Somenath Sebait

LinkedIn: https://www.linkedin.com/in/somenath-sebait-52575823b/
Email: sebaitsom6297@gmail.com
GitHub: https://github.com/0x-soM3n4th   Mobile:+91-6297205455

SKILLS

- **Languages**:   Python, Bash, PowerShell, C
- **Tools/Platforms**:   Evilginx2, GoPhish, Metasploit, SliverC2, Mythic C2, PowerShell Empire, Shellter, BloodHound, SharpHound, Impacket, Responder, CrackMapExec, Rubeus, Certify, Active Directory Module, Mimikatz, Burp Suite, SQLMap, FFuF, Nmap, Nessus, OpenVAS, Chisel, Proxy chains, Aircrack-ng, Wazuh, Snort, Wireshark, Sysinternals Suite, Ghidra, x64dbg.
- **Soft Skills**:   Problem-Solving Skills, Team Player, Adaptability, Report Writing, Blog Writing.

INTERNSHIP

- **Linux System Administration Intern Red Hat (Summer Training)**   June 2025 – July 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.
  - **Key Projects:**
    - **Automated User Provisioning:** Created Bash scripts to onboard users with specific group permissions and password policies.
    - **Storage Management:** Configured LVM (Logical Volume Manager) to allow dynamic resizing of file systems without downtime.
    - **Web Server Deployment:** Deployed an Apache/Nginx server, configuring FirewallD and SELinux contexts to ensure secure access.
    - **System Hardening:** Audited and secured SSH configurations and file permissions to meet security standards.
    - **Task Scheduling:** Implemented Cron jobs for automated system backups and log rotation.
  - **Tech stacks used:** RHEL, Bash, LVM, SELinux, VI/Vim, Package Management (dnf/yum).

PROJECTS

- **Black hat python – a repo of offensive python code snippets**:   June 2025 - Present
  Designed to streamline Red Team operations, this repository features a curated collection of Python scripts for automating routine offensive tasks. It focuses on rapid prototyping for custom exploits and OpSec-compliant tooling, creating a reliable, reusable toolkit for authorized security assessments and educational research.

- **CTF writeup finder – useful script to find writeups of CTFs:**   August 2025
  Engineered a Python-based utility to address the inefficiency of manual research by automating the discovery of CTF write-ups. The tool intelligently queries multiple sources to locate specific solutions, significantly reducing research time and accelerating post-CTF learning and analysis.

- **Virtual Cybersecurity & Infrastructure Home Lab**   March 2025 - Present
  Architected a complex, multi-segmented virtual environment to simulate enterprise network scenarios and attack vectors. The setup utilizes custom virtual networks to strictly isolate attacker machines (**Kali**) from vulnerable targets (**Metasploitable2**) and production servers **(Windows Server 2022, Linux Mint)**, effectively enabling safe Red and Blue team practice with active monitoring via **Wazuh**.

- **Personal Technical Blog – comprehensive documentation for security & sysadmin**   July 2025 - Present

  Established a technical platform dedicated to documenting cybersecurity labs, Linux system administration, and Offensive Security guides. The initiative aims to solidify personal learning through teaching, providing the wider community with detailed, step-by-step walkthroughs on Blue team operations and complex CTF challenges.

CERTIFICATIONS

- **eJPT** : eLearnSecurity Junior Penetration Tester | **INE Security**   May 2025 – July 2025

EDUCATION

- **Lovely Professional University**   Punjab, India
  Bachelor of Technology - Computer Science and Engineering; **CGPA: 6.03**   August 2023 – Present

- **Ramsagar High School**   West Bengal, Bankura
  Intermediate; **Percentage: 86%**   April 2021 - March 2022

- **Ramsagar High School**   West Bengal, Bankura
  Matriculation; **Percentage: 90%**   April 2019 - March 2020