Twinkle Kamdar

tkamdar@andrew.cmu.edu | +1 (956) 278 4371 | Pittsburgh, PA | LinkedIn | GitHub

Work Authorization: Eligible to work in the U.S. from May 2026 under F-1 CPT

EDUCATION

Carnegie Mellon University **Pittsburgh, PA**

Masters of Science in Information Security (MSIS) **December 2026**

- Coursework: Introduction to Computer Systems (15-213), Introduction to Information Security, Network Forensics, Cloud Security, Security in Networked Systems, Advanced real world data networks.

Pandit Deendayal Energy University **Gandhinagar, India**

B.Tech. in Computer Science Engineering | CGPA: 3.8/4 **May 2025**

- Coursework: Cyber Security, Computer Networks, Information Security, Blockchain, Information Retrieval, Operating Systems, Internet of Things, Cloud Computing

EXPERIENCE

Silver Touch Technologies **Ahmedabad, India**

SOC Intern **May 2024 – July 2024**

- Performed vulnerability scanning and VAPT for enterprise clients using Nessus, Burp Suite, Metasploit, Kali Linux; triaged 50+ CVEs, documented risk exposure findings, supported incident containment and remediation.
- Led cross-functional collaboration with security teams to improve detection quality and operational effectiveness using threat intelligence frameworks.
- Monitored SIEM for alert triage, log analysis, and incident response; created and updated playbooks and incident documentation ensuring data protection and compliance.
- Conducted malware analysis and offensive security exercises including network reconnaissance and exploitation across Linux/Unix systems — supporting threat intelligence research and vulnerability remediation workflows.

PROJECTS AND RESEARCH

Autonomous Cybersecurity Intelligence System | Python, Kubernetes, ML, PQC | GitHub **Dec 2025 – Present**

- Independently architected a 3-layer ensemble ML voting IDS/IPS (Isolation Forest + Random Forest + Rule-Based) achieving 99% attack detection accuracy across 2.5M+ real network flows with autonomous threat blocking in <5ms.
- Engineered post-quantum cryptographic pipeline (Dilithium3 + Kyber768) with SHA-256 chained audit ledger, self-healing watchdog, NIST CSF-aligned incident response, and live SOC dashboard, fully autonomous, zero human intervention.

AWS Security Posture Scanner | Python, AWS, Click, Boto3 | GitHub **Feb 2026 - Present**

- Spearheaded development of CLI vulnerability scanner detecting 13+ S3 misconfigurations; generated severity-based JSON vulnerability reports for risk exposure management. Open-sourced, 1,680+ lines, CI/CD pipeline.
- Architected modular Python framework supporting scalable security checks across multiple AWS services with automated remediation guidance.

Abuse Detection & Media Forensics System **Jan 2025 – May 2025**

- Built media forensics platform using metadata analysis to detect inauthentic/manipulated content applicable to spam & abuse detection and platform trust & safety.
- Engineered content authenticity scoring pipeline integrating ExifTool metadata extraction with a Flask REST API classifying and flagging suspicious media submissions in real time with automated abuse signal detection.

SKILLS

Programming Languages: C | C++ | Python | Bash | JavaScript | Java | SQL | x86 Assembly | ARM

Offensive Security: Penetration Testing | Exploit Development | SQLi | XSS | CSRF | Web Application Security | Reverse Engineering | Buffer Overflow | OWASP Top 10

Tools: Burp Suite | Metasploit | Nessus | Wireshark | Suricata | Snort | Zeek | Elastic Stack | Security Onion | Falco

Cloud: AWS: EC2, VPC, S3, IAM, CloudTrail, CloudWatch | Kubernetes | Docker | Terraform | Ansible | CI/CD

Networking & OS: Linux/Unix | TCP/IP | BGP | OSPF | DNS | VLANs | OpenFlow | Wireless Networks | Packet Analysis

Security Frameworks: MITRE ATT&CK | OWASP | Sigma Rules | NSA/CISA | Zero Trust | Secure Architecture Design | Threat Hunting | Incident Response Vulnerability Management | Risk Exposure Management | Log Analysis | Malware Analysis | Playbook Development | Process Automation | Incident Documentation

Certifications: IBM Threat Intelligence & Hunting | Cisco Introduction to Cybersecurity