Tanishka Ganesh Mali

State College, PA | +1 (814) 280-6430 | tanishkamali114@gmail.com | LinkedIn | GitHub | Portfolio

Education

Penn State University, University Park Aug 2024–May 2026
Master of Science: Cybersecurity Analytics & Operations *GPA: 3.98*

Pune University Aug 2021–May 2024
Bachelor of Engineering: Computer Engineering *GPA: 3.56*

Work Experience

Penn State University Aug 2024–Dec 2025
Teaching Assistant, State College PA

- Facilitated weekly lab sessions for over **40 students** in Cyber 366, teaching **malware detection, analysis, and reverse engineering** using **Ghidra** and **IDA Pro**, resulting in improved student proficiency in static and dynamic analysis techniques.

Balbird Industries Jun 2023–Dec 2023
Vulnerability Management Intern, Pune IN

- Led ERP **vulnerability assessments** across **12+ modules** using **Nessus**, **OpenVAS**, and **OWASP ZAP**; remediated **DOM-based XSS** by replacing unsafe *JavaScript* functions and enforcing **input validation** and **CSP**, reducing exploitability by **40%**.
- Developed an **account lockout system** preventing brute-force attempts with a five-try threshold and 10-minute cooldown; piloted **2FA**, resulting in a **75% increase** in authentication security and a measurable decline in unauthorized login attempts.
- Ensured compliance with **IT Act (2000)** and **PDPB** by deploying secure password policies and lockout controls; applied **data minimization** to reduce log exposure by **60%**, lowering the risk of sensitive data leakage.

Keenhour (99 Digital) Feb 2023–May 2023
Software Developer Intern, Pune IN

- Improved application loading speed by **40%** through **code splitting** and **lazy loading** using **Webpack** and `React.lazy`, reducing initial bundle size and delivering noticeably smoother navigation for users.
- Streamlined data retrieval by implementing **Axios** with **exponential backoff** and **fallback mechanisms**, reducing API-related failures by **30%** and improving overall **application reliability**.

Competitions

INJ Cyber Competition (Incident Response Simulation) 2nd Place, 2025

- Performed incident response to detect **CVE-2021-4034** exploitation and credential abuse, recovering **59.6%** of compromised systems, identifying a **red team operator's IP**, and containing attacks across SSH, RDP, MySQL, and LDAP services.

Raymond James Intercollegiate CTF *[Best Team Spirit Award]* 8th Place, 2025

- Identified **S3 bucket misconfiguration** enabling transcript exfiltration, analyzed **RAG data-poisoning** vectors, and used **Python** to automate the "*Guess the Number*" challenge by scripting 1000 sequential correct guesses to obtain the flag.

DASSH Homeland Security Design Challenge [Github] 2025

- Built an **AI-driven log analysis and automated incident-response system** for DHS, using LLM-based log parsing, Wazuh-style correlation, and Python automation to cut false positives by **60–70%** and reduce response time from minutes to seconds.

iCTF–International Capture the Flag Competition 13th Place, 2024

- Solved **OSINT** & **prompt-engineering** tasks via **Overpass API**, and **decrypted an 8-bit PyTorch model** to restore functionality.

Certifications

CompTIA Security+ (SY0-701) [Badge]

- Demonstrated foundational cybersecurity proficiency, validating skills in **threat detection**, risk management, incident response, cryptography, **secure network architectures**, IAM, and compliance frameworks (NIST, ISO).

Projects & Published Research

Container Security Pipeline with Binary Authorization (GCP) [Github] Aug 2025–Nov 2025

- Built a **12-step Binary Authorization pipeline** on GCP using PowerShell, automating container build/push, KMS asymmetric key creation, Grafeas Note/Attestor setup, and attestation signing for supply-chain integrity.
- Applied and validated **GKE Binary Authorization policies** by enforcing digest and attestation checks, proving DENY for unsigned images and ALLOW for KMS-signed, attested images across repeated deployment tests.

CyberProbe–A PenTesting Framework [Github][Paper] Aug 2023–May 2024

- Built **CyberProbe**, a penetration-testing automation framework with **300+ modules** across **16 PTES categories**, supporting **x86/x64** detection, **32-bit/64-bit** tool selection, and **ASLR-compatible** installers.
- Implemented architecture-aware module execution, dependency handling, and update workflows, enabling reliable deployment of exploitation, post-exploitation, wireless, recon, and credential-attack tools across diverse Linux environments.

Skills

Cybersecurity: Threat Detection & Intelligence, Incident Response (IR) & Digital Forensics (Splunk, ELK, Wireshark, Autopsy, Volatility), Network Traffic Analysis, Vulnerability Assessment & Management (Nessus, OpenVAS, OWASP ZAP), Host Hardening & Firewall Configuration, IAM (SSO, MFA), Cryptography (SSL/TLS, Protocol Analysis), Supply Chain Security (Binary Authorization, KMS Signing, Attestations), Cloud Security (AWS IAM, GCP IAM), MITRE ATT&CK, OWASP Top 10.
AI/ML: Prompt Engineering, NLP, Data Analytics, LLMs (GPT, BERT), Model Training & Evaluation.
Development Tools & Cloud Platforms: Linux, Bash, Git, Docker, Kubernetes, CI/CD Pipelines, AWS, Azure, GCP, Jenkins, Jira.
Languages: Python, C/C++, SQL, Java, Assembly, JavaScript.