GUYANI YOUMBI KAMENI

Offensive Pentester | Red Team & Active Directory

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

PROFILE

5 years · 16 engagements · 14 AD domains compromised. Whether through Kerberoasting, DCSync or ACL Abuse in Active Directory, a web application flaw (OWASP Top 10) or a phishing campaign — I always find the path that answers the client's question. Latest engagement: **SSRF chained into internal RCE**, reaching the internal network from the Internet. Author of technical writeups on Medium. Available immediately for offensive engagements, Red Team or complex AD audits.

PROFESSIONAL EXPERIENCE

Offensive Pentester — Confidential engagement · Healthcare sector | Apr 2026 – Jun 2026

→ Web, internal and external penetration test (Red Team approach). AD domain compromised: Kerberoasting → DCSync → **Domain Admin**.

→ SSRF on the exposed web application, chained into **internal RCE** — access to the internal network from the Internet.

→ Lateral movement via **Active Directory ACL abuse**. Bilingual FR/EN report: attack paths and prioritised remediation.

Offensive Security Pentester / Consultant — KALAO GLOBE TREK | Feb 2023 – Mar 2026

→ **15 clients compromised** — 100% remediation within 30 days. RCE, Kerberoasting, DCSync, SQLi, privilege escalation, lateral movement — PTES/OWASP methodology.

→ **20+ bilingual FR/EN reports** delivered to executive committee with CVSS scoring and actionable remediation plans. Accelerated security decisions on every engagement.

→ **Reduced post-engagement attack surface** by demonstrating realistic lateral-movement scenarios, translated into concrete recommendations for IT teams.

Information Security Analyst — KALAO GLOBE TREK | Sep 2021 – Feb 2023

→ **AD incidents handled end to end** (detection → containment → remediation) on Active Directory and Windows Server. Weekly threat-intelligence briefings shared with technical teams and management.

→ **First internal penetration tests** carried out independently with criticality-prioritised reports — direct foundation for the move into offensive pentesting.

KEY PROJECTS

AD Red Team Lab — Full documented Kill Chain
BloodHound → Kerberoasting → PTH → DCSync → Domain Admin compromised. Writeup published on Medium. Reproducible lab on GitHub.

Web App Pentest Lab — Business Logic & OWASP Top 10
Full manual exploitation with Burp Suite Pro (SQLi, SSRF, IDOR, XXE). Focus on vulnerabilities missed by automated scanners.

Pentest Automation — Python/Bash Open Source
Open-source scripts to automate recon and exploitation in real engagements — 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

EDUCATION

MBA Cybersecurity Expert — RNCP Level 7
Studi × HETIC · Paris · 2025–2027
Pentest & Red Team specialisation

BSc Computer Science — Networks & Telecom
Univ. Marien-Ngouabi · Brazzaville · 2019–2023
RNCP/EQF Level 6 equivalence

TECHNICAL SKILLS

Tools: 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 · Targeted campaigns

Scripting: Python · Bash · PowerShell

Systems: Kali Linux · Windows Server · Active Directory

Languages: French (native) · English (fluent)

METHODOLOGIES

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

PUBLISHED TOOLS

Predat0r — web reconnaissance crawler

CommentHunter — HTML comment extraction (recon)

INTERESTS

CTF: TryHackMe Top 2% · HackTheBox Active

Watch: Medium writeups · Offensive R&D · OSINT

AVAILABILITY

Permanent or freelance · Remote + travel
Paris · Lyon · Nationwide mobility
FR/EN reports · Available immediately