AARUSHI DWIVEDI

Austin, TX, (404) 416-3536, aarushidwivedi799@gmail.com, linkedin.com/in/aarushi-dwivedi

Education

Georgia Institute of Technology Aug 2021 – May 2023

Master of Science in Cybersecurity

Maharaja Agrasen Institute of Technology Aug 2017 – June 2021

Bachelor of Technology in Information Technology

Experience

Praetorian Security Inc, TX – Senior Security Engineer Oct 2024 – Current

- Lead complex cloud and web security engagements across AWS, Azure, and GCP, performing attack path mapping, full cloud environment analysis, and risk-informed threat modelling with clear technical and business-aligned recommendations.
- Develop and enhance internal security tooling (including the Nebula multi-cloud enumeration platform), contributing automation, methodology development, and proof-of-concept solutions using Python, Go and cloud-native services.
- Interpret and analyze threats and vulnerabilities across cloud, application, and network layers, leveraging security technologies and analytics to identify detection opportunities and strengthen client security posture.
- Collaborate with diverse stakeholders and mentor junior engineers while delivering high-quality findings, reports, and presentations across rapidly changing client engagements (every 2–3 weeks).
- Apply data analytics and experiment with **AI/ML techniques** to enhance detection logic, automate analysis workflows, and support cloud security use-cases.
- Build strong client relationships by clearly communicating technical risks, guiding remediation, and acting as a trusted security advisor.

Praetorian Security Inc, TX - Security Engineer Jun 2023 – Oct 2024

- Performed diverse security assessments, including **Android/iOS mobile testing**, foundational **web application reviews**, and **cloud configuration assessments** across major cloud providers.
- Identified vulnerabilities and misconfigurations, delivering **clear, risk-based reports** with actionable remediation guidance for both technical and non-technical audiences.
- Supported client teams during remediation and collaborated with senior engineers to refine testing methodologies and ensure high-quality engagement delivery.

Georgia Institute of Technology, GA – Head Graduate Teaching Assistant Jan 2022 – Dec 2023

- Instructor for CS6260: Applied Cryptography (Fall 2022, Spring 2023)
- Instructor for CS2600: Intro to Artificial Intelligence (Spring 2022)
- Responsibilities included holding weekly office hours, grading assignments and exams, and reviewing projects.

CSX Technology, FL – Security Infrastructure Technology Intern Jun 2022 – Aug 2022

- Performed proof of concept for Cloud security posture management solution for the company.
- Collaborated with GRC team for daily threat intel exercises, threat modelling, access control and security governance.
- Evaluated and deployed Microsoft Defender for cloud and worked with Azure, GCP and AWS.

Technical Skills

Concepts: Cloud Security · Threat Modelling · Attack Path Mapping · Incident Response · Vulnerability Analysis · Python · Go · Security Automation · AI/ML in Cybersecurity · AWS · Azure · GCP · Tool Development · Stakeholder Communication · Mentoring & Leadership

Research Publications

Obfuscation Based Security Protocol for Wireless Network – 3rd International Conference on Innovative Computing & Communications (ICICC) 2020.

Implementation of Machine Learning and Deep Learning Techniques in IoT Security – 4th International Conference on Innovative Computing & Communications (ICICC) 2021.

Projects

Nebula – A Modular and Efficient Open-Source Multi-Cloud Offensive Toolkit (Go): Co-developed with the cloud security team an offensive toolkit that enables rapid, automated enumeration and analysis across AWS, Azure, and GCP. Built modular components supporting cloud mapping, misconfiguration detection, and attack-path discovery, providing a scalable unified framework for multi-cloud security assessments.

Distributed System Security (Python): Developed a secure shared-store service enabling multi-user document storage and retrieval across distributed local machines.

Malware Analysis (Assembly, C, IDA Pro, Ghidra): Reverse engineered the Greencat malware, producing detailed documentation, control-flow graphs, and a custom def-use plugin for IDA Pro.

Advanced Keylogger & Backdoor (Python): Built a low-CPU-usage keylogger with extended capabilities and developed a Windows backdoor deployed from Kali Linux.

Active & Passive Information Gathering (Nmap, Kali Linux, Metasploit): Conducted reconnaissance on live websites and local environments, delivering comprehensive reports on findings and techniques.

Certifications

1. AZ900- Azure Fundamentals (Microsoft)