Vishnupriya Ramesh

Atlanta, Georgia, United States
404-820-7374
vishnupriyaramesh12@gmail.com
linkedin.com/in/vishnupriya-ramesh-027102217
github.com/12Vishnupriya12/Cybersecurity

Personal Profile

I am a dedicated **2nd-year Master's** student pursuing an **MS in Cybersecurity** with a passion for securing digital assets and a strong foundation in cybersecurity principles, seeking a **summer internship** to apply academic knowledge and gain practical experience in the field.

Technical Skills

- **Cybersecurity Technologies:** Firewalls, IDS/IPS, VPNs
- **Network Protocols and Security:** TCP/IP, DNS, SSL/TLS
- **Operating Systems:** Windows, Linux, MacOS
- **Intrusion Detection and Prevention:** Snort, Splunk
- **Security Tools:** Wireshark, Nmap, Metasploit, angr, seccomp
- **AWS Services:** Lambda, API Gateway, S3, DynamoDB, Cognito
- **Reverse Engineering:** IDA Pro, Ghidra, GDB (GNU Debugger)
- **Programming and Scripting:** Python, Bash, PowerShell, C++/C, Java, HTML, PHP, Java
- **Security Frameworks:** NIST Cybersecurity Framework, CIS Controls, SIEM
- Strong analytical and problem-solving skills

Education

Master of Science in Cybersecurity and Privacy

Georgia Institute of Technology

Graduating in Fall 2024

Current CGPA: 3.63

Relevant Courses: Network Security, Advanced Malware Analysis, Computer Networks, Incident Response, Securing Internet Infrastructure, Secure Computer Systems, Applied Cryptography, Enterprise Cybersecurity Management

Bachelor of Technology in Computer Science and Engineering

Govt. College of Engineering, Kannur

Experience

- **Graduate Office Assistant**

  Graduate Living Housing, Georgia Tech *June 2023 - Present*

  - Demonstrated a strong commitment to data security by implementing and adhering to best practices for handling sensitive resident information and package tracking, ensuring data confidentiality and privacy.
  - Collaborated with the IT team to identify and address potential security vulnerabilities in package tracking and office systems, contributing to a more robust and secure environment.
  - Cultivated a keen eye for detail when verifying package information and resident records, reducing the risk of errors and ensuring accurate data handling, a crucial skill in cybersecurity.
  - Worked closely with colleagues to ensure a cohesive approach to resident support and information security, fostering teamwork and communication skills important in cybersecurity incident response and teamwork.

- **Internship in the area of 'Software Development in Java'**

  G-Media Computers, Calicut, India *June 2018*

  - Collaborated on Java-based software projects, applying best practices for development and maintenance.
  - Conducted code reviews, debugging, and optimization, ensuring code quality and efficiency.
  - Worked cross-functionally to meet project requirements and deadlines.
  - Gained proficiency in Java frameworks and contributed to documentation.
  - Participated in knowledge transfer sessions, promoting teamwork and innovation.

Project Portfolio

- **Capstone Research Project** (In progress)
  - Fortifying the security of GPT-4 against one of the top 10 OWASP vulnerabilities in LLMs, i.e. Training Data Poisoning

    - To create a security framework along the lines of a NIST document, involving a CVSS Model, tailored for GPT-4 which aims to provide organizations with explicit guidelines for risk assessment and management.
- **Serverless Photo Gallery Application**
    - Full Stack Development:
        - Developed a dynamic web interface using HTML and JS, seamlessly hosted on AWS S3 static website hosting, ensuring a responsive and user-friendly experience.
        - Implemented and configured AWS API Gateway endpoints and Lambda functions to enable robust application functionality, covering serverless architecture from front-end to back-end.
    - Secure Cloud Integration:
        - Utilized Amazon Cognito to manage user pools, ensuring secure and authenticated access to the serverless Photo Gallery Application.
        - Implemented comprehensive cloud storage solutions by configuring DynamoDB for efficient records management and S3 for hosting the static website and securely storing photos.
    - *Technologies Used:* AWS Lambda, API Gateway, S3, DynamoDB, Cognito
    - *Skills Demonstrated:* Cloud computing, serverless architecture, web development, AWS services integration.
- **Penetration Testing** in Bash
    - **Objective:** Conducted penetration testing to assess system security, focusing on common vulnerabilities and attack tools.
    - **Shellshock Vulnerability Exploitation:** Demonstrated hands-on experience in exploiting the Shellshock vulnerability to gain insights into its operation and potential impact.
    - Tasks **Accomplished:**
        - Conducted network scanning using nmap and netcat.
        - Executed the Shellshock attack on a remote web server with CGI scripts.
        - Established a reverse shell using Metasploit for remote command execution.
        - Explored privilege escalation through setUID vulnerabilities.
        - Conducted password cracking exercises to assess weak passwords.
    - **Tools Utilized:** nmap, netcat, Metasploit, Shellshock vulnerability exploitation.
- **Binary Exploitation:**
    - **Skills Demonstrated:** Buffer Overflow, ROP Chains, Use-After-Free Vulnerabilities
    - **Tools Used:** angr (crash analysis), ropper (ROP chain generation), pwntools (payload execution)
    - **Achievements:** Successfully exploited a binary, overcame DEP restrictions, worked with seccomp filtering
    - **Experience:** Hands-on application of binary exploitation techniques in a challenging environment.
- **Mini Internet Project:**
    - **Scope:** Implemented a mini internet project modeled after ETH Zurich's network architecture.
    - **Tasks:** Progressed through a series of five assignments aimed at creating and managing an autonomous system (AS) network:
        - Acquired knowledge in device interaction and network configuration
        - Completed tasks related to Intra-domain routing, Inter-domain routing, BGP Policies, and Security
    - **Skills Demonstrated:** Demonstrated network configuration, OSPF, BGP, network security, and route origin validation (RPKI) throughout the project.

Personal Projects

- **Log4j**/logging; JNDI/LDAP lookups
    - Hands on experience with the **Log4shell** exploit
    - Used **pwntools** for debugging
- **Capture the Flag** - solving exploits on binary programs
    - **picoCTF** (score of 4850)
    - Participated in **HackGT** organized by Georgia Tech in 2023
    - **Georgia Tech Grey Hat Club Member**
        - Actively participating in bi-weekly Capture The Flag (CTF) challenges, continuously enhancing practical cybersecurity skills and collaborative problem-solving.
    - Control flow hijacking using certain vulnerabilities in C programming
- Analysis of **Malware** behavior using **IDA Pro**
    - **Objective:** Conducted a focused analysis of the "greencat-2" binary to determine:
    - **Skills Demonstrated:** Malware analysis, cyber forensics, network traffic analysis.
    - Secondary Project: Analysis of Malware using Malheur
        - Clustering and classifying malwares
- Analyzing network traffic using **Wireshark** and packet captures (PCAP) reading
    - Man in the Middle exploit