GIRIDHARAN K

+91 79042 39322 | giridharank790@gmail.com|giridharank.netlify.app| github.com/nextboxis |
linkedin.com/in/giridharan-k1315 | india,Tamilnadu selam

PROFESSIONAL SUMMARY

Front-End Developer and cybersecurity enthusiast with hands-on experience building secure, responsive web interfaces using React.js, JavaScript, and Bootstrap. Completed 40+ practical cybersecurity labs on TryHackMe (Global Top 260K, 8 Badges) and virtual job simulations with Tata (IAM) and Telstra (Incident Response). Proficient in OWASP Top 10, MITRE ATT&CK, and application security best practices. Seeking an entry-level Software Developer or Application Security Analyst role.

TECHNICAL SKILLS

FrontendDevelopment: HTML5, CSS3, JavaScript (ES6+), React.js, Bootstrap 5, Responsive Web Design, DOM Manipulation

Backend&Development: Python, Flask, MongoDB, WebSocket / Socket.IO, Server-Sent Events (SSE), REST APIs, Git, GitHub,Linux CLI, Docker, CI/CD, VS Code

Cybersecurity Tools: Nmap, Burp Suite, Wireshark, Kali Linux, Metasploit, SQLmap, Scapy, TShark, PCAP Analysis & Forensics

SecurityConcepts: OWASP Top 10, MITRE ATT&CK Framework, XSS Prevention, Penetration Testing, SOC Analysis, Threat Hunting,Threat Intelligence, IAM / RBAC, Incident Response

MachineLearning: scikit-learn (RandomForest Classifier), NVD CVE API Integration, Shannon Entropy / DGA Detection

Soft Skills:Problem Solving, Analytical Thinking, Communication, Continuous Learning, Active Listening

P R OJECTS

NexShield — AI-Driven Cybersecurity Dashboard | Python / Flask / MongoDB / scikit-learnOct 2025 – Feb 2026
GitHub: github.com/nextboxis/NexShield

- Architected a full-stack cybersecurity dashboard that automates network reconnaissance with Nmap, scans 28+ sensitive service signatures, and maps discovered vulnerabilities to MITRE ATT&CK techniques.
- Designed a 9-engine threat analysis pipeline covering port risk scoring, version vulnerability matching (Log4Shell, Heartbleed, SambaCry), and default credential detection.
- Trained a RandomForest ML classifier (scikit-learn) on synthetic exploit profiles to predict threat severity; integrated the NVD CVE API with 7-day MongoDB caching to reduce redundant API lookups by ~80%.
- Implemented real-time WebSocket (Socket.IO) push events with token-based authentication, composite host risk scoring, and one-click CSV/JSON threat report exports.

DNS Sinkhole — Real-Time DNS Threat Surveillance Platform | Python / Flask / Scapy / TShark / MongoDBDec 2025 – Mar 2026
GitHub: github.com/nextboxis/DNS-Sinkhole

- Developed a real-time DNS traffic interception and threat surveillance platform with Scapy and TShark dual-engine packet capture.
- Engineered a threat intelligence layer detecting DGA (Domain Generation Algorithm) domains via Shannon entropy analysis, DNS tunneling patterns, and suspicious TLD identification.
- Built multi-protocol detection supporting DNS-over-TCP, DNS-over-TLS (DoT), DNS-over-HTTPS (DoH), and DNS-over-QUIC (DoQ), with live Server-Sent Events (SSE) for real-time browser updates.
- Implemented PCAP drag-and-drop forensic replay, row-level CSV/JSON export, and MongoDB persistence with graceful in-memory fallback for offline environments.

EXPERIENCE & VIRTUAL JOB SIMULATIONS

Cybersecurity Analyst Job Simulation | Tata Consultancy Services via Forage Jan 2026

- Analyzed enterprise IAMarchitecture and recommended access control improvements using RBAC and least-privilege principles, reducing simulated attack surface.
- Documented 3 risk mitigation strategies derived from real-world security breach case studies, aligned with ISO 27001 best practices.
- Produced a structured IAM security assessment report mapping identified access control gaps to business risk, simulating SOC analyst deliverables.

Cybersecurity Job Simulation | Telstra via Forage Dec 2025

- Triagedsimulated security incidents and identified malware propagation patterns across multiple network segments using SIEM-style log correlation.
- Reconstructed the full attack timeline — from initial intrusion vector to lateral movement — using log analysis and forensic investigation techniques.
- Produced post-incident reports detailing attack vectors, affected assets, and remediation steps in line with incident response frameworks.

Cybersecurity Practitioner (Self-Study) | TryHackMe Present

- Completed40+hands-onlabs covering network enumeration, web application exploitation, privilege escalation, and OSINT.
- Earned 8 achievement badges; ranked in the global top 260,000 out of 3M+ platform members.
- Operated offensive security tools — Nmap, Burp Suite, Metasploit, and Kali Linux — in legal CTF and lab environments.

EDUCATION

B.Sc. Computer Science & Applications | Kongu Arts and Science College, Bharathiar University2023 – 2026 (Expected)
Aggregate: 70% | Relevant Coursework: Computer Networks, Operating Systems, Data Structures, Database Management

CERTIFICATIONS

Cybersecurity Analyst Job Simulation — Tata Consultancy Services via Forage Jan 17, 2026

IAMFundamentals | IAMStrategy| CustomIAM Solutions | PlatformIntegration

Cybersecurity Job Simulation — Telstra via Forage Dec 28, 2025

MalwareResponse | AttackAnalysis | Mitigation | Incident Postmortem

Linux Unhatched — Cisco Networking Academy Mar 12, 2026

Credential: Linux command line proficiency, system navigation, and user management