Ramya Radjesh

Cybersecurity Engineer

CONTACT

+91 6380588908
ramyaradjesh1@gmail.com
Chennai, India

Portfolio:
ramyaradjesh.github.io
LinkedIn:
linkedin.com/in/ramyaradjesh
GitHub:
github.com/ramyaradjesh
Medium:
medium.com/@ramya15112000

TECHNICAL SKILLS

Frameworks
ISO 27001, NIST, OWASP Top 10, GDPR, HIPAA, MITRE ATT&CK, CWE

Security
VAPT, Pentesting, Malware Analysis, Heuristic Detection, eBPF, SOC Ops, Incident Response, Digital Forensics, Threat Intelligence, Network Forensics, ARP Spoofing Detection, Cryptography

Tools
Wazuh, Splunk, Wireshark, Nmap, Kali Linux, Burp Suite, Cowrie, Auditd, Scapy, VirusTotal API

Programming
Python, SQL, Bash

Infrastructure
Docker, Kubernetes, Linux, VMs, Ubuntu, SHA-256, eBPF

EDUCATION

MSc Computer Security
EPITA, Paris
Apr 2025
Europe's top cybersecurity engineering school

BE Computer Science
Sri Manakula Vinayagar Engineering College
Apr 2022 | Puducherry

LANGUAGES

English — C1 Professional
Tamil — Native
French — B1 Intermediate

ABOUT

MSc Computer Security graduate (EPITA Paris) with hands-on experience building security tools and conducting independent research. Designed BPFroid at Orange Telecom, built a full three-layer antivirus engine, SOC home lab, and network forensics tools. Currently researching eBPF abuse for rootkit stealth and cloud-native attacks. Seeking entry-level SOC, penetration testing, or security engineering roles.

EXPERIENCE

Security Policy Developer — Orange — **Telecom Infrastructure Internship**

Feb 2024 – Jul 2024 | Paris

- Designed and implemented BPFroid, an eBPF-based Android malware detection prototype — detecting threats at kernel level, bypassing user-space AV limitations and mapping OS-layer credential risk patterns.
- Analysed eBPF integration in Android security: evaluated performance metrics, assessed system call hooks and traffic monitoring use cases, and produced PoC documentation for orange stakeholders.

MY OWN PROJECTS

● Research Project

1. eBPF Threat Atlas [In Progress]

eBPF, Linux Kernel, Kubernetes, Cloud-Native, CVE Research

- Building an attack taxonomy mapping how eBPF is abused for rootkit stealth, persistence, and privilege escalation across Linux, containers, and cloud-native environments.
- Researching verifier-bypass CVEs; pairing findings with defences — CAP_BPF/CAP_PERFMON hardening, unprivileged BPF restrictions, and bpffs controls.

● SOC & Detection

1. SOC Home Lab — Wazuh SIEM, Honeypot & MITRE ATT&CK Mapping [In Progress]

Wazuh, Cowrie, MITRE ATT&CK, Ubuntu, Auditd

- 3-VM lab (Kali attacker, Ubuntu target + monitor); simulated SSH/MySQL brute force, SQL injection, RCE, DB exfiltration, lateral movement — all mapped to MITRE ATT&CK.
- Custom Wazuh correlation rules + active response covering GhostEnum (insider enumeration), Cloud Shadow (credential exposure), and Stale Base (DB exfiltration) scenarios.

2. Advanced Packet Sniffer + ARP Spoofing Detector [In Progress]

Python, Scapy, Network Forensics, MITM Detection

- Real-time packet capture and ARP spoofing detection — monitors IP-to-MAC mappings, identifies ARP poisoning anomalies, and flags man-in-the-middle attacks on local networks.
- Supports network forensics and packet capture for post-analysis; useful in lab environments and as a monitoring component in a larger security setup.

3. SSH Brute Force Detector

Python, Log Analysis, Security Automation

- Parses Linux auth logs to detect SSH brute-force — configurable threshold, IP whitelist, alert logging, blocked-IP tracking, and optional UFW firewall response.

● Security Tools

1. MyAV — Three-Layer Antivirus Simulation

Python, VirusTotal API, SHA-256, Heuristics

- Layer 1 (SHA-256 local signatures), Layer 2 (VirusTotal API, 70+ engines, cached), Layer 3 (heuristic: double extension, dangerous location, size mismatch). Includes quarantine, email alerts, audit log, browser dashboard, and HTML report generator.

CERTIFICATIONS

- Cybersecurity Tools & Technologies — Microsoft
- Tools of the Trade: Linux & SQL — Google
- Networks & Network Security — Google
- Play It Safe: Manage Security Risks — Google