Simranjit Singh Pabla

OSINT SAGE | PURPLE GUY

India GJ-06 | MH-12 | PB-08
LinkedIn BIO.LINK GitHub Projects

Professional Summary

Cybersecurity enthusiast with 1.5 years of hands-on experience in offensive and defensive security, performing full-scope red team assessments and implementing blue team mitigation strategies. Proven track record of simulating real-world attacks, securing infrastructure, and reducing incident response times with high-impact solutions.

Skills

Offensive Security

Tools/Techniques: Nmap, Nessus, Burp Suite, Metasploit, MSF Venom, Wireshark, SQL Map
AD Exploits: Kerberoasting, Golden Ticket, Kerberoasting, Zero Logon. LLMNR, SMB Relay, Pass the Hash, Mimikatz
Enumeration & Recon: Bloodhound, Responder, CrackMapExec, Harvester, Google Dorks, OSINT
Web Attacks: SQLi, XSS, SSRF, CSRF, IDOR, OWASP

Defensive Security

Monitoring & Response: AlienVault, LogRhythm, Wazuh, Log Analysis, OS hardening, threat analysis
Frameworks Compliance: MITRE ATT&CK, NIST SP 800-115, RMF

Professional Experience

Suma Soft Pvt Ltd, Pune

Security Analyst — Dec 2023 – May 2025

- Discovered and exploited misconfigured AD, leading to privilege escalation and lateral movement.
- Conducted OSINT & LinkedIn enumeration to generate user/password combos leading to successful brute-force.
- Cracked NTLM hashes using secretsdump, gaining remote access via RDP and pivoted internally.
  Identified and exploited exposed info.php revealing server configuration & environment variables.
- Helped prevent a major DDoS attack by identifying and blocking IPs through WAF rules.
- Implemented Zero Trust architecture, reducing unauthorized access by 90%.
- Reduced average incident response time from 3 hours to 30 minutes via alert playbook automation.

Kendriya Vidyalaya, Vadodara

Computer Instructor (IT & Networking) — Oct 2021 – Mar 2022

- Conducted secure network practices for faculty systems
- Delivered workshops on digital safety and endpoint awareness

Projects & Labs

Active Directory Attack Lab: Simulated attacks including Kerberoasting and Golden Ticket on self-built domain lab
Bug Bounty Lab: Discovered XSS, CSRF, and IDOR vulnerabilities in intentionally vulnerable applications
Monitoring DFI Environment: OS hardening, privilege audit [GitHub Link]
Cybersecurity Incident Navigation: Response strategy + threat actor profiling [GitHub Link]

Certifications and Accomplishment:

PNPT [Practical Network Penetration Tester]
LRSA [LogRhythm Security Analyst] and LRPA [LogRhythm Platform Admin]
Research Paper: Machine Learning-Based Multi-temporal Image Classification Using Object-Based Image Analysis and Supervised Classification

Education:

Practical Ethical Hacking – TCM Security — Nov 2022 – Aug 2023
Intro to Cybersecurity – Udacity — Dec 2022 – Jul 2023
Deep Learning Nanodegree – Udacity — Dec 2019 – Sep 2020
B.Tech CSE | Parul University | CGPA: 8.52 — Aug 2016- May 2020