TUSHAR BASAK

+91 8299312126 ◇ Delhi, India

Mail: tushar.basak@yahoo.com ◇ LinkedIn: tusharbasak97 ◇ Portfolio: bit.ly/basakwebsite

OBJECTIVE

Motivated and detail-oriented IT professional with hands-on experience in cybersecurity operations, system administration, and technical support. Skilled in incident response, log analysis, vulnerability assessment, and endpoint security across Windows and Linux environments. Proven ability to manage user access, troubleshoot critical issues, and support IT infrastructure with adherence to SLAs.

Currently seeking to contribute to Wipro's Security Operations Center as a Cyber Security Analyst - L1, leveraging my practical training in SOC monitoring and threat detection, along with my commitment to continuous learning and process improvement, to help safeguard enterprise assets and enhance the organization's security posture.

Security Operations | Incident Response | SIEM & Log Monitoring | Vulnerability Management | Windows/Linux Administration | Active Directory | Endpoint Protection | ITSM Tools | Network Troubleshooting

EXPERIENCE

Cybersecurity Trainee View — May 2024 – Sept 2024
Tata Strive | SAP India — *Anand, Gujarat*

- Trained extensively in **Security Operations Center (SOC)** functions including **real-time threat detection**, **incident response**, and **log analysis**.
- Used **SIEM tools** for event correlation, alert investigation, and basic threat hunting.
- Participated in **vulnerability assessments** and supported mitigation planning for identified risks.
- Conducted **threat modeling** and **risk analysis** to assess attack surfaces and propose countermeasures.
- Gained working knowledge of **secure communication protocols**, **encryption**, and **key management** relevant to embedded systems.
- Supported **incident triaging**, maintaining documentation and contributing to post-incident reporting.
- Utilized tools such as **Wireshark, Burp Suite, and Nmap** for traffic analysis and vulnerability scanning.

IT Support Engineer — Jan 2023 – Mar 2024
Secure Life HR Service Private Ltd. — *New Delhi*

- Delivered Tier-1 and Tier-2 technical support across **Windows/Linux environments**, resolving user issues within defined SLAs.
- Handled user access and permissions via **Active Directory**, supporting identity and access management protocols.
- Monitored and maintained **endpoint security**, antivirus compliance, and system patching processes.
- Troubleshot **network issues** (LAN/WAN, VPN, DNS, DHCP) and managed **network equipment configuration**.
- Provided remote support via **RDP, SSH**, and documented incidents using **ITSM platforms**.
- Contributed to **incident documentation**, knowledge base updates, and root cause analysis for recurring issues.

TOOLS & SKILLS

- **Cybersecurity Operations:** Threat Detection, Incident Response, Log Analysis, SIEM (Splunk, Elastic, OSSIM)
- **Vulnerability Management:** Nessus, OpenVAS, Nmap, Burp Suite, Metasploit
- **ITSM & Remote Support:** ServiceNow, Freshservice, RDP, SSH
- **Networking & Security Tools:** Wireshark, IDS/IPS, VPN, Firewall Configuration (Cisco, Palo Alto)
- **Identity & Access Management:** Active Directory, Group Policy, MFA, User Provisioning
- **Scripting & Automation:** Python, Bash, PowerShell (for log parsing and task automation)
- **Operating Systems:** Windows Server, Linux (Ubuntu, CentOS), System Hardening & Patching

EDUCATION

Master of Computer Applications, Manipal University, Jaipur — May 2021 - July 2023
CGPA: 8.92

Bachelor of Science, Swami Vivekananda Subharti University, Meerut — July 2017 - Dec 2019
Percentage: 68.5%

CERTIFICATIONS

- Tata Group - Cybersecurity Analyst Job Simulation — View
  Forage — July 2024

PROJECTS

- **Embedded Device Security Assessment:** Extracted firmware from an IoT device and performed static and dynamic analysis using *IDA Pro* and *Ghidra*. Identified misconfigurations, decrypted stored credentials, and recommended hardening measures. Gained hands-on experience with UART and JTAG exploitation for unauthorized access and debugging.
- **Web & Binary Exploitation Labs (PortSwigger & TryHackMe):** Completed 30+ labs on PortSwigger covering OWASP Top 10 vulnerabilities such as *SQLi, XSS, CSRF, SSRF*, and 5+ machines on TryHackMe involving *privilege escalation, misconfigurations, and secure coding flaws*. Strengthened practical skills in reconnaissance, exploitation, and remediation.
- **Penetration Testing on Metasploitable2 and IoT Device:** Conducted full-scope VAPT by scanning with *Nmap*, identifying vulnerabilities, and exploiting them using the *Metasploit Framework*. Demonstrated exploits such as *buffer overflows* and *firmware backdooring*. Documented findings and proposed mitigations aligned with CVSS scoring.

LEADERSHIP

City President — Jan 2023 - Dec 2023
BloodConnect Foundation — *Kanpur, UP*

- Spearheaded a 2-tier team of 20+ students, efficiently managed a budget of INR 2.5 LPA, and improved helpline processes for enhanced customer satisfaction.
- Organized 20+ blood donation camps, collecting 1K+ units of blood, impacting 3K+ lives, and inspiring campus community participation.
- Demonstrated leadership, budget management, process improvement, and community engagement.