SUJAN SHANSHIKANT PISAL

+91 9359264299 ◇ Pune, Maharashtra, India

pisal.sujan@gmail.com ◇ LinkedIn ◇ Github Portfolio

SUMMARY

Entry-level Cybersecurity Analyst and 2025 Engineering graduate with hands-on experience in SOC operations, vulnerability assessment, and network security, supported by real-world exposure in network operations and cybersecurity internships. Skilled in log analysis, incident triage, OWASP Top 10, API security, and security monitoring using tools such as Splunk, Nmap, Wireshark, Burp Suite, and Metasploit, with working knowledge of Python and Bash for security automation. Demonstrates a strong understanding of attacker techniques and defensive controls through Red Team and Blue Team simulations, combined with operational discipline gained from SLA-driven environments. Highly motivated, detail-oriented, and eager to contribute to security monitoring, threat detection, and continuous improvement in a professional SOC or cybersecurity team.

SKILLS

Technical Skills :
Cybersecurity Fundamentals, Network Security, VAPT, Incident Analysis (Foundational), OWASP Top 10(2025), API security, DevOps Fundamentals, CI/CD Concepts, GenAI concepts, Windows Fundamentals, Linux & System Fundamentals, OOPs, Prompt Automation.

Soft Skills :
Problem Solving, Adaptability, Attention to Detail, Logical Thinking, Time Management, Ownership & Responsibility

Tools & Programming languages :
Splunk (Basic), Wireshark, Nmap, Metasploit, OSINT Frameworks, Cisco Packet Tracer, Python, Java, Bash Scripting,

EDUCATION

Boston Institute Of Analytics, Pune(June 2025 - November 2025)
Cyber Security and Ethical Hacking Course

Ajinkya DY Patil School of Engineering, Lohegaon, Pune(2021 - 2025)
B.E.-Electronics and Telecommunication Engineering, CGPA: 6.88 / 10.00

Novel Junior College of Science (2019 - 2021)
12th MSBSHSE, Percentage: 69.33 / 100

Sterling High School (2018 - 2019)
10th CBSE, Percentage: 61.60 / 100

EXPERIENCE

Network Support Analyst - June 2025 - Present
Spectram Telecommunications - Pune, Maharashtra

- Provide remote technical support and incident resolution for enterprise network environments under defined SLAs.
- Investigate network and security-related issues by analyzing traffic patterns, logs, and system alerts.
- Correlate incident data across multiple sources to support root cause identification.
- Maintain accurate service records, incident documentation, and configuration details.
- Collaborate with internal technical teams to escalate unresolved issues and support service recovery.
- Develop strong operational discipline aligned with 24×7 support environments.

- Supported incident investigation and escalation workflows aligned with ITIL-based operational processes.

Cyber Security Intern - Dec 2023 - Jan 2024
DCDIUM Technologies - Pune, Maharashtra

- Conducted vulnerability assessments based on OWASP Top 10, identifying common web and API security flaws.
- Assisted in security monitoring and threat analysis, simulating SOC-style workflows.
- Participated in Red Team & Blue Team exercises, improving understanding of attacker techniques and defensive controls.
- Performed basic threat modeling and system auditing to identify security gaps.
- Automated reconnaissance and data collection tasks using Python and Bash scripts, reducing manual effort.
- Documented vulnerabilities, attack paths, and mitigation strategies for technical and non-technical stakeholders.

PROJECTS

Scratcher-Recon – Automated Reconnaissance Framework
Technologies: Bash, Git, Nmap, httpx, subfinder, findomain, gf

- Designed and developed a modular reconnaissance automation tool to collect, validate, and organize target intelligence.
- Automated repetitive reconnaissance tasks, significantly reducing manual effort during early-stage penetration testing.
- Simulated real-world attacker reconnaissance workflows used in bug bounty and red team engagements.
- Enhanced understanding of attack surface discovery, subdomain enumeration, and exposure identification.

Secure Network Design & Simulation
Technologies: Cisco Packet Tracer

- Designed secure enterprise-style network architectures incorporating segmentation and access controls.
- Simulated attack scenarios and defensive responses to analyze network weaknesses.
- Applied networking and security principles to understand real-world infrastructure risks.
- Industry Relevance: Aligns with SOC, Network Security, and Cloud Infrastructure Security fundamentals.

CERTIFICATIONS

- API Security Fundamentals (December 2024)
- Google Cyber Security Professional Certificate (June 2024)
- Cyber Security and Ethical Hacking BIA Institute, Pune (November 2025)
- Splunk fundamentals (December 2025)
- TCS iON Career Edge - Young professional (January 2024)
- Multi Cloud Red team Analyst(MCRTA) Certification