KALEAB ABDURAHMAN

Red Team Lead · Offensive Security Specialist · Exploit Researcher

kaleab8745@gmail.com https://kaluabd.github.io upwork.com/freelancers/~0172c8bd17d5c282b8
Addis Ababa, Ethiopia (Remote)

PROFILE HEADLINE

Red Team Lead & Exploit Researcher | National Cybersecurity Agency | MITRE ATT&CK |

PROFILE OVERVIEW

Red Team Lead and offensive security specialist with 4+ years embedded at Ethiopia's apex national cybersecurity authority (INSA), executing adversary simulations, exploit research, and full red team operations against critical infrastructure. I've held every role in the red team hierarchy — from Penetration Tester through to Red Team Lead — giving me rare end-to-end operational depth: I've executed the attacks myself and led the team that delivers them.

I deliver government-level confidentiality, high quality reporting, and full-lifecycle offensive engagements for international clients. Whether you need a comprehensive penetration test, an APT-style red team campaign, or a rigorous web application security review — I bring precision to every engagement.

- ✓ Government-grade operational security and confidentiality on every engagement
- ✓ Promoted through 5 roles at Ethiopia's national cybersecurity agency in 4+ years
- ✓ Full red team lifecycle: recon → enumeration → exploitation → persistence → objective → executive report
- ✓ Proficient in MITRE ATT&CK, OWASP Top 10 and EDR evasion
- ✓ Executive-level reporting that translates technical risk into business-impact language
- ✓ Available globally for remote engagements with rapid turnaround

PROFESSIONAL EXPERIENCE

Information Network Security Administration (INSA)

National Cybersecurity Authority · Addis Ababa, Ethiopia · Government

Feb 2022 – Present

INSA is the Federal Democratic Republic of Ethiopia's lead national cybersecurity authority, responsible for protecting the nation's critical information infrastructure, sovereign government networks, and digital strategic assets against state-sponsored actors, criminal syndicates, and advanced persistent threats. Progressively promoted through five distinct roles over four years of service.

Red Team Lead

Feb 2026 – Present

- Direct and coordinate adversary simulation operations at the national level, defining rules of engagement (ROE), campaign objectives, and operational timelines for engagements against critical information infrastructure.
- Lead a multi-person red team unit, mentoring senior and junior operators in offensive tradecraft, TTP execution, and post-exploitation methodology aligned to MITRE ATT&CK Enterprise.
- Architect and maintain red team infrastructure: command-and-control (C2) frameworks, phishing platforms, payload delivery pipelines, and redirector configurations for advanced, red team operations.
- Author and deliver executive threat briefings, red team operation reports, and strategic risk assessments consumed at agency and higher level, translating offensive findings into remediation mandates.
- Collaborate with blue team and SOC leadership on purple team exercises, adversary emulation plans, and detection engineering improvements informed by live red team telemetry.

Senior Red Teamer
Sep 2025 – Feb 2026

- Executed sophisticated multi-stage red team campaigns against hardened critical environments, achieving sustained network access with extended dwell periods while evading deployed EDR solutions and SIEM-based alerting.
- Conducted advanced Active Directory attacks — Kerberoasting, Pass-the-Hash, DCSync, Golden Ticket, Silver Ticket, and ACL-based privilege escalation — against a number of domains, mapping full Domain Admin compromise paths.
- Developed custom payload obfuscation, process injection techniques, and in-memory execution frameworks to bypass antivirus and endpoint detection during live engagements.
- Led structured technical debrief sessions with client security leadership following each red team engagement, presenting prioritized findings, exploitation chains, and actionable remediation roadmaps.

Junior Red Teamer
Feb 2025 – Sep 2025

- Joined the national red team and executed initial access, lateral movement, and privilege escalation operations against hardened targets under senior operator supervision.
- Applied adversary simulation methodology using MITRE ATT&CK TTP mapping; operated BloodHound/SharpHound for AD enumeration, CrackMapExec for lateral movement, and Impacket for credential-based attacks.
- Executed phishing and social engineering operations as the initial access component of red team campaigns, incorporating pretexting, credential harvesting, and payload delivery via crafted lure documents.
- Developed proficiency in post-exploitation tradecraft: LSASS memory dumping, credential extraction, persistence mechanisms (scheduled tasks, registry run keys, startup programs), and data exfiltration simulation.

Exploit Researcher
Jun 2023 – Feb 2025

- Conducted in-depth vulnerability research on software and systems deployed across national infrastructure: analyzing patch differentials, and developing simple exploitation proofs-of-concept for internal red team use.
- Produced exploit research reports and security briefings for national cybersecurity leadership, covering vulnerability severity analysis, exploitation feasibility, and coordinated disclosure timelines with affected vendors.
- Built and maintained AI based Python exploitation tools and automation frameworks for internal red team operations, significantly reducing manual effort across reconnaissance, payload staging, and post-exploitation workflows.
- Monitored and analyzed adversary threat research feeds, tracking APT TTPs targeting infrastructure and translating findings into actionable detection and hardening guidance for the national SOC.

