Bennet Sharwin

Cybersecurity Enthusiast • Network Security • Linux Security • Threat Detection

bennetsharwin76@gmail.com 7994026917 Kerala, India linkedin.com/in/bennetsharwin

Summary

Ambitious cybersecurity practitioner with hands-on experience in log analysis, System security, network monitoring, and investigative troubleshooting. Built security automation and detection tools for file integrity monitoring and log forensics. Comfortable documenting findings, triaging alerts, and supporting incident response workflows. Seeking an roles to contribute analytical skills and practical tooling experience.

Skills

Security Operations: Log Analysis, Event Triage, Incident Documentation, IOC Review, Alert Investigation
Monitoring & Detection: Zeek Logs, Linux Audit Logs, File Integrity Monitoring, Baseline Monitoring
Scripting & Automation: Python (log parsing, alert automation), Bash
Networking: TCP/IP, DNS, HTTP/S, Ports & Protocols, Packet Inspection

Projects

Tor-based Encrypted Chat Application

- Designed and implemented an end-to-end encrypted chat application routed over the Tor network and secured with TLS to ensure confidentiality and anonymity.
- Integrated TLS certificate handling, secure session setup, and onion-routing configuration to protect metadata and message content.
- Tested for possible anonymity leaks, evaluated traffic patterns, and applied mitigations to reduce fingerprinting risks.
- Documented deployment steps, threat model, and forensic artifacts to support security investigations and operational handover.

File Integrity Monitoring System

- Created a Python-based FIM using SHA256 hashing to detect unauthorized file changes on Linux systems.
- Automated Jira ticket creation for alerts to simulate SOC workflows and support incident tracking.

Network Forensic Log Analysis Toolkit

- Parsed Zeek logs with Python and Pandas to extract connection metadata, protocols, and anomaly indicators.
- Identified suspicious patterns (port scans, unusual user agents, repeated failed connections) for further investigation.
- Produced visualizations and concise forensic summaries to support alert triage and incident analysis.

Network Reconnaissance & Host Enumeration Tools

- Built Scapy and Nmap based tools for host discovery, port enumeration, and service fingerprinting.
- Used scan baselines to detect unexpected services and potential exposure relevant to threat hunting.
- Documented findings in an incident-report style suitable for SOC processes.

Secure Web Application Hardening

- Hardened a Flask application by setting protections against XSS, CSRF, and SQL injection.
- Added Cloudflare Turnstile to reduce automated abuse and improve authentication resilience.

Tools & Technologies

Nmap, Burp Suite, Wireshark, Zeek, Scapy, Linux, Python, Bash, Docker, Git, Jira, n8n, AWS (EC2, VPC, IAM), Azure, MongoDB, Redis, Cloudflare Turnstile, HTML/CSS/JS, Node.js, TLS/SSL, YARA, Sigma, IDS/IPS, VPN, Firewalls, OSINT Tools

Education

Higher Secondary — Computer Science 2023 – 2025
Kerala, India

Languages

Malayalam (Proficient) — **English (Proficient)**