Somenath Sebait

LinkedIn: www.linkedin.com/in/somenath-sebait
GitHub: https://github.com/0x-s0M3n4th
Email: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

  - **About:** Underwent intensive training in Red Hat Enterprise Linux (RH124 & RH134). Applied theoretical knowledge to 5 real-world scenarios to simulate enterprise system administration.
  - Acted as a Junior System Administrator focused on infrastructure automation, storage management, and security hardening within a RHEL environment.
  - Managed automated user provisioning via Bash scripts, configured LVM for dynamic storage, and deployed secure web servers (Apache/Nginx) using SELinux .
  - Monitored system health through automated Cron jobs for backups and log rotation while managing package deployments via DNF and YUM.
  - Gained practical expertise in maintaining high system availability through automated backups and log rotation while auditing SSH configurations to meet enterprise security standards.2
  - **Tech stacks used:** RHEL, Bash, LVM, SELinux, VI/Vim, Package Management (dnf/yum).

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 Evilgnix2, 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.

Shell | C , Linux | Github Jan' 2026 – Present

- Developing a custom Unix-like shell in the C programming language to gain a deep understanding of system-level operations and process management.
- Engineering core functionalities including command parsing, execution of external binaries, and built-in command handling through system calls.
- Implementing robust error handling and environment variable management to ensure stable interaction within a Linux-based terminal environment.

Certifications

- **Red Hat System Administration | (RH124) | Red Hat Academy** Jun' 2025 – Jul' 2025
- **Red Hat System Administration || (RH134) | Red Hat Academy** Jun' 2025 – Jul' 2025
- **eJPT** : eLearnSecurity Junior Penetration Tester **| INE Security** May' 2025 – Jul' 2025
- **Practical Help Desk | TCM Security** Sep' 2025 – Oct' 2025
- **OBSCURA: The future of cybercrime | Flare Academy**

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*