Pranav Waghanna

Rochester, New York

pranav.waghanna@gmail.com | +1 585-537-9675 | Website | LinkedIn | Github

Education

University of Rochester, Master of Science in Computer Science — Aug 2024 – Dec 2025
- CGPA: 3.59/4.0
- **Coursework:** Computer Security Foundations, Collaborative Programming, Intro to Cryptography

Pune Institute of Computer Technology, Bachelor in Information Technology — Aug 2020 – Jun 2024
- CGPA: 8.19/10
- **Coursework:** Operating Systems, Computer Networks, Processor Architecture, Data Structures and Algorithms

Experience

Full Stack Developer, Huf India Pvt. Ltd – Pune, India — Jul 2023 – May 2024
- Led and managed a team of 8 engineers in developing a MERN stack application;provided real-time production data, enabling quicker decision-making.
- Integrated Ant-Design forms for streamlined data submission and automated task scheduling through cron jobs, decreasing manual data entry errors by **15%** and freeing up **10 hours per week** for plant supervisors.
- Leveraged ThingSpeak to store and retrieve data of produced items sent by ESP32 microprocessor. Utilized AWS EC2 instance to host the server along with Netlify for the frontend.
- Engineered role-based access controls enabling technicians to monitor production via CanvasJS dashboards, trigger automated maintenance alerts, and perform quality assessments, resulting in **15% fewer errors weekly**.
- Reduced the manual processing time of the internal work from **1 week to a few seconds** through digitization of documents and instant generation of graphs.
- Facilitated daily stand-ups and weekly reviews, improving team communication and reducing blockers, which accelerated overall development progress by **20%**.

Projects

eBPF System and File Access Monitor (GitHub) — Nov 2025 – Dec 2025
- Designed and implemented a kernel-level security monitor with eBPF (BCC) to trace critical syscalls, capturing 14K+ events in 32 seconds (447 events/sec) with zero event loss.
- Developed heuristic-based detection mechanisms for identifying suspicious file access, directory traversal, and sensitive port activity; flagged 404 malicious activities (2.8% of total events) in real time.
- Evaluated runtime overhead using syscall tracing techniques, identifying a 2x latency increase in 'ls' execution (0.015s to 0.031s) while maintaining a minimal CPU and memory footprint.

Houdini: VFS-layer Rootkit for FreeBSD (GitHub) — Sept 2025 – Dec 2025
- Implemented kernel-mode rootkit at the VFS layer, intercepting getdirents64() and process list VFS operations, hiding 6 files and processes.
- Evaded security tools by bypassing traditional syscall based monitoring using VFS function pointers, demonstrating deep kernel compromise and overcoming challenges with defined constants.
- Demonstrated expertise in kernel-mode programming on the FreeBSD operating system through VFS layer manipulation, investing 60 hours in rootkit design and implementation.

Skills

Languages: C++, C, Java, SQL, JavaScript, Python, Rust, HTML, CSS, Shell, Bash.
Technologies: MERN stack (MongoDB, Express, ReactJS, Node.js), nmap, Sockets, Cybersecurity, CAD, Cryptography, Computer Networks, Penetration Testing, Web Fuzzing, Footprinting, AWS(EC2, S3), Git, Unix, CAD

Publications

Effects of Adopting Industry 4.0 on a Manufacturing plant — Mar 2024

P. Waghanna, A. Reddy, S. Deshpande, S. Chavan, V. R. Jaiswal and V. Naranje

10.1109/ICRITO61523.2024.10522189