Prakshit Vikram Jain

412-641-9744 pvj@andrew.cmu.edu linkedin.com/in/prakshitjain
prakshit.me github.com/prakshitvjain medium.com/@prakshit

Education

Carnegie Mellon University Expected Dec 2027
Master of Science in Information Security *Pittsburgh, PA*

- **Relevant Coursework:** Introduction to Computer Systems, Hacking and Offensive Security, Cyber Risk Modeling

Anna University Aug 2022 to May 2026
Bachelor of Engineering in Computer Science *Chennai, TN*

Technical Skills

Programming Languages: C, C++, Python, x86 ASM, Bash
Reverse Engineering and Debugging: GDB, WinDbg, Ghidra, Valgrind, ASan
Exploitation and Offensive Security: pwntools, Metasploit Framework, Nmap, Burp Suite
Systems: x86-64 internals, TCP/IP, caches, memory allocators
Areas of Interest: Systems Security, Reverse Engineering, Binary Exploitation

Experience

Bitcot Technologies Pvt Ltd Dec 2024 to Mar 2025
Security Intern *Chennai, India*

- Engineered network hardening controls by implementing MAC binding and network segmentation, directly mitigating lateral movement risks.
- Configured Fortinet firewalls with SSL inspection and IPS/IDS policies to detect and block malicious network traffic.
- Conducted Gap Analysis for ISO 27001 and SOC 2 audits, identifying security control weaknesses and creating a Risk Register to prioritize remediation, reducing audit time by 40%.
- Managed Asset Labeling and Access Control implementation, enhancing physical security posture against onsite social engineering attacks.

Projects

Memory-Corruption HTTP Server (server-havoc) | *C, pwntools, GDB, Fil-C* GitHub

- Built an HTTP server from raw sockets in C with intentionally planted memory-corruption bugs: stack overflow, format string, integer overflow leading to heap overflow, use-after-free, double free, and out-of-bounds write.
- Developed a matching proof-of-concept exploit for each vulnerability using pwntools to validate the corruption behavior.
- Compiled the same source with Fil-C, a capability-based memory-safe C compiler, and compared undefined behavior in the baseline build against deterministic runtime fault isolation.

Dynamic Memory Allocator (malloc) | *C* Academic integrity policy - Available on request

- Built a dynamic memory allocator in C from starter code with an implicit free list, then added an explicit LIFO free list, segregated free lists by size class, footer removal on allocated blocks, and a better-fit search.
- Improved memory utilization and throughput over the baseline implementation, earning full score on the lab.

Autonomous Red Team Drop Box (rogue-pi) | *Network Penetration Testing* GitHub

- Built an autonomous drop box that tests enterprise network security when plugged into an exposed ethernet port, requiring no operator interaction once connected.
- Automated subnet discovery, port scanning, stealthy service scans, SMB enumeration, LLMNR/NBT-NS poisoning, and AS-REP roasting to simulate a real engagement.
- Collected the sensitive data gathered across these attacks to demonstrate the impact of each weakness.

Secure Password Vault (safex-vault) | *LAMP Stack* GitHub

- Built a password vault on the LAMP stack with security by design: password hashing, AES-CBC data encryption, and strict input validation.
- Used prepared statements throughout to prevent SQL injection attacks.

Linux Hardening Tool | *Python* GitHub

- Developed a Python automation script to audit and apply CIS Benchmark security configurations across Linux systems, distinguishing between automated and manual remediation requirements.
- Automated the configuration hardening process while documenting remediation coverage gaps for steps requiring manual review.

CTF Writeups and Blogs | *Medium* Medium

- Published technical writeups for DEADFACE CTF 2025, ScriptCTF 2025, and NahamCon CTF 2025, covering web exploitation, cryptography, forensics, and reverse engineering.
- Wrote additional unpublished writeups for Hack The Box machines and other CTFs.

Certifications

- **eJPT:** eLearnSecurity Junior Penetration Tester
- **Arch1001:x86** Open Security Training 2 (OST2)

Leadership

Co-founder and President | *CyberX, College Cybersecurity Club — MNMJEC*

- Co-founded a college cybersecurity club with 7 members, scaling membership to 70+ students within 2 months through targeted outreach.
- Organized and conducted technical workshops on defensive security practices, Capture The Flag (CTF) competitions, and practical cybersecurity skills development.

Event Lead | *Hackescape, COGNIT'25 (Annual Department Symposium) — MNMJEC CSE*

- Conceptualized and executed the "Secure the Flag" security competition (defensive-focused CTF variant) as the flagship event for the department symposium.