George Muscat

Sydney, Australia

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

Aspiring Security Engineer & Incident Responder

Experience

Casual Academic
UNSW
Sep. 2022 — Ongoing Sydney, AUS

- Course Administrator for ENGG1811 (Computing for Engineers)
  - Manage 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 and CGI.
  - Sole individual responsible for setting up and running exams in an in-house virtual exam environment.
- Tutor for COMP6443 (Web Application Security)
  - Teach students to discover, report and remediate discovered vulnerabilities. Students are taught to write reports that focus on remediation and explaining business impacts of the discovered vulnerabilities.
  - 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.

Education

Undergraduate
University of New South Wales
Feb. 2021 — May 2024 Sydney, AUS

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

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 queries to detect MITRE 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

Designed with modularity and speed as the main design goals. 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 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

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.

A more detailed resume can be found at https://muscat.sh/resume/long.pdf