

NITHIN KUMMARI

+91 7569363011 | Mail: nithin.kummari1897@gmail.com |

LinkedIn: [linkedin.com/in/nithin-kummari](https://www.linkedin.com/in/nithin-kummari) | GitHub: github.com/NithinKummari

Portfolio: <https://nithinkummari.github.io/Portfolio/>

Career Objective

Cybersecurity professional with hands-on experience in threat detection, incident response, penetration testing, vulnerability management, and cloud security through internships, simulations, and academic projects. Skilled in using SIEM tools, offensive security frameworks, and defensive monitoring solutions to secure enterprise systems, and seeking opportunities in Cybersecurity Operations, Penetration Testing, Threat Intelligence, or Cloud Security to strengthen organizational defenses while continuously growing my expertise.

Education

Bachelor of Technology (B.Tech) – Computer Science Engineering (Cybersecurity)

St. Mary's Engineering College, Hyderabad | 2021 – 2025

Technical Skills

- **Security Operations & SIEM:** Splunk, Wazuh, Zeek, Wireshark, ELK Stack (Elasticsearch, Logstash, Kibana), Log Analysis, Security Event Correlation
- **Penetration Testing & Vulnerability Assessment:** Nmap, Metasploit, Burp Suite, Nessus, OSSEC, UFW Firewall, MITRE ATT&CK Framework
- **Incident Response & Threat Hunting:** Threat Detection, Malware Traffic Analysis, Phishing Analysis, Alert Triage, Escalation, Reporting, Root Cause Analysis
- **Identity & Access Management (IAM) & Zero Trust:** IAM Administration, Zero Trust Policies, Authentication Security, Access Control
- **Programming & Automation:** Python (Security Tools, Automation, Log Parsing), Bash (Linux Automation), SQL (Database Security Testing)
- **Operating Systems Security:** Linux (Ubuntu, Kali, CentOS), Windows (Server & Client), macOS (basic) – Hardening, Monitoring, and Access Control
- **Networking & Protocol Security:** TCP/IP, UDP, HTTP/HTTPS, DNS, DHCP, SSL/TLS, VPN, IDS/IPS Fundamentals, Packet Analysis
- **Cloud Security & Virtualization:** AWS Security (IAM, Security Groups), Docker (Container Security), VMware/VirtualBox

- **Governance, Risk & Compliance (GRC):** Vulnerability Management, Security Policies, Awareness Training, Incident Reporting
 - **Professional Skills:** Security Documentation, Technical Presentations, Collaboration with SOC/Blue & Red Teams
-

Professional Experience

Cybersecurity Intern – Pinnacle Labs (Jan 2024 – Mar 2024)

- Designed and implemented a Python-based keylogger to understand how malicious input capture works and developed countermeasures for prevention.
- Built a security alert chatbot using NLP tools to simulate automated incident notifications and improve SOC team awareness.
- Conducted password strength evaluations and enforced stronger policies to enhance authentication security.
- Developed testing scripts to identify weak login mechanisms and demonstrated mitigation strategies.
- Gained hands-on experience with Linux security administration, including system hardening and log monitoring.
- Documented findings in a technical report, ensuring reproducibility and knowledge sharing for future interns.

Key Skills: Python, NLP, Linux Administration, Security Automation, Authentication Security, Technical Documentation

Virtual Internships & Simulations (Forge Platform)

Mastercard – Security Awareness Simulation (Apr 2025)

- Investigated 50+ simulated phishing emails and identified common social engineering tactics.
- Built a phishing risk model to assess department-level exposure.
- Designed an awareness training framework with real-world phishing scenarios.

Key Skills: Phishing Detection, Security Awareness, Threat Analysis

AIG – Cyber Threat Intelligence Simulation (Jan 2025)

- Researched emerging vulnerabilities using CISA threat feeds and mapped them to MITRE ATT&CK tactics.
- Developed a Python automation script to simulate ransomware decryption key cracking.
- Compiled a threat intelligence report with risk ratings and mitigation actions.

Key Skills: Threat Intelligence, Python, MITRE ATT&CK, Malware Analysis

ANZ – Cybersecurity Management Simulation (Apr 2024)

- Performed email header analysis and reviewed attachments for phishing detection.
- Investigated PCAP traffic with Wireshark and Zeek, detecting brute-force and scanning attempts.
- Prepared an incident response report with SOC-level defensive recommendations.

Key Skills: Packet Analysis, Wireshark, Zeek, Email Security

TCS – Identity & Access Management Simulation (Apr 2024)

- Identified IAM gaps in a simulated enterprise environment.
- Proposed Zero Trust access policies aligned with NIST standards.
- Delivered a consulting-style report with an IAM maturity assessment.

Key Skills: IAM, Zero Trust, NIST Framework, Access Control

Projects

AI-Driven Threat Detection & Incident Response System (Zeek + Wazuh Integration)

- Designed and deployed a **network intrusion detection system** using **Zeek** to monitor real-time traffic and capture security logs.
- Integrated **Wazuh SIEM** with Zeek logs for centralized log management, **threat intelligence correlation**, and automated alerting.
- Configured Wazuh Dashboard (Kibana) for **visualization of security events**, including port scans, suspicious traffic, and authentication anomalies.
- Implemented **custom log parsing rules** to detect phishing attempts, brute force attacks, and malware traffic patterns.
- Automated **incident response workflows** for alert triage, threat containment, and remediation recommendations.
- Environment: **Docker, Linux (Ubuntu), Zeek, Wazuh, Elasticsearch, Kibana**

Key Skills: Network Security, SIEM, Log Analysis, Threat Detection, Incident Response, Docker, Linux Administration

Network Anomaly Detection with Wireshark

- Captured live **network traffic** and **applied filters** to spot unusual patterns.
- **Analyzed malicious packets** to understand attacker behavior.
- Documented anomalies and created SOC-style evidence reports.
- Applied TCP/IP knowledge to classify traffic as normal or suspicious.
- Simulated SOC incident escalation workflows.

Key Skills: Wireshark, TCP/IP, Threat Detection

Linux Firewall Setup (UFW)

- Configured **UFW firewall rules** to allow only safe connections.
- Hardened **Linux server** by restricting unnecessary ports and services.
- Tested firewall against **scanning tools** and **brute-force attempts**.
- Documented rule sets for repeatable deployments.
- Practiced defense-in-depth concepts with layered security.

Key Skills: Linux, UFW Firewall, Access Control

Flask-based AI Security Chatbot

- Built a **Flask web app** integrated with **OpenAI API** for a chatbot.
- Trained it to answer security-related queries and simulate SOC response.
- Implemented **NLP** features for realistic interaction.
- Deployed on a Linux environment for testing.
- Enhanced cybersecurity awareness through interactive learning.

Key Skills: Python, Flask, OpenAI API, NLP, Web App Development

Certifications

- Ethical Hacking Essentials – EC-Council
- Cyber Security Analyst – CareerX
- SQL Injection Attacks – EC-Council
- Network Performance Monitoring – Splunk
- Introduction to Ethical Hacking – Great Learning
- Forage Simulations – Mastercard, AIG, ANZ, TCS