While studying, I have spent the past year working at UNSW as a Casual Academic, where I get the most enjoyment teaching new CS students how awesome computers can be. In my free time I develop and participate in CTFs as a committee member of the UNSW Security Society. I enjoy attending conferences such as BSides and secEduCon, where I attended as a Speaker to discuss security education, an area I am extremely passionate about. I also enjoy blue teaming in attack & defence wargames such as the NATO run Locked Shields.

Much of my time is spent tinkering with technology, looking for ways I can improve the efficiency, usability and security of the tech. Reading is another huge passion of mine. Currently, I am reading "Distributed Systems" (Maarten van Steen & Andrew S. Tanenbaum) and I plan to start attempting practical implementations to solidify my understanding. Outside of tech, I spend the majority of my time playing team sports such as volleyball and football, in which I also volunteer to referee.

Experience

Casual Academic
UNSW

Sep. 2022 — Ongoing Sydney, AUS

- Course Administrator for ENGG1811 (Computing for Engineers):
  - Manage 15 academic staff and coordinate over 250 undergraduate students per term.
  - Responsible for setting up and maintaining course infrastructure, with technologies such as Linux (Debian Server), Bash, Python, PHP and CGI.
  - Sole individual responsible for setting up and running exams in an in-house virtual exam environment.
- Tutor for COMP6443 (Web Application Security)
  - Students to discover, report and remediate discovered vulnerabilities found in specially developed web applications. Students are taught to write reports that focus on remediation and explaining business impacts of the discovered vulnerabilities without overwhelming non-technical readers.
  - Vulnerabilities exploited and remediated include SQLi, XSS, LFI and SSRF.
- Tutor for COMP1531 (SWE Fundamentals)
  - Teaching TypeScript, ExpressJS, CI/CD, Git Version Control and Agile Development.
  - Member of the exam development and implementation team.

Cafe All Rounder
Northside Burgers + Gelatiamo

Apr. 2021 — Sep. 2022 Sydney, AUS

- Took pride in providing quality customer experience, often receiving praise from new and regular customers.
- Helped improve workflows and systems.

References available on request.

Education

Undergraduate
University of New South Wales

Feb. 2021 — May 2024 Sydney, AUS

B.Sc. Computer Science (Security Engineering) - Distinction
- HD in Web Application Security & Testing
- HD in Computer Science Project (Capstone)
- HD in Computer Networks & Applications
- HD in Object Oriented Design and Programming in Java
- HD in Solving Modern Programming Problems with Rust

Projects

Locked Shields 2024 - NATO CCDCOE Wargames

Lead the Australian incident response team in a simulated cyberwarfare exercise organised by the NATO CCDCOE. Used the EDR tool SentinelOne and wrote custom bash scripts to manage and monitor over 150 endpoints running various versions of Linux and Windows. Wrote detection S1QL queries to detect ATT&CK behavioural indicators, detecting and responding to incidents in various endpoint environments. Other responsibilities included liaising with non-technical members and maintain clear communication in a fast and stressful environment. https://ccdcoe.org/exercises/locked-shields/

FuzzyWuzzy - An in memory resetting binary fuzzer

This project was undertaken as a 4 person group for a university course. Our fuzzer was designed with modularity and speed as our main goals. Modularity allows a user to easily write new strategies for generating fuzzing inputs. 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

sshnoop was created from a personal need when blue teaming. Written in Rust, it parses strace to find all read syscalls intercepting all data read by an ssh session. The tool can also write data to the ssh session using IOCTL. I have used this tool when blue teaming to quickly hijack an attacker's ssh session, reading all the commands they were entering and being able to kill their session. Source code can be found here https://github.com/GeorgeMuscat/sshnoop

CTFs

COMP6443 Assessment CTF

As part of my university Web Application Security & Testing course, I completed a term long CTF which covered content such as SQLi, XSS, SSRF, CSRF, WAF Bypass and LFI. We also wrote a report that assessed business impact, risk and impact, steps to reproduce and remediation steps for each vulnerability that was discovered (available upon request).

DamCTF

Participated with UNSW Security Society and our team (K17) achieved 2nd out of 451 teams. My role in this was primarily a leader with broad experience in most fields who could connect individuals with specialised knowledge together to solve the most complex challenges. https://ctftime.org/event/1872

Rookie Code Rumble

Developed challenges for this CTF focused on introducing absolute beginners to the world of security. Made a challenge related to basic file system reconnaissance and a couple OSINT and puzzle challenges.

Analysis of common misconfigurations of WPA/WPA2 enterprise networks

I have observed that a lot of enterprise networks are not correctly issuing and requiring certificates to connect to access points. The risk of this is exacerbated by most organisations requiring users to use the same username and password to access the network and other infrastructure. The aim of this project was to complete a proof concept and a report detailing remediation, further recommendations, risks related to current implementation and a discussion of further avenues of research. I wrote a report about my findings, which I can provide upon request.

Spark - A platform for student society discovery

Lead Engineer in a team of 5, designed and implemented a NodeJS full-stack webapp for university students and societies using JIRA to aid Agile Development. Backend technologies include TypeScript, ExpressJS and Prisma ORM (sqlite). Frontend technologies include TypeScript, React and MUI. Presented as a MVP with an associated report (available upon request). Received a 97/100 overall mark and highest participation/contribution mark of 20/20. Source available on request.

Interests

- Reading
  - Recently, Distributed Systems (Maarten van Steen & Andrew S. Tanenbaum)
- Sports (Volleyball, Baseball, Skiing, Football)
- Teaching
- Strategy Games
- Meeting new people
- CTFs
- Reading security blog posts
- Attending security events such as SecTalks and BSides