LARHRIB ISMAIL

+212 781-413701 | larhribismail87@gmail.com | Casablanca, Morocco
GitHub | LinkedIn

PROFILE

Software Engineering student at 1337 (UM6P) and 42 Paris, and aspiring SOC Analyst. Passionate about applying practical skills in threat detection, network forensics, and incident response. Recently achieved 1st place in the IDEH national Moroccan CTF with Team MIR4GE.

TECHNICAL SKILLS

- **Security Operations:** Alert Triage, SIEM (Splunk, ELK), EDR, SOAR, Incident Response, MITRE ATT&CK, Phishing Analysis & Remediation.
- **Network & Web Security:** Traffic Analysis (Wireshark), Snort, NetworkMiner, DDoS/SQLi Detection.
- **Systems & DevOps:** Linux Hardening (Debian), Docker, VirtualBox, Shell Scripting (Bash).
- **Programming:** C, C++, Python, HTML, CSS, JavaScript, Tailwind, React, Next.js, Nest.js, PostgreSQL.
- **Forensics:** Phishing Analysis, Malware Classification, Windows/Linux Log Analysis.

ACHIEVEMENTS & CERTIFICATIONS

- **1st Place IDEH national Moroccan CTF:** Secured 1st place finish with team MIR4GE (January 2026).
- **3rd Place Morocco Blockchain & Cryptocurrency Days CTF:** Secured a podium finish in the national finals with team MIRAGE.
- **Odyssey CTF Finals 2025:** Successfully cleared all Forensics/DFIR challenges in Morocco's premier cybersecurity event.
- **TryHackMe SOC Analyst L1:** Specialized path covering alert triage and log investigation (In Progress).
- **TryHackMe Memory Sleuth Badge:** Advanced memory forensic abilities (Top 0.1% of TryHackMe users).

TECHNICAL PROJECTS

ASSAS (Automated SOC Surveillance & Analytic Solution) *SaaS Startup, Log Analysis, Event Correlation*

- Architected and engineered a centralized SaaS security operations platform from scratch for real-time log ingestion, continuous monitoring, and event correlation.
- Developed custom interactive dashboards featuring automated alerting mechanisms for rapid incident triage and proactive threat hunting.

Inception (42/1337) *Docker, System Administration, Infrastructure*

- Orchestrated a secure, multi-container infrastructure using Docker Compose on a Debian VM.
- Configured Nginx (TLS), MariaDB, and WordPress as isolated services ensuring secure communication.

Minishell (42/1337) *C, Unix Logic, Process Management*

- Built a functional Bash-like shell from scratch, handling complex process pipes and signal management.

Born2beroot (42/1337) *System Hardening, Virtualization*

- Implemented a rigid Debian server with LVM partitioning, SSH hardening, and strict sudo policies.

EDUCATION

42 Paris | Paris, France 2026 – Present

Software Engineering

- Intensive Peer-to-Peer Curriculum focused on software architecture, networking, and cybersecurity.

1337 (UM6P) | Khouribga, Morocco 2024 – Present

Software Engineering

- Developed high-standard self-learning and peer code review skills.

TryHackMe & Cyber Defenders | Online 2023 – Present

Practical Cybersecurity Labs & CTF Challenges

- Practicing in blue-team labs to refine threat detection and analysis.

LANGUAGES

Arabic: Native | **French:** Fluent | **English:** Fluent