GUYANI YOUMBI KAMENI

Pentester Offensif | Red Team & Active Directory

guyanikameni@gmail.com · +33 7 58 45 34 30 · github.com/guyanikameni · LinkedIn · Medium · TryHackMe Top 2% · HackTheBox · Portfolio

PROFIL

5 ans · 16 missions · 14 domaines AD compromis. Que ce soit par Kerberoasting, DCSync ou ACL Abuse en Active Directory, une faille applicative web (OWASP Top 10) ou une campagne de phishing — je trouve toujours le chemin qui répond à la question du client. Dernière mission : **SSRF chaînée jusqu'à une RCE interne**, accès au réseau interne depuis Internet. Auteur de writeups techniques sur Medium. Disponible immédiatement pour missions offensives, Red Team ou audits AD complexes.

EXPÉRIENCES PROFESSIONNELLES

Pentester Offensif — Mission confidentielle · Secteur santé | Avr. 2026 – Juin 2026

→ Test d'intrusion web, interne et externe (approche Red Team). Domaine AD compromis : Kerberoasting → DCSync → **Domain Admin**.

→ SSRF sur l'application web exposée, chaînée jusqu'à une **RCE interne** — accès au réseau interne depuis Internet.

→ Mouvement latéral par **abus d'ACL Active Directory**. Rapport bilingue FR/EN : chemins d'attaque et remédiation priorisée.

Pentester / Consultant Sécurité Offensive — KALAO GLOBE TREK | Fév. 2023 – Mars 2026

→ **15 clients compromis** — remédiation 100 % sous 30 jours. RCE, Kerberoasting, DCSync, SQLi, privilege escalation, lateral movement — méthodologie PTES/OWASP.

→ **20+ rapports bilingues FR/EN** livrés en COMEX avec scoring CVSS et plans de remédiation actionnables. Décisions sécurité accélérées sur chaque engagement.

→ **Surface d'attaque réduite** post-engagement via démonstration de scénarios de mouvement latéral réalistes, traduits en recommandations concrètes pour les équipes IT.

Analyste en Sécurité Informatique — KALAO GLOBE TREK | Sept. 2021 – Fév. 2023

→ **Incidents AD gérés bout en bout** (détection → containment → remédiation) sur Active Directory et Windows Server. Veille cybersécurité hebdomadaire diffusée aux équipes techniques et à la direction.

→ **Premiers tests d'intrusion internes** réalisés en autonomie avec rapports priorisés par criticité — fondation directe de l'évolution vers le pentest offensif.

PROJETS CLÉS

Lab AD Red Team — Kill Chain complète documentée
BloodHound → Kerberoasting → PTH → DCSync → Domain Admin compromis. Writeup publié sur Medium. Lab reproductible sur GitHub.

Web App Pentest Lab — Business Logic & OWASP Top 10
Exploitation manuelle complète avec Burp Suite Pro (SQLi, SSRF, IDOR, XXE). Focus sur les vulnérabilités non détectées par les scanners automatiques.

Automatisation Pentest — Python/Bash Open Source
Scripts open-source pour automatiser la reconnaissance et l'exploitation en engagement réel — github.com/guyanikameni

CERTIFICATIONS

- ✓ CRTP — Altered Security
- ✓ CRTA — CyberWarfare Labs
- ✓ CRTS — CyberWarfare Labs · AD Red Team
- ✓ PNPT — TCM Security
- ✓ eCPPTv3 — INE Security
- ✓ eJPTv2 — INE Security
- ○ CRTO — Zero Point Security · sept. 2026
- ○ CPTS — HackTheBox · sept. 2026

FORMATION

MBA Expert en Cybersécurité — RNCP Niv. 7
Studi × HETIC · Paris · 2025–2027
Spécialisation Pentest & Red Team

Licence Informatique — Réseaux & Télécom
Univ. Marien-Ngouabi · Brazzaville · 2019–2023
Équivalence Niv. 6 RNCP/CEC

COMPÉTENCES TECHNIQUES

Outils : Nmap · Burp Suite Pro · BloodHound · Metasploit · Impacket · CrackMapExec

Active Directory : Kerberoasting · Pass-the-Hash · DCSync · Lateral Movement · Privilege Escalation · ACL Abuse

Web : OWASP Top 10 · SQLi · SSRF · XXE · IDOR · Business Logic Flaws

Social Engineering : Phishing · Pretexting · Campagnes ciblées

Scripting : Python · Bash · PowerShell

Systèmes : Kali Linux · Windows Server · Active Directory

Langues : Français (natif) · Anglais (courant)

MÉTHODOLOGIES

PTES · OWASP · MITRE ATT&CK · Cyber Kill Chain

OUTILS PUBLIÉS

Predat0r — crawler web de reconnaissance

CommentHunter — extraction de commentaires HTML (recon)

CENTRES D'INTÉRÊT

CTF : TryHackMe Top 2% · HackTheBox Active

Veille : Writeups Medium · R&D offensive · OSINT

DISPONIBILITÉ

CDI ou Freelance · Remote + déplacements
Île-de-France · Lyon · Mobilité nationale
Rapports FR/EN · Disponible immédiatement