Somenath Sebait

Email:sebaitsom6297@gmail.com
Portfolio: https://0x-s0m3n4th.github.io/
Address: Jalandhar(Punjab)
Github: https://github.com/0x-s0M3n4th
Twitter: https://x.com/cyb3r_Insi6ht
LinkedIn: https:/www.linkedin.com/in/somenath-sebait-52575823b/

Education

- **Lovely Professional University(LPU)** Jalandhar, India
2023 - present

  - **Degree**: Bachelor of Technology (B.Tech) – Computer Science and Engineering
  - **Courses**: Computer Architecture and Organization, Operating Systems, Computer Architecture, Data Structures, Analysis Of Algorithms, Artificial Intelligence, Networking, Databases , Python Programming.

Skills Summary

- **Programming Languages:** Java, C++, C, Python, JavaScript, Bash, PowerShell
- **Soft Skills:** Report Writing, Blog Writing
- **Skills:** Vulnerability Assessment & Penetration Testing (VAPT), Phishing simulations, Web Application Security, Windows Security, Windows ,Defense Evasion, Enterprise Security, PowerShell, AV/EDR Evasion, OSINT, Offensive Tool Development using python, Active Directory exploitation, Active Directory Certificate Services(ADCS exploitation), Network Pen Testing.
- **Tools:** Evilginx, GoPhish, Metasploit, Sliver C2, Powershell Empire, Shelter BloodHound, SharpHound, Active Directory Module, Certify, Responder, Ping Castle, BurpSuite, Nessus, SQLMap, SysInternals Tools, Impacket, Nmap, Impacket, Rubeus, Mimikatz, CrackMapExec, x64Dbg, Ghidra, Sysmon, Aircrack-ng, ProxyChains, Wazuh, Suricata, Wireshark.

Certifications

eJPT : INE Security Junior Penetration Tester (Credential ID:154157229)

Experience

Personal Penetration Testing & Defense Lab | 2025 – Present

Designed, deployed, and maintain a multi-segment virtual cybersecurity lab for practical, hands-on penetration testing and blue team exercises.

Lab Architecture & Administration:

- Engineered a complex, isolated network environment using VMware, segmenting virtual machines across distinct subnets (e.g., ATTACK-NET, PENTEST-NET, PIVOT-NET, SECURE-NET).
- Configured and manage a diverse range of target systems, including Windows Server (2019, 2022), Ubuntu Server, and various vulnerable-by-design (VBD) machines like Metasploitable2 and Kioptrix.
- Deployed an ATTACK-BOX (Kali Linux) and an OSINT machine (tl-osint) to simulate real-world attacker infrastructure.

Red Team / Penetration Testing (Simulated):

- Executed penetration testing scenarios focusing on the full attack lifecycle from reconnaissance to post-exploitation.
- Conducted network-level attacks, including port scanning, vulnerability assessment, and exploitation of services on machines within the PENTEST-NET.
- Successfully practiced lateral movement and pivoting techniques between compromised hosts across different network segments (PENTEST-NET to PIVOT-NET).
- Performed simulated attacks against Windows Active Directory environments (EXTERNAL-RED, SECURE-NET), focusing on enumeration , exploitation and privilege escalation.

Blue Team / Defensive Operations (Simulated):

- Established a "Blue Team" lab environment to practice defensive security principles.

- Conducted "on-premise practicals" by analyzing attack traffic, hardening systems (like WIN_2K22 in SECURE-NET, Ubuntu server), and implementing basic monitoring to detect simulated intrusions as well as custom IDS/IPS rules along with firewall configurations .

Publications

- **Security Blog** : Publishing my methodologies, research, notes and cybersecurity learning journey on my Personal Blog.