Raghav Rathi

Phone: (850) 284-2292 | Email: raghav_rathi@outlook.com
https://raghavrathi10.github.io/

PROFESSIONAL EXPERIENCE

Cyber Security Engineer | Florida Department of Children and Families January 2025 - Present

- Security Operations Center & Incident Response – investigate and remediate security incidents in a SOC setting by leveraging Microsoft Sentinel (KQL), Microsoft Defender, SentinelOne, and threat intelligence from Recorded Future, integrating data from Intune and ExtraHop. Perform deeper malware analysis using Recorded Future sandbox and Kali Linux to potentially find the source of the attack.
- Automation and Tuning - Develop and optimize automation rules and playbooks in Azure Sentinel, continuously tuning analytic rules to enhance detection accuracy, improve SOC efficiency, and reduce analyst fatigue.
- Red teaming - Conduct continuous red team exercises, by utilizing Atomic Red Team Testing and deploying custom Caldera agents with advanced evasion techniques to bypass Microsoft Defender and Palo Alto XSIAM, identifying security gaps and improving defensive controls.
- Security awareness campaign - Led organization-wide phishing simulation campaigns to assess user security awareness and strengthen phishing detection and reporting capabilities.

Research Assistant | Department of Computer Science, Florida State University *August 2019 – December 2024*

- Capture signals from Starlink satellites to analyze the channel used by them. Funded by NSF
- Improved the channel capacity by 1.66x of existing LoRa networks by increasing the nof confirmed traffic in downlinks.
- Improved the packet detection capability in LoRa networks by introducing a technique to detect collided packets in uplink by 2.46× over the state-of-the-art. Funded by NSF

TECHNICAL SKILLS

Skills: Penetration Testing, Web Application Security, Malware Reverse Engineering, Digital Forensics, Static Analysis, Dynamic Analysis, Binary Exploitation, Cyber Forensics, Steganography, IDS/IPS, SEIM, DLP, Fuzzing, NIST Framework, Cyber Risk Assessment.

Tools & Software:
- *Security Tools & Platforms*: Microsoft Sentinel (KQL), Microsoft Defender for Endpoint, SentinelOne, Palo Alto XSIAM, ExtraHop, Recorded Future, Intune, Cisco ETD, Elastic (Kibana), Security Onion.
- *Penetration testing & Network Security*: Burp Suit, Nmap, Wireshark, Metasploit, John the Ripper, Hashcat, EnCase, Sleuth Kit, FTK Imager, SQLMap, Kali Linux, Commando VM, Procmon, Process Explorer, Ffuf, Dirb, DirBuster, Wpscan, Active Directory Domain.

-*Reverse Engineering*: IDA pro, Ghidra, radare2, GDB, GDBpeda, PwnTools.

Programming Languages: C, C++, MATLAB, Python, Arduino, SQL, MIPS, Git.

Other Tools: PyTorch, TensarFlow, Keras, Pandas, Docker, OpenCV.

Scripting Language: JavaScript, Bash, PHP, Powershell.

EDUCATION

Doctor of Philosophy in Computer Science · *Florida State University* *May 2020 – December 2024*

Master of Science in Computer Science - Cybersecurity Major · *Florida State University* *August 2017 – December 2019*

Bachelor of Science in Computer Science · *RGPV, India* *August 2012 – July 2016*

RESEARCH AND ACADEMIC PROJECTS

- **StarAngle: User Orientation using StarLink Beacons (Published)** *September 2023 – July 2024*
- **2-Pipe: Simultaneous Downlink Transmissions in LoRa (Accepted)** *April 2022 – August 2023*
- **TnB: Resolving Collisions in LoRa (Published)** *November 2021 – April 2021*
- **Intrusion Detection Using Deep Active Learning** *August 2019 – December 2019*
- **Malware Classification and Detection using Data Mining** *August 2018 – December 2018*

ACHIEVEMENTS AND INTERESTS

- Dean's Award for excellence in research and academics, 2023.
- Ted and Syauchen Baker Award for Excellence in Student Research, Fall 2023.
- Placed 1st in CyberCorps Division in 2023 JerseyCTF competition hosted by the NJIT.
- Former member of FSU Cybersecurity team (Nol3ptr).
- Soccer: Liverpool. Football: Jaguars.