Penetration Tester
Feb 2022 – Jun 2023

- Delivered external and internal network penetration tests, web application security assessments, and social engineering engagements against critical infrastructures and national infrastructure operators.
- Executed comprehensive OWASP Top 10 assessments across a number of web portals and internal applications, identifying and documenting critical vulnerabilities including SQL injection, authentication bypass, IDOR chains, XSS, and LFI.
- Conducted 100+ security audits across government entities, producing risk-ranked remediation roadmaps and compliance scorecards adopted as national security policy baseline — improving measurable compliance posture.
- Designed and executed spear-phishing and social engineering campaigns targeting high-privilege accounts, delivering quantified human risk assessments that directly drove enterprise-wide MFA implementation.
- Delivered structured penetration test reports with CVSS-scored findings, attack chain documentation, and executive summaries consumed by agency leadership, reducing Mean Time to Detect and Respond.

Independent Security Consultant — 2023 – Present
Remote · Upwork · Direct Referral · International Clients

Recognized as a Top-Rated cybersecurity professional on Upwork with a 100% Job Success Score, reflecting consistent delivery of high-quality penetration testing and security consulting services. Successfully completed 15+ engagements across web, network, and adversary simulation projects, earning 5.0 client ratings for technical depth, clear communication, and actionable reporting. I maintain rapid response time and strong client retention by translating complex vulnerabilities into business-focused risk insights.

- Executed full-scope web application penetration tests (OWASP Top 10) for SMB and enterprise clients, delivering CVSS-scored findings with business-impact context and remediation roadmaps within agreed turnaround timelines.
- Provided network penetration testing and vulnerability assessment services for clients requiring external attack surface validation prior to product launches, compliance audits, and investor due-diligence reviews.
- Authored and delivered executive security reports tailored to non-technical stakeholders, translating technical exploitation chains into business risk language that drives remediation decisions.
- Maintained perfect client confidentiality standards across all engagements; all findings, methodologies, and client data handled under strict information security protocols consistent with government-level operational standards.

SERVICES OFFERED

Full-Scope Penetration Testing External/internal network, web app, AD, social engineering — end-to-end with executive report	**Web Application Security** OWASP Top 10 assessment, API testing, auth bypass, injection flaws, business logic vulnerabilities	**Red Team Operations** APT-style adversary simulation aligned to MITRE ATT&CK. Stealth, lateral movement, persistence.
Active Directory Audit Enumeration, Kerberoasting, Pass-the-Hash, BloodHound analysis, privilege escalation mapping	**Social Engineering Ops** Spear-phishing, pretexting, vishing, physical security assessment, human risk quantification	**Vulnerability Assessment** Authenticated/unauthenticated scans, CVSS scoring, risk-ranked findings, remediation roadmaps
Incident Response Consulting Triage support, containment guidance, forensic analysis, post-incident reporting	**AI Assisted Security Code Review** Reviewed code for injection risks, credential exposure, logic flaws	**Exploit Research & Dev.** Custom PoC development, vulnerability analysis, security research reporting

PORTFOLIO HIGHLIGHTS

Category	Engagement	Key Outcome
RED TEAM	**APT Infrastructure Simulation**	Exposed critical segmentation failures; emergency patching at national level
AD ATTACK	**Active Directory Attack Chain Research**	Full Domain Admin path mapped & remediated pre-exploitation
EXPLOIT	**National Infrastructure Vuln. Research**	10+ high-severity PoCs developed; coordinated vendor disclosure
PHISHING	**Spear-Phishing Operation**	Campaign drove enterprise-wide MFA rollout across sensitive systems
WEB APP	**Government Portal Assessment**	SQLi, XSS, IDOR and LFI chains — patched within 72hr emergency cycle

AUDIT	**100+ System Compliance Audit Programme**	compliance improvement; adopted as national policy baseline
FREELANCE	**Web App Pentests (International Clients)**	OWASP-aligned reports; found critical findings across engagements

TECHNICAL TOOLKIT

Offensive	Metasploit Framework, Burp Suite Pro, Impacket Suite, BloodHound/SharpHound, CrackMapExec, Responder, Mimikatz, PowerSploit, Rubeus
Recon & OSINT	Nmap, Masscan, Gobuster, ffuf, Amass, theHarvester, Shodan, Maltego, Recon-ng
Exploitation	SQLmap, Nikto, Hydra, Hashcat, John the Ripper, ExploitDB / SearchSploit, BeEF
Languages	Python (tool dev, exploit scripting, automation), Bash
C2 / Infrastructure	Cobalt Strike (concepts & custom profiles), Havoc, Metasploit PRO, GoPhish (phishing infrastructure)
Defensive & SOC	Wireshark, AnyRun
Frameworks	MITRE ATT&CK, OWASP Top 10

CERTIFICATIONS

✓ **Practical Ethical Hacking (PEH)** — TCM Security	✓ **Junior Penetration Tester (eJPT)** — INE Security
✓ **CCNA: Introduction to Networks** — Cisco	✓ **Advent of Cyber 2024** — TryHackMe

EDUCATION

B.Sc. Computer Science — Rift Valley University
B.Sc. Mechanical Engineering — Hawassa University
B.A. Economics — Madda Walabu University

READY TO WORK

If you need someone who operates like a threat actor, thinks like a defender, and reports like an executive — let's talk.

kaleab8745@gmail.com · kaluabd.github.io · upwork.com/freelancers/~0172c8bd17d5c282b8