

Parshuram Kalunkhe

+91 9370166755 | kalunkheparshuram@gmail.com | [LinkedIn](#) | [GitHub](#)

Bhiwandi, Maharashtra - 421305

Career Objective

Aspiring SOC Analyst with hands-on experience in SIEM, IDS/IPS, packet analysis, and vulnerability assessment through lab projects and teaching roles. Skilled in log analysis, security monitoring, and troubleshooting, seeking an entry-level SOC position to apply and grow in incident detection and response.

Skills/Tools

- **Skills:** SIEM Monitoring | EDR (Endpoint Detection and Response) | NDR (Network Detection and Response) | Understanding IDS/IPS alerts | Packet Analysis | Firewall | Running Basic Scans | Technical Documentation & Writeups
- **Tools:** Rapid 7 | Wazuh | ELK | Zeek (Bro) | Suricata | Snort | Wireshark | Nmap | Nuclei | OpenVAS (Greenbone) | OPNsense | Kali Linux | Clonezilla | Redo Rescue

Experience

Computer Trainer	VIDYA India	June 2024 – Present
<ul style="list-style-type: none">• Delivered training sessions in Basic IT, Advanced Excel, and Hardware & Networking, helping students build strong IT fundamentals and apply concepts in practical lab environments.• Conducted interactive sessions on Cybersecurity Essentials (Cisco NetAcad), covering secure network behaviour, firewalls, and threat awareness to improve student readiness for digital threats.• Guided students through hands-on troubleshooting exercises and created detailed documentation to enhance their problem-solving approach and knowledge retention.• Assisted IT Support Administrator with lab setups at schools and training centers, including hardware installation, LAN cabling, and software configuration for seamless classroom operations.		
Intern	Swayam Siddhi College of Management and Research (Exam Center)	Oct 2023 – March 2024
<ul style="list-style-type: none">• Assisted with system and network configuration during exam setups, ensuring secure, uninterrupted operations.• Provided technical support under pressure during high-stakes exams, demonstrating adaptability in a fast-paced, dynamic environment.• Collaborated with TCS iON team to monitor and validate system performance, ensuring integrity and reliability of IT systems.		

Education

Bachelor of Science in Information Technology	Mumbai University	CGPA 8.63
-----------------------------------------------	-------------------	-----------

Projects

- **SOC Home Lab** – Built a virtual SOC using Wazuh + ELK for SIEM & EDR, integrated OPNsense firewall and Suricata/Snort IDS, and simulated attacks with Kali Linux to generate, monitor, and analyze alerts.
- **Threat Hunting & Network Analysis** – Used Wireshark and Zeek to capture and investigate malicious traffic from Nmap and Nuclei scans, performing packet analysis and documenting findings.
- **Vulnerability Assessment & Hardening** – Conducted scans with OpenVAS and Nuclei, identified and remediated high-risk vulnerabilities, applied firewall rules, and verified mitigation with re-scans.

Certificates

- Introduction to Cybersecurity – Netacad
- Cybersecurity Essentials – Netacad
- Fortinet NSE 1, 2, 3 – Network Security Associate
- Networking Basics – Netacad
- CCNA 200-301 Network Fundamentals – Simplilearn