

MOHAMED FHAFAH

End-of-studies internship – IAM/PAM security, security audit, Active Directory pentest

Master's student in Cybersecurity (M2, FSI track), Aix-Marseille University, France – 6 months from February/March 2027

Marseille, France | +33 6 56 67 69 54 | mohamedfhafah975@gmail.com

linkedin.com/in/mohamed-fhafah | github.com/mohamedfhafah | mohamedfhafah.dev | Hack The Box: MohamedFAFA (ID 2771083)

PROFILE

Final-year Master's student in Reliability and Cybersecurity (SecNumedu-certified). In a supervised team research project, I owned identity and access management (IAM) on Entra ID (SAML 2.0 SSO, SCIM, ABAC) and AI agent identities; I practise penetration testing on Hack The Box, focusing on Active Directory (Pro Hacker, 36 machines).

EDUCATION

MSc in Computer Science, Reliability and Cybersecurity track (Master Informatique FSI) 2025 – 2027

Aix-Marseille University, Marseille – programme certified SecNumedu by ANSSI, the French national cybersecurity agency

- M1 completed with honours (mention Bien, 15.25/20). M2 in progress: cloud security, cryptography, software safety, advanced networking.

BSc in Computer Science (Licence) – Aix-Marseille University – mention Assez Bien

2022 – 2025

PROFESSIONAL EXPERIENCE

Cybersecurity Analyst Intern

April 2025 – June 2025 (2 months)

Tanger Alliance – TC3 container terminal, Tangier (Morocco)

- Ran an ISO 27001 / 27002 gap analysis of 3 security policies and procedures (passwords, vulnerabilities): maturity (CMM model), 15 prioritised recommendations (MFA, PAM, KPIs), 12-month roadmap, audit report for the IT department.
- Developed a security awareness platform following the audit (Flask, SQLAlchemy, Flask-Login): training and quizzes, simulated phishing campaigns tracking opens, clicks and reports.

PROJECTS

Supervised research project (M1, team) – Cloud identity security

May 2026 – July 2026

Aix-Marseille University, Marseille

- Answered an IAM/PAM specification for a MedTech SME: risk analysis, comparison of Entra ID, Okta, BeyondTrust and CyberArk, access policy aligned with ISO 27002 (controls 8.2 and 8.4), HDS health data rules and GDPR.
- My part, identity and access: SAML 2.0 federation between Entra ID (IdP) and GitLab (SP), with SCIM provisioning: automatic account creation, update and deactivation (joiner-mover-leaver lifecycle, JML).
- My part, AI agent identities: non-human account governance, ABAC with dynamic groups, legacy authentication blocking.

Active Directory lab (pair project): attack and hardening

Proxmox, Kerberos, BloodHound, GPO

- Three-VM domain (Windows Server domain controller, client workstation, attack machine): Kerberoasting, AS-REP roasting, DCSync and AD CS abuse, then remediation through a tiered administration model and GPOs.

CVE reproduction lab (M2)

Vagrant, Ansible, CERT-FR

- Automatically deployed vulnerable environments, analysis of CERT-FR advisories, replayable PoC exploit, IoC extraction and remediation plan following ANSSI guidelines.

Segmented enterprise network (M2)

Linux, Windows, firewall

- Segmentation into trust zones, out-of-band administration, DNS/DHCP, network flow matrix and acceptance test plan.

Consent-based telemetry platform (personal project, prototype)

Java 21, Kotlin/JavaFX, gRPC, PostgreSQL

- Hexagonal Java 21 microservices (ingestion, consent, provisioning): Ed25519-signed ingestion with replay protection, HMAC-chained audit log, OIDC/PKCE admin client, CI with JaCoCo/PMD/SpotBugs/SonarCloud.

SKILLS

- **Identity and Access Management (IAM):** federate applications through SSO (SAML 2.0, OIDC / OAuth 2.0), provision accounts (SCIM), configure access control (RBAC, ABAC) and Conditional Access (Entra ID, formerly Azure AD), manage secrets (HashiCorp Vault); Privileged Access Management (PAM) basics: policy and CyberArk/BeyondTrust comparison.
- **Active Directory penetration testing (lab and Hack The Box):** scan the network (Nmap), map attack paths (BloodHound), exploit ACLs, Kerberos delegation, NTLM relay and AD CS (Impacket, Certipy, Responder), then recommend hardening (tiered administration model, GPO).
- **Security audit and GRC (governance, risk, compliance):** run ISO 27001 / 27002 gap analyses, assess maturity, prioritise recommendations, write audit reports and roadmaps, integrate GDPR and HDS requirements.
- **Development and automation:** build secure applications in Java and Python (OIDC, Ed25519, HMAC audit log), program in C, script in Bash and PowerShell, use Docker and GitHub Actions (CI) on Linux.
- **Hack The Box (CTF platform, September 2026):** Pro Hacker rank – 36 machines, 5 Fortresses (incl. Synacktiv and Akerva), 2 Mini Pro Labs (Puppet, Mythical), 7 challenges, 3 Sherlocks.

LANGUAGES AND ADDITIONAL INFORMATION

Languages: Arabic (native), French (C2), English (C1) | **Mobility:** France and the EU | driving licence (B).