



AARUSHI DWIVEDI

Atlanta, GA, (404) 416-3536, aarushidwivedi799@gmail.com, adwivedi47@gatech.edu, [linkedin.com/in/aarushi-dwivedi](https://www.linkedin.com/in/aarushi-dwivedi)

Education

Georgia Institute of Technology, Atlanta, GA

Aug 2021 – May 2023 (Expected)

Master of Science in Cybersecurity

Relevant Courses: Binary Exploitation, Advance Malware Analysis, Secure Computer System, Network Security

Maharaja Agrasen Institute of Technology, New Delhi, India

Aug 2017 – June 2021

Bachelor of Technology in Information Technology

Experience

Georgia Institute of Technology, GA – *Head Graduate Teaching Assistant*

Jan – May 2023

- Responsibilities include holding weekly office hours, creating and grading assignments and exams, and reviewing projects about **symmetric and asymmetric schemes, and hashing algorithms**.

- Managing 3 TA's and a class of 120 students for CS6260: **Applied Cryptography**.

- Previous roles: Graduate Teaching Assistant for CS6260: Applied Cryptography (Fall 2022), CS3600: Intro to AI (Spring 2022)

CSX Technology, FL – *Security Infrastructure Technology Intern*

Jun – Aug 2022

- Performed proof of concept for **Cloud security** posture management solution for the company using Agile methodology.

- Collaborating 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.

Verzeo, Microsoft, India – *Intern*

Sept – Nov 2020

- Received **Certified Ethical Hacking** training. Researched and implemented web forensics tools and developed threat models.

- Performed **penetration testing** and reviewed violations of website security procedures and developed mitigation plans.

- Received in-depth experience with **vulnerability analysis** and common methods of exploiting vulnerabilities.

Defense Research and Development Organization (DRDO), India – *Intern*

Jun – Jul 2019

- Designed, implemented, and monitored their web portal, plugins, and functionality for continuous improvement and security of their web portal to replace their existing paperwork.

Skills

Concepts: Threat Modelling, Penetration Testing, Network & Web Security, Cryptography, Owasp 10, SDLC, Reverse Engineering

Software: IDA Pro, Nmap, Burpsuite, Ghidra, Windbg, Azure, Linux, Maltego, Proofpoint, Tableau, AWS, GCP, Jira

Language: Python, C, C++, Assembly, SQL, HTML, CSS, JavaScript, x86, x64 assembly

Soft skills: Leadership, Communication skills, Customer service, Problem solving, Agile methodology.

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

1. Distributed System security (*Python, Linux*)

Developed a Secure Shared Store service that allows for the storage and retrieval of documents created by multiple users who access the documents on their local machines.

2. Cloud watching (*Python, AWS, Azure, GCP, Nmap*)

Measured the abuse of Rapidly Changing Cloud IP Address. Analyzed 80,000 different IP addresses and taxonomized the most common types of abuse and the likelihood of allocating an abusable cloud IP address.

3. Malware Analysis (*Assembly, C, IDA Pro, Ghidra*)

Reverse engineered the whole Greencat malware in assembly. Implemented and prepared a detailed documentation of the malware, control flow graphs, and def use plugin in python for IDA pro.

4. Penetration Testing (*Nmap, Metasploit, Kali Linux*)

Exploited Bash vulnerability, Shellshock remotely. This project included network scanning using Nmap, attacking CGI program, creating a reverse TCP shell using Metasploit and using that for privilege escalation and password cracking.

5. Advanced Keylogger and Backdoor (*Python*)

Developed a keylogger with myriad of features keeping the CPU usage minimum and a backdoor in Kali Linux for Windows.

Certifications

1. AZ900- Azure Fundamentals (Microsoft)
2. Introduction to Cyber security tools and attacks – IBM (Coursera)
3. The complete Cyber security course: Hackers exposed! (Udemy)