

Nithin Yadav

Security Engineer | Offensive Security | Detection & Response

Bengaluru, India · 6363331908 · nithinyadavofficial@gmail.com

linkedin.com/in/nithinyadav-offensivesecurity · github.com/nithin-yadav-07

SUMMARY

Security engineer with hands-on identity and access management (JumpCloud), CASB (Netskope) and AWS experience, plus offensive security tooling in Python. Built an AI-driven SOC platform on Wazuh and a phishing-detection extension; finalist (top 5 of 650+) at a national hackathon.

EXPERIENCE

Security Engineer Intern | Wizowl Solutions

Sep 2026 – Present

- Administer identity and access management in **JumpCloud** for 20 employees and 35 devices: user lifecycle, group-based access policies, **SSO, MFA, device policies and LDAP/RADIUS**.
- Implemented and maintain **Netskope CASB** on **AWS** to monitor cloud app usage, enforce data-protection policies and flag risky or unsanctioned SaaS activity.
- Enforce least-privilege access through role-based groups and periodic access reviews.
- Investigate access anomalies and CASB policy alerts, and document remediation steps.

PROJECTS

Zitan Security: AI-Driven SOC Monitoring Platform | Wazuh, Cowrie, FastAPI, Qwen2.5, Twilio

- Built a SOC pipeline that collects system and web-server logs through **Wazuh** and passes them to a **local LLM (Qwen2.5)** to detect attack patterns.
- Implemented automated response that **blocks unauthorized deletion and copying of sensitive files**.
- Deployed a **Cowrie honeypot** and built a FastAPI dashboard with **2FA, JWT and RBAC**, a live log feed, AI-explained event details and **Twilio SMS/call alerts**.

CyberShield: Phishing & Spam Detection | Chrome Extension (Manifest V3), Web App

- Built a Chrome extension and web app that scans domains and emails and **blocks suspicious, phishing and spam domains and emails**.
- Scores links using **Levenshtein distance (typosquatting), brand-impersonation allowlists, blocklists, suspicious-TLD checks and urgency-keyword analysis**.
- Passed **43/43 test cases** in validation.

Vulnerability Scanner | Python, Nmap NSE, CVE/NVD

- Automated service discovery and CVE/NVD correlation to prioritize exploitable weaknesses, with structured remediation-oriented reports.

Recon Framework & Port Scanner | Python, Sockets, Multithreading

- Modular recon workflow (subdomain discovery, DNS enumeration, service fingerprinting) plus a from-scratch multithreaded TCP scanner with service/version detection.

TECHNICAL SKILLS

IAM & Cloud Security: JumpCloud, Netskope CASB, SSO, MFA, RBAC, LDAP/RADIUS, AWS

Detection & Response: Wazuh, Cowrie honeypot, log analysis, LLM-assisted threat detection

Offensive Security: Penetration Testing, Vulnerability Assessment, Web & Network Security, Reconnaissance, Active Directory Attack Paths

Tools: Nmap, Burp Suite, Metasploit, Kali Linux, Wireshark

Programming: Python, Bash, Docker, FastAPI, REST APIs

CERTIFICATIONS

- CEH v13** – in progress, targeting December 2026

ACHIEVEMENTS

- Finalist (Top 5 of 650+ participants nationwide)** – Jain National Hackathon, Tech for Agriculture, with IBM

EDUCATION

Bachelor of Computer Applications (BCA), Cybersecurity – SSMRV College, Bengaluru

Expected 2027