Ramya RADJESH

Chercheur en Sécurité

CONTACT

+91 6380588908
ramyaradjesh1@gmail.com

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

Compétences Techniques

Cadres et Norms
ISO 27001, NIST, OWASP Top 10, GDPR, HIPAA, MITRE ATT&CK, CWE

Sécurité Offensive et Defensive
VAPT, Tests d'intrusion, Analyse de logiciels malveillants, Détection Heuristique, eBPF, SOC opérations, Réponse aux Incident, cyberville, nvestigation Réseau.

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

Programmation et Infrastructure
Python, SQL, Bash, Docker, Kubernetes, Linux.

ÉDUCATION

MSc – Computer Security
École Pour l'Informatique et les Techniques Avancées - EPITA
Apr 2025 | Paris

B. Tech - Computer Science
Sri Manakula Vinayagar Engineering College
Apr 2022 | Puducherry

LANGUES

Anglais— C1 Professionnel
Tamoul — Langue Maternelle
Français — B1 Intermédiaire

CERTIFICATIONS

Security+	En Cours
OCSP	Prévu
Microsoft Cybersecurity	Terminé
Google Networks	Terminé
Google Security	Terminé

À PROPOS

Diplômé d'un MSc en sécurité informatique (EPITA Paris), je possède une expérience pratique de la détection des menaces basée sur eBPF, des opérations SOC et des outils de sécurité. Passionné par la recherche en sécurité au niveau du noyau (kernel) et l'ingénierie de détection, j'ai acquis une expérience concrète tant dans le domaine offensif que défensif. Je prépare actuellement la certification CompTIA Security+.

EXPERIENCE

Développeur de politiques de sécurité

Orange — Équipe de protection des données- **RESEARCH INTERNSHIP**

Feb 2024 – Jul 2024 | Paris

- Conception et mise en œuvre de BPFroid, un prototype de détection de logiciels malveillants Android basé sur eBPF : interception de plus de 8 points d'ancrage (*hooks*) d'appels système au niveau du noyau, contournement des limitations des antivirus en espace utilisateur et modélisation de 3 scénarios de risque liés aux identifiants au niveau du système d'exploitation.
- Présentation de résultats de recherche sur l'implémentation d'eBPF pour la sécurité mobile et sur son utilisation au sein de divers systèmes d'exploitation mobiles.
- Rédaction de la documentation du PoC et réalisation de tests de performance pour les parties prenantes chez Orange ; ces travaux ont contribué à l'évaluation interne d'eBPF pour la surveillance des menaces Android à grande échelle.

PROJETS DE SÉCURITÉ

eBPF Threat Atlas - RECHERCHE INDÉPENDANTE

***Stack**: eBPF, Linux Kernel, Kubernetes, Cloud-Native, CVE Research*

- Élaboration d'une taxonomie des attaques recensant les abus d'eBPF pour la furtivité, la persistance et l'élévation de privilèges des rootkits dans les environnements Linux, conteneurisés et cloud-native.
- Recherche sur les CVE de contournement de vérificateur ; association des résultats avec les défenses : renforcement de CAP_BPF/CAP_PERFMON, restrictions BPF pour les utilisateurs non privilégiés et contrôles bpffs.

SOC Home Lab — Wazuh SIEM, Honeypot & MITRE ATT&CK Mapping

***Stack**: Wazuh, Cowrie, MITRE ATT&CK, Ubuntu, Auditd*

- Déploiement du pot de miel Cowrie pour capturer et analyser des comportements réels d'attaques par force brute SSH; enregistrement de 6 techniques d'attaque correspondant à 8 tactiques du framework MITRE ATT&CK.
- Corrélation des événements du pot de miel avec la fonctionnalité de réponse active de Wazuh dans le cadre des scénarios de menace GhostEnum, CloudShadow et StaleBase.

Wazuh – Laboratoire de détection des menaces – StaleBase, Cloud Shadow et Ghost Enum

***Stack:** Wazuh, OpenSearch, DVWA, MariaDB, Auditd, Kali linux, Ubuntu*

- Conception et exécution de trois scénarios d'attaque (exfiltration de base de données, exposition d'identifiants et énumération par un initié avec persistance via crontab), alignés sur les tactiques MITRE ATT&CK au sein d'un environnement isolé composé de trois machines virtuelles.
- Création de plus de dix règles de corrélation Wazuh personnalisées et de trois procédures de réponse active (playbooks) exploitant les sources de logs FIM, Auditd et Apache/MySQL, permettant une visibilité complète sur l'ensemble de la chaîne d'attaque (kill chain) pour les trois scénarios.

MyAV — Simulation d'antivirus à trois couches

Stack : Python, API VirusTotal, SHA-256, Heuristique

- Couche 1 (signatures locales SHA-256), Couche 2 (API VirusTotal, plus de 70 moteurs, mise en cache — réduction du temps d'analyse répétée d'environ 80 % grâce à la mise en cache des hachages locaux), Couche 3 (heuristique : double extension, emplacement dangereux, incohérence de taille).
- Inclut la mise en quarantaine, les alertes par e-mail, le journal d'audit, le tableau de bord par navigateur et le générateur de rapports HTML.