BHARATHKUMAR N

Avinashi, Tiruppur, Tamil Nadu
Phone: 9344128641 — Email: bharathkumarnatarajan6@gmail.com
LinkedIn: linkedin.com/in/bharath-kumar-n-8904512a1

Professional Summary

Early-career Computer Science (Cybersecurity) student with strong foundations in Python, SQL, networking, and system automation, and hands-on experience building data collection, monitoring, and alerting tools. Interested in data pipelines, backend systems, and infrastructure engineering, with a focus on reliability, observability, and scalable data platforms.

Technical Skills

Programming & Scripting: Python, Java, SQL

Data & Backend Foundations: Data collection pipelines, structured data processing, logging, automation scripts, CSV/JSON handling, basic query optimization

Systems & Networking: Linux (CLI), TCP/IP fundamentals, DNS, ports & services, network traffic analysis

Security & Tooling (Infra/Data Relevant): Nmap, Burp Suite (basic), Metasploit (basic), WhatWeb, service enumeration, system monitoring

Concepts: Data ingestion, observability, fault detection, system reliability, automation, version-based vulnerability mapping

Projects

PortGuardian – Port Watch & Alert Automation Tool
Python

- Built a Python-based monitoring system to continuously scan system ports and detect unauthorized changes.
- Implemented timestamped logging to track historical port-state data for audit and analysis.
- Automated alert generation and daily email reports, simulating real-world infrastructure observability pipelines.
- Applied concepts relevant to infrastructure monitoring, reliability engineering, and automated data workflows.

DNS Record Finder for Bug Bounty
Python, DNS, WhatWeb

- Developed a tool to collect and structure DNS records (A, MX, TXT, CNAME) as part of an automated data-gathering pipeline.
- Integrated technology fingerprinting to extract backend stack and version metadata from target domains.
- Enabled version-based CVE lookup, demonstrating structured data enrichment and downstream analysis.
- Modeled a real-world data ingestion and enrichment pipeline used in security and platform analytics.

CyberSentinel – Unified Network & Application Monitoring
Python, Networking

- Designed a modular system to collect, normalize, and analyze network and application-level signals.
- Implemented service enumeration and open-port detection modules to generate actionable system insights.
- Focused on data-driven monitoring aligned with backend observability and platform health use cases.

Internships & Practical Experience

Cybersecurity Intern
Hackup Technologies — June 2025 – July 2025

- Performed vulnerability scanning and network analysis, collecting and interpreting system data.

- Assisted in analyzing scan outputs and translating findings into structured technical reports.

- Gained hands-on exposure to real-world systems, tooling, and operational workflows.

Cybercrime Investigation Intern
Cybercrime Unit — June 2025 – August 2025

- Assisted in cybercrime case analysis, including digital fund-tracking workflows.

- Supported domain monitoring and data correlation, reinforcing investigative data analysis skills.

- Observed how large datasets are used in forensic and investigative pipelines.

Certifications & Workshops

- Smart India Hackathon (SIH) 2024 – Drones & Technology Track

- DRDO Sponsored Workshop: Cyber Threat Detection Using Deep Learning

- CSIR Sponsored Seminar: In-Vehicle Intrusion Detection Systems & Security Challenges

Education

Bachelor of Engineering – Computer Science Engineering (Cybersecurity)
Dr. N.G.P. Institute of Technology — 2023 – 2027
CGPA: 8.39

Higher Secondary Certificate (HSC)
Kongu Kalvi Nilaiyam Matriculation Hr. Sec. School — 2021 – 2023
Score: 88.3%