Jayaraj Patil

SOC Analyst | Cybersecurity Researcher | Python Network Defender

+91 7349426572| jayarajvp2005@gmail.com | LinkedIn | GitHub | Website

Address 30, 22 main D cross Pipeline Road JC Nagar Kurubarahalli Bangalore Karnataka India pin-code 560086

PROFESSIONAL SUMMARY

Entry Level SOC Analyst with hands-on experience in IDS/IPS deployment, firewall configuration, and log analysis using IBM QRadar. Experienced in developing network security scripts and simulating malware for testing and defines evaluation. Proficient in detecting and mitigating threats through SIEM-based monitoring and incident response. Published a research paper on mobile browser vulnerabilities covering phishing, clickjacking, and fingerprinting, tracking.

EDUCATION

Seshadripuram Arts, Science & Commerce College, Bengaluru Bachelor of Computer Applications (BCA) — *CGPA: 9.14*

Awarded 4 subject-level excellence certificates for academic excellence. Active member of Chathurya – Developers Club and Pragnya Science Forum, contributing to workshops, coding contests, and tech events. Demonstrated leadership and teamwork through active campus participation.

TECHNICAL SKILLS

Security & Analysis: Network Security, Threat Detection, Incident Response, Vulnerability Analysis, Penetration Testing, ARP Spoofing, Firewall Rules, Log Analysis, Ticketing

Tools & Platforms: QRadar, Burp Suite, Metasploit, Nmap, Wireshark, Scapy, VMware, WSL

Operating Systems: Windows, Ubuntu, Kali Linux

Networking: TCP/IP, DNS, Network Troubleshooting

Programming & Reporting: Python Scripting, C Programming, Research Reporting

CYBERSECURITY INTERNSHIP

1. **Research Paper: *"Analysing Security Vulnerabilities in Mobile Browsers"– Seshadripuram College* | *Dec 2024 – Mar 2025***

Conducted 25+ hands-on experiments to evaluate mobile browser risks like phishing, clickjacking, fingerprinting, and tracking. Used 100+ real phishing URLs from the PhishTank dataset, custom attack pages, and Python scripts for controlled testing. Analysed browser behaviour across 4 major platforms and proposed 5+ key security improvements to enhance user protection. Findings were compiled into a published research paper aimed at strengthening browser defences against real-world threats.

PROFESSIONAL EXPERIENCE

Freelance IT and network Support – *ImagineHealthcare, Karnataka* | *Dec 2024 – May 2025*

Provided secure remote and onsite support, configuring systems, routers, and DR setups. Integrated medical imaging tools with diagnostic hardware, ensuring data integrity and secure access. Maintained technical documentation and asset tracking with basic log checks for endpoint visibility. Assisted in troubleshooting network issues and implementing basic security practices to reduce system vulnerabilities.

PROJECT EXPERIENCE

1. **Firewall Log Analyzer Python:** Engineered a robust real-time firewall log monitoring tool using real-world log files from sources like Windows Defender. Processed 10,000+ entries daily with 50+ rule-based filters to detect intrusions, anomalies, and policy violations. Generated actionable, timestamped alerts—boosting SOC response time by 60% through intelligent parsing and threat classification.
2. **Intruder Detection System IDS:** Led a team of 3 to develop a packet-based Intrusion Detection System using Scapy and Python, deployed for real-time monitoring in Seshadripuram College lab. Inspected 5,000+ packets/hour by analysing IP headers and payloads to detect unauthorized access and protocol misuse. Achieved over 90% detection accuracy on test datasets, significantly improving network visibility and early threat detection.
3. **Advanced Network Packet Sniffer:** Collaborated with a team of 4 to develop a robust deep packet inspection sniffer using Python, deployed in Seshadripuram College lab for network activity monitoring. Captured and analysed 10,000+ live packets daily, decoding protocols like TCP, ICMP, and DNS using custom-crafted filters. Detected anomalies and suspicious traffic patterns, significantly enhancing lab network security and enabling in-depth security audits.
4. **ARP Poisoning & Packet Interception Tool:** Engineered an advanced Man-in-the-Middle (MitM) attack simulation tool leveraging ARP spoofing, tested in a controlled network environment. Intercepted, manipulated, and logged 5,000+ packets per session across 2–5 target devices by forcefully rerouting traffic. Empowered deep packet inspection and real-time payload tampering—built for high-impact penetration testing and exploit demonstrations.
5. **Multi-Vector Flooding Tool DDoS Simulator:** Co-engineered a DDoS simulation script with a team of 2, utilizing three threaded attack vectors—TCP, UDP, and ICMP—with randomized IP spoofing and dynamic payloads. Tested the resilience of local servers by generating 300–500 packets/sec, accurately replicating real-world traffic surges. Successfully evaluated defensive setups under controlled stress conditions, enhancing incident readiness and infrastructure robustness.

CYBERSECURITY COURSE

Microsoft Cyber Shikshaa – Cybersecurity Certification | *SEP 2024 – OCT 2024*

Completed Microsoft Cyber Shikshaa 75-hour certification covering network, application, system security, and penetration testing. Trained in Windows/Linux hardening, access control, and threat analysis (phishing, malware, social engineering). Worked with tools like Wireshark, Nmap, and Burp Suite; conducted vulnerability reporting and mitigation planning.

ADDITIONAL INFORMATION

- **Languages Spoken:** English, Kannada, Hindi
- **Soft Skills:** Problem Solving, Critical Thinking, Attention to Detail, Incident Prioritization, Time Management, Adaptability, Ethical Responsibility, Team Collaboration, Written & Verbal Communication, Analytical Reasoning, Stress Management, Situational Awareness.
- **Stand Out in Group Discussion by TCS iON:** Learned techniques to effectively contribute, lead, and present ideas in group discussions.