MERVIN SUMITH SEQUEIRA

Mangaluru, Karnataka | mervinsequeira485@gmail.com | +91 8861265255 | linkedin.com/in/mervin-sequeira-438a033b1/ | github.com/m0vi0

PROFESSIONAL SUMMARY

B.E. CSE (AI & ML) graduate with hands-on experience in network monitoring, protocol analysis, and multi-node infrastructure administration. Deployed and operate a distributed Wazuh SIEM across heterogeneous devices (Linux, Raspberry Pi 3B+) — managing agent deployment, syslog ingestion, and custom detection rules for network threat visibility. Built a real-time 3D network traffic visualizer using Scapy for live packet capture and analysis. Strong foundation in TCP/IP, wireless networking, and Linux systems.

SKILLS

Networking & Protocols
TCP/IP, DNS, DHCP, subnetting, packet analysis (Scapy, Wireshark), VPN (Tailscale), network enumeration (Nmap), wireless monitoring (Kismet monitor mode)

Network Monitoring & SIEM
Wazuh SIEM administration (manager + multi-node agent deployment), log correlation, custom detection rule authoring, alert triage, false-positive tuning, syslog forwarding

Infrastructure & Systems
Linux administration, Raspberry Pi deployment, heterogeneous device management, Docker, uptime/health monitoring (Netdata, Uptime Kuma)

Security Fundamentals
Firewall concepts, access control, vulnerability awareness, endpoint security, Active Directory concepts

Scripting & Development
Python (Scapy, network scripting), Bash, React, TypeScript, Node.js, PostgreSQL

EXPERIENCE

Network Monitoring & Infrastructure (Self-Directed Home Lab)
Independent Lab Environment | 2025 – Present

- Deployed a multi-node Wazuh SIEM (manager + 2 agents) across heterogeneous devices — an HP laptop running Linux and a Raspberry Pi 3B+ — managing agent enrollment, syslog ingestion, and certificate-based secure communication
- Authored and tuned custom Wazuh detection rules for wireless deauthentication-flood attacks, piping Kismet alerts into Wazuh via syslog and reducing false-positive alert volume by 40% through threshold tuning
- Performed ongoing log analysis and alert triage across the SIEM, investigating anomalies across multiple networked nodes and documenting findings for incident visibility
- Deployed proactive network and service health monitoring (Netdata, Uptime Kuma) across all nodes, maintaining continuous uptime visibility and automated alerting

Independent Security Researcher
Bug Bounty Programs (Bugcrowd) | 2025 – Present

- Identified and reported an unauthenticated production API endpoint exposing internal payment metadata for OYO Rooms; validated across multiple hotel IDs and payment modes, producing a reproducible PoC
- Conducted passive recon and asset enumeration for targets including OSL, Foot Locker, and TNSI using subfinder and ffuf, mapping attack surfaces through automated fingerprinting

PROJECTS

PacMap — Real-Time 3D Network Traffic Visualizer
React, Three.js, Python, Scapy | github.com/m0vi0/pacmap

- Built a real-time 3D network traffic visualizer with live packet ingestion, pcap replay, and graph-based path tracing — demonstrating Python scripting and network protocol analysis skills
- Implemented packet capture and parsing with Scapy, extracting IP headers and protocol metadata to drive 3D visualization of network flows

Multi-Node SIEM Infrastructure
Wazuh, Raspberry Pi 3B+, Linux | 2025

- Architected a distributed SIEM environment with Wazuh manager on a primary machine and agents deployed to a Raspberry Pi 3B+ and an HP laptop, achieving cross-device log correlation and centralized alert visibility

TECHNICAL TRAINING

- Comptia Network + in progress
- Hack The Box Academy CPTS Path — Network enumeration, web exploitation, shells & payloads, pivoting/tunneling, Windows/Linux privilege escalation (in progress)
- PortSwigger Web Security Academy — Completed labs covering access control bypasses and request manipulation
- TryHackMe / OverTheWire Bandit / Gandalf — Completed core web, Linux, and troubleshooting-focused challenge tracks

EDUCATION

B.E. in Computer Science & Engineering (AI & ML)
Sahyadri College of Engineering & Management, Mangaluru, Karnataka | 2022 – 2026 (Graduated)