

MOHAMED FHAFAH

Stage de fin d'études – audit technique et test d'intrusion

Étudiant en Master 2 cybersécurité (parcours FSI), Aix-Marseille Université – 6 mois à partir de février/mars 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)

PROFIL

Étudiant en M2 Fiabilité et Sécurité Informatique (label SecNumedu de l'ANSSI). Je pratique les tests d'intrusion sur Hack The Box, surtout en Active Directory (rang Pro Hacker, 36 machines, 5 Fortresses dont Synacktiv et Akerva) : cartographie des chemins d'attaque avec BloodHound, faiblesses Kerberos, NTLM et AD CS, puis recommandations de durcissement. En stage, j'ai aussi rédigé un rapport d'audit ISO 27001 / 27002 restitué à la DSI.

FORMATION

Master Informatique, parcours Fiabilité et Sécurité Informatique (FSI) 2025 – 2027

Aix-Marseille Université, campus de Luminy – formation labellisée SecNumedu (ANSSI)

- M1 validé, mention Bien (15,25/20). M2 en cours : sécurité du cloud, cryptographie, sûreté logicielle, réseaux avancés.

Licence Informatique – Aix-Marseille Université, campus de Luminy – mention Assez Bien

2022 – 2025

EXPÉRIENCE PROFESSIONNELLE

Stagiaire analyste cybersécurité avril 2025 – juin 2025 (2 mois)

Tanger Alliance – terminal à conteneurs TC3, Tanger (Maroc)

- Analyse d'écarts ISO 27001 / 27002 de 3 politiques et procédures de sécurité (mots de passe, vulnérabilités) : maturité (modèle CMM), 15 recommandations priorisées (MFA, PAM, KPI), feuille de route sur 12 mois, rapport restitué à la DSI.
- Développement d'une plateforme de sensibilisation issue de l'audit (Flask, SQLAlchemy, Flask-Login) : formation et quiz, campagnes de phishing simulé avec suivi des ouvertures, clics et signalements.

PROJETS

Lab Active Directory en binôme : attaque et durcissement Proxmox, Kerberos, BloodHound, GPO

- Domaine à 3 machines virtuelles (contrôleur de domaine Windows Server, poste client, machine d'attaque) : Kerberoasting, AS-REP Roasting, DCSync et abus AD CS, puis remédiation par modèle d'administration en tiers et GPO.

Laboratoire de reproduction de CVE (M2) Vagrant, Ansible, CERT-FR

- Environnements vulnérables déployés automatiquement, analyse d'avis CERT-FR, exploit PoC rejouable, extraction d'loC et plan de remédiation selon les guides de l'ANSSI.

Projet de recherche encadré (TER M1, en équipe) – Sécurité des identités dans le cloud mai 2026 – juillet 2026

Aix-Marseille Université, Marseille

- Réponse à un cahier des charges IAM/PAM pour une PME MedTech : analyse de risques, comparatif Entra ID, Okta, BeyondTrust et CyberArk, politique d'accès alignée sur l'ISO 27002 (mesures 8.2 et 8.4), HDS et RGPD.
- Ma partie, identités et accès : fédération SSO SAML 2.0 entre Entra ID (IdP) et GitLab (SP), avec provisionnement SCIM : création, mise à jour et désactivation automatiques des comptes (cycle de vie Joiner-Mover-Leaver, JML).
- Ma partie, identités des agents IA : gouvernance des comptes techniques (identités non humaines), ABAC par groupes dynamiques, blocage de l'authentification héritée.

Réseau d'entreprise segmenté (M2) Linux, Windows, pare-feu

- Segmentation en zones de confiance, administration hors bande, DNS/DHCP, matrice de flux et plan de recette.

COMPÉTENCES

- **Tests d'intrusion Active Directory (lab et Hack The Box)** : reconnaître le réseau (Nmap), cartographier les chemins d'attaque (BloodHound), exploiter les ACL, la délégation Kerberos, le relais NTLM et AD CS (Impacket, Certipy, Responder), puis proposer un durcissement (modèle d'administration en tiers, GPO).
- **Hack The Box (plateforme CTF, septembre 2026)** : rang Pro Hacker – 36 machines, 5 Fortresses (dont Synacktiv et Akerva), 2 Mini Pro Labs (Puppet, Mythical), 7 challenges, 3 Sherlocks.
- **Audit et GRC (gouvernance, risques, conformité)** : mener une analyse d'écarts ISO 27001 / 27002, évaluer la maturité, prioriser des recommandations, rédiger un rapport d'audit et une feuille de route, intégrer les exigences RGPD et HDS.
- **Identity and Access Management (IAM)** : fédérer des applications par SSO (SAML 2.0, OIDC / OAuth 2.0), provisionner les comptes (SCIM), configurer le contrôle d'accès (RBAC, ABAC) et l'accès conditionnel (Entra ID, ex-Azure AD), gérer des secrets (HashiCorp Vault) ; notions de Privileged Access Management (PAM) : politique et comparatif CyberArk/BeyondTrust.
- **Développement et automatisation** : développer des applications sécurisées en Java et Python (OIDC, Ed25519, audit HMAC), programmer en C, scripter en Bash et PowerShell, utiliser Docker et GitHub Actions (CI) sous Linux.

LANGUES ET INFORMATIONS

Langues : arabe (langue maternelle), français (C2), anglais (C1) | **Mobilité** : France entière | permis B.