Noah Ostle

noahostle@gmail.com - +61 450 901 337
https://noahostle.github.io/noah/links

Skills

Certifications: Comptia Security+, Completed PortSwigger Web Security Academy

Can program in: C, C++, Java, Python, HTML/CSS/JS, NodeJS/Express

Experience in: Cryptography, Pure Maths & Number Theory, Malware, Application Security, IoT Security, Web Security, Theoretical Computing Science

Education

Macarthur Anglican - 93.15 Atar - Band 6 in; Math Adv (completed Ext 1), Software Development & Design, Info Processes & Tech

UTS - 90 WAM, 6.56 GPA, Dean's List **2024** & **2025**
Bachelor of Computing Science (Honours)
Maj. Cybersecurity & Networking
Graduation: Spring 2026

Industry Experience

Cybersecurity Analyst - Sydney City Council (04/2025 - Present)

- 2 year contract as a Purple Team CyberSecurity Analyst at Sydney Town Hall awarded by NSW govt. program.
- Experience dealing with CyberSecurity incidents and alerts, reporting, and root cause analysis/patching.
- Dealing with sensitive information and process improvement / scripting with confidentiality requirements.

Bug Bounty Hunter (01/2023-03/2025, Freelance)

- Bug bounty hunter on Hackerone

Harvey Norman Cybersecurity & IT department Work Experience (2023)

- Work Experience under the IT security team at Harvey Norman.
- Helped monitor the Crowdstrike console and write reports on malicious activity during the MoveIt vulnerability.

ASD Cybersecurity and Robotics Work Experience (2022)

- Educational program for high achieving STEM students in ACSC headquarters Canberra.
- Training provided by ASD based on real-world cybercrime case.
- Studied Web Security, Digital Forensics, and Operational Strategy to trace and hunt a cyber criminal.

Technical Experience

Malware: I am currently writing a research paper which I aim to get published, in which I design a novel architecture for **Bypassing Windows Defender** in order to deliver even heavily signatured payloads, such as those generated by *msfvenom*. The technique I have developed utilizes a shellcode execution that acts as a stager via a C2 Server, to execute arbitrary payloads via process injection entirely within memory, without malicious code ever touching the disk. This method is currently fully undetected by up-to-date versions of Windows Defender.

I have designed the delivery in such a way that there would have to be major changes in Defenders scanning methodology in order to detect the malicious payload, demonstrating a potential security issue with Defender even on modern Windows 11 systems. I also developed a simple exploitation framework that allows the C2 server and all the compiled executables to be generated via a one-click script.

Cryptography: I am currently studying cryptography at university, as well as self-studying both the mathematical concepts as well as the implementation vulnerabilities, and I plan to do my honours thesis, and potentially postgraduate research in this topic. I am currently making substantial progress on ‘Cryptohack’ an online CTF style cryptosystem hacking challenge, and have been rated top 10 weekly twice.

Web security: I am a skilled web security tester. I have found complex vulnerabilities in hardened web infrastructure of well known companies through Bug Bounty programs such as hackerone, and I have also completed every lab from the Portswigger Web Security Academy.

I have a lot of experience from CTF's and HacktheBox and have a good technical eye for bugs/misconfigurations. My extensive web knowledge lends itself to fast initial access in red teaming scenarios, and is often my strong suit in HacktheBox.

Application Security / Reverse Engineering: I have developed software using dll injection and the Win32 API in order to modify both the memory, and assembly code of games for the purpose of "cheating" in offline single player games. This process involves not only sophisticated methods of process injection to evade detections, and very low level C coding, but the complex task of analysing memory dumps, and reverse engineering oftentimes enormous and very complicated binaries using static analysis tools like Ghidra, and debuggers such as gdb, x64dbg and CheatEngine.

With the help of write-ups I completed the Ghost in the Shellcode CTF; "Pwnie Island", building my own proxy to manipulate the network traffic being sent to the game servers. I am also completing the MicroCorruption CTF to practice binary exploitation.

CTF's: I have competed and/or placed top 3 in several CTF's including CyberTaipan, CyberCX Hackathon, PeCan+, and have a good amount of experience in full exploitation scenarios involving a broad variety of methods of initial access and privilege escalation through HacktheBox (on which I am ranked #896 Globally with over 1M users).

Notable Projects: I have written;

- A **process injector** to allow cheating in the video game **'noita'** with sophisticated methods for modifying game code / memory in order to teleport, never die, fly, etc.
- **Maze Solver;** A web app that solves photos taken of mazes and displays the shortest path to the exit.
- **Pixel8;** A website that converts images to pixelart based on user inputted dimensions, can restrict the pixel colors to a persistently saved user inputted palette, and then give the user instructions to color it in.
- **Bet;** A sweepstakes website with secure admin login and a custom API in ExpressJS.
- **Dex;** A fully working mock social media website in ExpressJS with my own custom API.
- The netcode for a hobbyist videogame.
- Many other technical and computer science related projects. Code can be seen on my github *(see cover page).*

Academic/Research Experience

I am currently helping my Highschool Teacher by writing lab manuals and learning materials for the Cybersecurity Module of her year 11/12 Software Engineering Class. This is as part of the new NESA syllabus for Software Engineering.

I am in the process of publishing a research paper on an evaluation of Windows Defenders security, detailing the novel method of delivering malicious shellcode that I have created, which is fully undetected even with well known malicious payloads on up-to-date versions on Windows Defender.

Awards

2024 and 2025 UTS Dean's List

- The Dean's list recognises the top ~30 students from each year across the whole university
- Received this award two years consecutively for outstanding marks across all subjects taken.

NSW iAwards winner (2023)

- Recognises innovation and excellence in the tech industry.
- Awarded the NSW student category winner for a website that solves images of mazes.

ADF Future innovators award (2023)

- Recognising STEM high achievers with a $550 Prize - awarded for excelling in ASD Cybersec workshop.

PeCan+ 2022 3rd place

- Awarded with 6 months of PentesterLab Pro, despite competing alone against teams of 4.