

# Somenath Sebait

LinkedIn: [www.linkedin.com/in/somenath-sebait](https://www.linkedin.com/in/somenath-sebait)

GitHub: <https://github.com/0x-s0M3n4th>

Email: [somnathsebait23@lpu.in](mailto:somnathsebait23@lpu.in)

Mobile: +91-6297205455

## SKILLS

- **Languages:** Python, Bash, PowerShell, C
- **Tools/Platforms:** Evilginx2, GoPhish, Metasploit, SliverC2, PowerShell Empire, Shellter, BloodHound, SharpHound, Impacket,Responder, NetExec, Rubeus, Certify, Mimikatz, Burp Suite, SQLMap, ffuf, Nmap, Nessus, OpenVAS, Chisel, Proxy chains, Aircrack-ng, Wazuh, Snort, Wireshark, Sysinternals Suite.
- **Soft Skills:** Problem-Solving Skill, Team Player, Adaptability, Report Writing, Blog Writing.

## INTERNSHIP

- **Linux System Administration Intern Red Hat | ([Summer Training](#))** Jun' 2025 – Jul' 2025
  - Acted as a Junior System Administrator within the IT department, focused on enhancing infrastructure reliability through rigorous automation, storage management, and security hardening of the **RHEL** environment.
  - Managed daily responsibilities by developing **Bash** scripts for automated user provisioning and configuring Logical Volume Manager (**LVM**) for dynamic storage, while deploying secure **Apache/Nginx** web servers using **SELinux** and **Firewalld**.
  - Gained practical expertise in maintaining high system availability through automated **Cron** backups and log rotation, successfully auditing **SSH** configurations and file permissions to ensure compliance with enterprise security standards.

## PROJECTS

- **Virtual Cybersecurity & Infrastructure Home Lab | ([Live Link](#))** Aug' 2025 – Nov' 2025
  - Architected a complex, multi-segmented virtual environment to simulate enterprise network topologies while strictly isolating attacker machines from production servers.
  - Conducted phishing simulations using Evilginx2, C2 operations using Powershell Empire and network pivoting using Proxy Chains, chisel from kali Linux to compromise isolated Windows Server 2022 and Domain joined Windows 10 workstations.
  - Leveraged Wazuh, custom Suricata rules for active monitoring to detect network traffic during attack simulations, which further helped me to carve attacks accordingly.  
**Tech:** Evilginx2, Powershell Empire, GoPhish, NetExec, Bloodhound, Wazuh, Suricata, shelter, mimikatz, Responder.
- **Nwatch – Network Throughput Logger | ([Github](#))** Jun' 2025 – Jul' 2025
  - Addressed the need for continuous bandwidth analysis and anomaly detection on critical network interfaces during Linux system administration training.
  - Developed Nwatch, a robust automation tool using Bash and vnstat to capture hourly traffic data, employing Cron jobs to schedule precise logging and daily summary generation.
  - Established a fully automated monitoring pipeline that generates granular throughput reports, enabling effective bandwidth analysis and rapid identification of traffic irregularities without manual intervention.  
**Tech:** Bash(Shell Scripting), vnstat(Traffic monitoring), Cron, grep, cut, wc, systemd.

## CERTIFICATES

- **OBSCURA: The future of cybercrime | ([Flare Academy](#))** Oct' 2025
- **Practical Help Desk | ([TCM Security](#))** Sep' 2025 – Oct' 2025
- **Red Hat System Administration | (RH124) | ([Red Hat Academy](#))** Jun' 2025 – Jul' 2025
- **Red Hat System Administration || (RH134) | ([Red Hat Academy](#))** Jun' 2025 – Jul' 2025

## CERTIFICATIONS

- **eJPT : eLearnSecurity Junior Penetration Tester | ([INE Security](#))** May' 2025 – Jul' 2025

## ACHIEVEMENTS

- **Technical Blog | ([Live Link](#))**
- Published detailed walkthroughs for blue team operations, forensics, and system administration, which provided actionable community guides while solidifying technical proficiency through documentation and teaching.
- Established a technical platform to document end-to-end research in Active Directory attacks, network penetration testing, and C2 operations, resulting in a comprehensive repository of offensive security methodologies.

## EDUCATION

- **Lovely Professional University** Punjab, India  
*Bachelor of Technology - Computer Science and Engineering; CGPA: 6* Aug' 2023 – Present
- **Ramsagar High School** West Bengal, Bankura  
*Intermediate; Percentage: 86%* Apr' 2021 – Mar' 2022
- **Ramsagar High School** West Bengal, Bankura  
*Matriculation; Percentage: 90%* Apr' 2019 – Mar' 2020