Mohammed Adnan Jakati

Interested in hands-on, high-impact work in computer security, with a focus on security research, and penetration testing.

New York, NY · (347) 798-5213 · adnanjackady@protonmail.com · github.com/jackhax · linkedin.com/in/adnanjakati

Education

Master of Science in Cybersecurity (GPA: 3.92/4) — New York, NY, USA
New York University — *Expected May 2025*
Courses: Application Security, Offensive Security, Applied Cryptography, Software Supply Chain Security

Bachelor of Engineering in Computer Engineering (GPA: 8.38/10) — Karnataka, India
KLE Technological University — *May 2022*

Technical Skills

Programming Languages: Python, C++, JavaScript, SQL
Frameworks and Libraries: Git, Flutter, Node.js, Flask, REST API
Cloud and DevOps: Amazon Web Services / AWS, Microsoft Azure, Docker, Kubernetes, CI/CD , Oauth, Lambda
Databases: MySQL, MongoDB, Firebase, NoSQL, DynamoDB
Threat Modeling: OWASP Top 10, CWE-25, Secure Code Review, Identity & Access Management
Security Tools: Ghidra, IAM, Wireshark, Metasploit, Nmap, Burp Suite, Splunk, pwntools, sqlmap, SAML, Hydra, Zap
Specialized Expertise: Reverse Engineering, Web Application Penetration Testing, Secure Code Review, Network Security

Work Experience

Offensive Security Researcher — New York, NY, USA
Center of Cybersecurity, New York University — September 2023 – Present

- Executed comprehensive static analysis on TP-Link Archer C20 firmware using Ghidra, mapping over 10,000 lines of assembly code, and uncovering 5 attack vectors.
- Reverse-engineered and decrypted over 10 configuration files by tracing execution flow and analyzing a shared library, successfully cracking DES-encrypted passwords using custom decryption scripts

Security Engineer — Bangalore, KA, India
Sony India — August 2022 – August 2023

- Built an early-stage Threat Detection and Response (TDR) system using honeypots and real-time monitoring, enabling instant detection of threats and reducing incident response time by 50%
- Designed and implemented an evasion attack system for vision models, generating adversarial samples that reduced classifier accuracy by up to 70% across 5,000+ test images.

Software Engineer Intern — Bangalore, KA, India
Alorb Technologies Pvt. Ltd. — January 2022 – May 2023

- Developed and deployed a Contactless Identity Access Management System (IAM) using Machine Learning and AWS, improving performance by 3x
- Improved system security posture by reducing code redundancy by 20% and enhancing access control mechanisms

Projects

Autonomous Recon Agent for HTB — March 2025 – April 2025
Python, Docker, LLM APIs (Groq/Ollama), Prompt Engineering, Red Team Automation — Demo GitHub

- Architected an autonomous LLM-powered recon framework that adaptively chained 40+ security tools based on discovered services, simulating red team reconnaissance at scale
- Hardened LLM output reliability through context-aware prompt tuning, structured validation, and misuse mitigation, enabling actionable triage across 15+ HTB targets

Honeypots and Threat Monitoring with Splunk — January 2025 – March 2025
Honeypot, Docker, Splunk, AWS Tunneling, WSL2, Network Security — GitHub upon request

- Deployed 2 vulnerable Docker web apps tunneled to AWS, capturing and analyzing 18,000+ logs over 60 days to identify 50+ real-world attacks from 20+ countries
- Developed 5 custom Splunk detection rules that reduced manual investigation time by 40% by flagging exploit signatures, brute-force attempts, and abnormal command sequences

Penetration Testing – Web-Based Media Player — September 2024 – January 2025
LFI, XSS, Stack Buffer Overflow, Structure Reversing, Cryptography Analysis, Linux, Privilege Escalation — Notes

- Uncovered 5 critical vulnerabilities, including LFI and Command Injection, through end-to-end testing of a production-grade web app and binary, achieving full RCE on all instances
- Leveraged Ghidra, gdb, and pwntools to exploit memory corruption and overwrite 2 `.got` entries, gaining root access via custom Python-based exploits
- Delivered a comprehensive 20-page report detailing findings, exploitation techniques, and mitigation strategies, enhancing the system's security posture