KARTHIKEYAN

Cybersecurity Analyst | Penetration Tester

9025523760 | karthikeyaneh@gmail.com | linkedin.com/in/karthikeyaneh | github.com/psyclox | Karaikal, Puducherry

PROFESSIONAL SUMMARY

Computer Engineering graduate with hands-on experience in ethical hacking, penetration testing, and vulnerability assessment. Proficient in identifying OWASP Top 10 risks, conducting VAPT engagements, and mapping adversary techniques to the MITRE ATT&CK framework. Developed multiple security tools in Python and JavaScript, including OSINT automation, SQL injection detection, and client-side encryption — each deployed and tested against real-world attack vectors. Holds CEH (Practical) and CAPIJ certifications.

TECHNICAL SKILLS

Exploitation: Metasploit, SQLmap, Hydra, Netcat, MSFvenom, BeEF, Burp Suite Pro,
Network & Traffic: Wireshark, tcpdump, Ettercap, Netcat
Password & Wireless: Hashcat, John the Ripper, Aircrack-ng, Crunch
Scripting & Automation: Python, Bash, PowerShell, JavaScript
Frameworks & Standards: OWASP Top 10, MITRE ATT&CK, PTES, CVSS v3, NIST
Domains: Web AppSec, Network PenTest, VAPT, OSINT, AD Attacks, Threat Modelling
Certifications: CEH Practical (EC-Council) | CAPIJ (The XSS Rat) | OSCP — In Progress (OffSec)

EXPERIENCE

Cybersecurity Analyst Trainee | **Cybervault Innovations and Technologies Pvt Ltd** *Oct 2025 – Present*

- Performed web application penetration tests targeting OWASP Top 10 vulnerabilities — including SQLi, XSS, IDOR, and broken authentication — using Burp Suite for manual exploitation and business logic flaw discovery, resulting in 15+ validated vulnerability findings per engagement.
- Analysed firewall rule sets, network segmentation, and ACLs to uncover security gaps; produced risk-rated reports with remediation guidance prioritised by CVSS scoring to support client patch planning.
- Mapped full-spectrum penetration test findings to MITRE ATT&CK TTPs, enabling clients to benchmark defensive coverage and identify detection blind spots across the kill chain.

PROJECTS

Vulnerability Assessment & Penetration Testing (VAPT) — Client Engagements

- Scoped and executed systematic VAPT across production and staging environments under signed Rules of Engagement, using Nmap for service enumeration, Burp Suite for manual web testing, and Metasploit for exploitation, achieving comprehensive coverage of the attack surface.
- Identified and documented critical-severity issues (CVSS ≥7.0) including authentication bypass and server-side request forgery (SSRF); produced executive-level reports with PoC screenshots and prioritised remediation plans, enabling clients to remediate 100% of critical findings within SLA.

ReconMate — OSINT & Recon Automation Tool | github.com/psyclox/Reconmate

- Built a Python-based multi-threaded OSINT tool that automates subdomain enumeration via DNS brute-forcing and certificate transparency logs, alongside port/service scanning — reducing manual recon time from hours to minutes on engagement targets.

Encrypt Anything — Client-Side Encryption Chrome Extension | github.com/psyclox/Encrypt-Anything

- Developed a JavaScript Chrome extension implementing AES-256-GCM encryption with PBKDF2 key derivation (100k iterations, SHA-256) entirely in the browser, ensuring plaintext never leaves the client — validated against cloud-compromise and man-in-the-middle scenarios.

SQLister — SQL Injection Detection & Exploitation Tool | github.com/psyclox/sqlister

- Engineered a Python-based SQLi scanner that automates error-based, union-based, and blind injection testing across HTTP parameters, with intelligent payload generation and WAF evasion techniques — built as a learning tool benchmarked against DVWA and bWAPP.
- Implemented response-diff analysis to reliably distinguish true positives from WAF-blocked and filtered responses, reducing manual verification effort during web application assessments.

EDUCATION

B.Tech — Computer Science and Business Systems *CGPA: 7.69*

EGS Pillay Engineering College, Nagapattinam | 2021 – 2025