GOUTHAM PRASANTH PAMARTHY

OSEP | CRTE | AWS Certified Security - Specialty | CompTIA Security+ | CCNA | (ISC)2 CC
(240) 495-8089 | gppamarthy@gmail.com | linkedin.com/in/gpamarthy7 | github.com/gpamarthy

SUMMARY

Security engineer with experience across penetration testing, vulnerability management, cloud infrastructure hardening, incident response, and detection engineering. OSEP and CRTE certified - both require passing live proctored attack labs, not a multiple-choice exam. Built two offensive security tools: one maps AWS IAM privilege escalation chains that scanners miss, the other generates AV/EDR-evading payloads across nine output formats.

WORK EXPERIENCE

Head of Security Engineering | SportsExcitement | *Remote* — Nov 2025 - Present

- Conducted 20+ web app and API penetration tests across the production platform; every engagement started with mapping the attack surface manually before running tools - that approach uncovered IDOR, stored XSS, and auth bypass issues that automated scanners missed, driving a 40% reduction in critical vulnerabilities.
- Secured VPS infrastructure from the ground up: rewrote firewall rules in the IONOS Cloud Panel, configured NAT Gateway for outbound-only VM exposure, enforced SSH key auth, closed unused ports, and set up a patching cadence - maintained 100% uptime across production services throughout.
- Set up Cloudflare WAF in front of production and wrote custom firewall rules targeting active scraping and DDoS patterns; configured rate-limiting and Cloudflare Access to lock internal tooling behind identity verification.
- Responded to a live cryptojacking and data exfiltration attempt - traced the attack through process trees, cron persistence, and outbound C2 traffic; evicted the loader, closed the initial access vector, and built Splunk detections so the same technique would not land again.
- Ran quarterly attack surface reviews with the CTO, translated technical findings into business risk, and co-designed network segmentation changes that cut overall exposure by 30%; also authored the company's first incident response playbook.

Graduate Teaching Assistant | University *of Maryland, College Park, MD* — Aug 2024 – Jan 2025

- Ran DFIR labs weekly for 60+ graduate students covering Splunk log analysis, Volatility memory forensics, and full-chain compromise reconstructions; built Python scripts that auto-generated realistic artifact sets for investigations, so students worked on varied evidence rather than the same canned scenario each week.

Security Engineer | Phoenix *Global* | *Hyderabad, India* — Jun 2022 - Aug 2022

- Built 25+ Splunk correlation rules by starting with raw log data, identifying the actual noise sources, then writing rules around real attacker behavior - false positives dropped 30% and Python triage automation saved the SOC around 15 hours per week.
- Audited IAM policies and security configurations across 50+ AWS assets - flagged overprivileged roles, dormant access keys, and gaps in CloudTrail coverage; co-authored the remediation guide that reduced cloud risk exposure by 35%.

PROJECTS

Domino: AWS IAM Privilege Escalation Path Prover — 2026

- Takes an IAM snapshot or pulls live credentials, models principals and resources as a networkx MultiDiGraph, then finds all paths to admin targets. Matches chains against 12 built-in attack tactics - PassRole+Lambda, IMDS credential theft, Confused Deputy via S3, IAM self-escalation, Lambda code hijack, and others - scoring each by tactic severity and hop difficulty.
- The problem it solves: Prowler tells you 200 individual misconfigs exist. Domino tells you which 5 of them chain into actual account compromise and shows you the exact path to get there.

MalForge: Multi-Format Payload Generator with AV/EDR Evasion — 2025

- CLI that takes raw shellcode or generates it via msfvenom, runs it through stackable encryption (XOR, AES-256-CBC, RC4, Caesar - any order, auto-reversed at runtime), and outputs across 9 formats: C# EXE, process hollowing, DLL (rundll32/regsvr32), VBA macro, HTA, PowerShell, JScript cradle, MSBuild inline task, InstallUtil.
- Evasion stack: never allocates RWX memory (RW then RX), patches AMSI and ETW at runtime, detects sandbox environments, and randomizes namespaces and class names on every build to stay ahead of static signatures.

TECHNICAL SKILLS

Offensive Security: Penetration testing, vulnerability management, AV/EDR evasion, AD exploitation, payload development, lateral movement, C2 frameworks (Cobalt Strike, Sliver), Burp Suite, Metasploit, BloodHound, Impacket, Mimikatz, Rubeus, CrackMapExec, Responder, Nmap, Nessus

Cloud and Infrastructure: IONOS Cloud (firewall, NAT Gateway, VPS hardening), Cloudflare (WAF, DDoS mitigation, Access, rate-limiting), AWS (IAM, S3, EC2, Lambda, GuardDuty, CloudTrail), Azure RBAC, VPC segmentation, KMS, iptables

Detection and Response: Splunk, ELK, SIEM correlation rule authoring, threat hunting, memory forensics (Volatility), incident response, log analysis, vulnerability assessment, CloudTrail auditing

Languages and Frameworks: Python, Bash, PowerShell, JavaScript, Ruby | MITRE ATT&CK, PTES, OWASP Top 10, NIST 800-53, PCI-DSS, HIPAA, GDPR, CMMC, secure SDLC

EDUCATION

M.Eng. in Cybersecurity, University of Maryland, College Park — May 2025

B.Tech. in Computer Science, Gandhi Institute of Technology and Management, India — Apr 2023