Simranjit Singh Pabla

OSINT SAGE
India 📍 GJ-06 | MH-12 | PB-08

pablasimranjit98@gmail.com LinkedIn Simranjit | BIO.LINK

Summary

Experienced **Purple Team Security Analyst** with a solid foundation in both **offensive** and **defensive** security. Proficient in **vulnerability analysis**, **network penetration testing**, **SIEM monitoring**, and **incident response**. A problem-solver with a passion for staying up-to-date on the latest cyber threats, tools, and methodologies, ensuring proactive protection and efficient threat detection for organizational security.

Skills

Offensive Security:
Network Penetration Testing: Metasploit, Burp Suite, Cobalt Strike, PowerShell Empire
Privilege Escalation: Gtfobins, Linpeas, Winpeas, pspy
Password Cracking: Hashcat, John the Ripper
Exploitation: Nmap, Nikto, Nessus

Defensive Security:
Monitoring & Threat Detection: SIEM/IPS/EDR (Alien Vault, LogRhythm, Wazuh, Snort)
Incident Response & Mitigation: IDS signatures, threat intelligence analysis, OS hardening
Compliance: NIST Cybersecurity Framework, RMF, FAIR Risk Assessment

Work Experience

Security Analyst Dec 2023 – Present
Suma Soft, Pune, India
- Monitored SIEM activities, ensuring quick detection and response to threats.
- Conducted Active Directory and network penetration testing, identifying critical vulnerabilities.
- Led client consultations for incident analysis, reporting, and resolution.
- Conducting Red Team attacks and collaborating with Blue Team for defense improvements
- Developing security strategies based on offensive findings and defensive needs

Computer Instructor Oct 2021 - Mar 2022
Kendriya Vidyalaya Gujarat, India
- Redesigned the school's networking infrastructure for security and reliability (i.e. Fail-Safe Solution).
- Helped in curriculum development and handled administrative duties to ensure smooth operations.

Projects

Monitoring and Securing the DFI Environment [GitHub link]
- Monitored servers using least privilege principles and provided recommendations for OS hardening and compliance improvements.
- Analyzed firewall reports and threat intelligence to suggest mitigation steps for identified vulnerabilities.

Navigating a Cybersecurity Incident [GitHub Link]
- Conducted in-depth research on threat actors and vulnerabilities to recommend improvements in incident response planning and implementation.

Certification

LogRhythm Certified (LRSA & LRPA)

Education

Practical Ethical Hacking, TCM Security Nov 2022 - Aug 2023
Intro To Cybersecurity Nanodegree, Udacity Dec 2022 - Jul 2023
Deep Learning Nanodegree, Udacity Dec 2019 - Sep 2020
BTech CSE, Parul University Aug 2016 - May 2020
CGPA: 8.52