Noah Ostle

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

Skills

Technical skills

Can program in: C, Java, Python, Js

Experience in: Web Security, Software Security, Reverse Engineering, Malware Development, Linux sysadmin.

Education

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

UTS - 86.7 WAM, Dean's List - Bachelor of Computing Science (Hons.), Maj. Cybersecurity & Networking

Technical Experience

Note: all examples of hacking mentioned have been done for educational purposes, within ToS, having minimal impact on other users, or with express permission from the device/service owner where applicable.

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 been paid. I have completed every lab from the Portswigger Web Security Academy available without a professional software licence.

I also have a lot of experience from CTF's and HacktheBox and have a very 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.

Reverse Engineering: I have developed sophisticated 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 process injection 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 learn binary exploitation.

Malware Development: Currently I am completing MalDev Academy in order to expand my red teaming skillset. I hope to build on the skills I gained using various low level Windows libraries for game hacking to learn how attackers evade antiviruses, and how antiviruses can get better at detecting malicious activity.

Networking: I am currently studying a sysadmin focussed Networking Servers unit, which is based on the coursework for the RedHat Certified Engineer (RHCE) certification, which I intend to complete once I finish this semester. I also have good knowledge of low level network engineering and administration, which I will continue to build on as I self study and finish my degree.

CTF's: I have competed and/or placed 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 and studying OSCP coursework (no certification).

Technical Experience (Cont.)

Notable Projects: I have made a mock cloud storage program, encrypting all data at rest, and hashing login information in C, as well as a website that solves photos taken of mazes, an image to pixel art converter with paint by number instruction capability, a fully working mock social media website, and the netcode for a hobbyist videogame among many other technical and computer science related projects for my degree, and for my own experimentation and learning.

Awards

2024 UTS Dean's List
- The Dean's list recognises the top ~30 students from each year across the whole university

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
- Responsible for the majority of my teams score (needed 4 people for a team, so some friends volunteered to compete with me).

Industry Experience

Bug Bounty Hunter (Freelance)
- Bug bounty hunter on Hackerone

ASD Cybersecurity Cadetship (Not hired)
- Passed skills/psychometric testing, and was accepted into the program, but was ultimately not hired because I study too far from Canberra.

Harvey Norman Cybersecurity & IT department Internship (2023)
- Work Experience under the IT security team at Harvey Norman.
- Experienced dealing with real world cyber threats, response, controls and infrastructure management (Crowdstrike, MITRE ATT&CK).

ASD Cybersecurity and Robotics Work Experience (2022)
- Educational program for high achieving STEM students in ACSC headquarters Canberra.
- Transport and accommodation paid for by ASD.