



HACK THE BOX

36 machines résolues
5 Fortresses sur 6
2 Mini Pro Labs

Rang Pro Hacker · [MohamedFAFA](#)
Fortresses : Jet, Akerva, Faraday, Synacktiv, Context. Mini Pro Labs : Puppet, Mythical. 7 challenges, 3 Sherlocks (profil public, septembre 2026).

COMPÉTENCES

Gérer les identités et les accès (IAM)

Entra ID SAML 2.0 OIDC SCIM
RBAC / ABAC Accès conditionnel
HashiCorp Vault PAM (notions)

SSO et SCIM entre Entra ID et GitLab (TER)

Attaquer et durcir l'AD

Active Directory Kerberos NTLM
AD CS BloodHound Impacket
Certipy GPO

Write-ups Hack The Box : Logging, Garfield, Puppet

Auditer la conformité (GRC)

ISO 27001 / 27002 Maturité CMM
Rapport d'audit RGPD HDS

15 recommandations prioritisées (Tanger Alliance)

Développer et automatiser

Python Java C Bash
PowerShell Docker GitHub Actions
Linux

Client OIDC/PKCE, signature Ed25519 (télémétrie)

LANGUES

Français C2
Anglais C1
Arabe langue maternelle

DISPONIBILITÉ

6 mois dès février/mars 2027
Mobilité France entière · permis B

MOHAMED FHAFAH

Master 2 Cybersécurité · IAM/PAM, audit et pentest AD

Marseille, France +33 6 56 67 69 54 mohamedfhafah975@gmail.com
linkedin.com/in/mohamed-fhafah github.com/mohamedfhafah mohamedfhafah.dev

🕒 Stage de fin d'études · 6 mois · dès février/mars 2027

Étudiant en M2 Fiabilité et Sécurité Informatique (label SecNumedu de l'ANSSI). En projet de recherche encadré en équipe, j'ai pris en charge l'IAM sur Entra ID – SSO SAML 2.0, SCIM, ABAC – et les identités des agents IA ; je pratique les tests d'intrusion sur Hack The Box, notamment en Active Directory.

FORMATION

- Master Informatique, parcours FSI 2025 – 2027
Aix-Marseille Université, Luminy · label SecNumedu (ANSSI)
M1 validé avec **mention Bien** (15,25/20). M2 en cours : sécurité du cloud, cryptographie, sûreté logicielle, réseaux avancés.
- Licence Informatique 2022 – 2025
Aix-Marseille Université, Luminy · mention Assez Bien

EXPÉRIENCE ET RECHERCHE

- Projet de recherche encadré (TER M1, en équipe) mai 2026 – juillet 2026
Sécurité des identités dans le cloud, Aix-Marseille Université · Marseille
 - Réponse à un cahier des charges IAM/PAM (PME MedTech) : analyse de risques, comparatif Entra ID, Okta, BeyondTrust et CyberArk, politique d'accès alignée sur l'ISO 27002, HDS et RGPD.
 - Ma partie, identités et accès : fédération SSO **SAML 2.0** entre Entra ID (IdP) et GitLab (SP), provisionnement **SCIM**, cycle de vie des comptes automatisé (JML).
 - Ma partie, **identités des agents IA** : gouvernance des comptes techniques, ABAC par groupes dynamiques, blocage de l'authentification héritée.
- Stagiaire analyste cybersécurité avril 2025 – juin 2025
Tanger Alliance, terminal à conteneurs TC3 · Tanger (Maroc), 2 mois
 - Analyse d'écarts **ISO 27001/27002** de 3 politiques et procédures (mots de passe, vulnérabilités) : maturité CMM, **15 recommandations prioritisées** (MFA, PAM, KPI), feuille de route sur 12 mois, rapport restitué à la DSI.
 - Plateforme de sensibilisation (Flask, SQLAlchemy, Flask-Login) : formation, quiz, **campagnes de phishing simulé** avec suivi des ouvertures, clics et signalements.

PROJETS TECHNIQUES

🏢 Lab Active Directory (binôme)

Domaine AD à 3 VM sous Proxmox : Kerberoasting, AS-REP Roasting, DCSync, abus AD CS. Cartographie BloodHound, puis remédiation par administration en tiers et GPO.

Kerberos BloodHound GPO

🛠️ Reproduction de CVE (M2)

Cibles déployées par Vagrant et Ansible, analyse d'avis CERT-FR, exploit PoC rejouable, IoC et remédiation (guides ANSSI).

Vagrant Ansible CERT-FR

🏠 Réseau d'entreprise (M2)

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

Linux Windows Pare-feu

👤 Télémétrie avec consentement

Prototype personnel : microservices Java 21 hexagonaux, ingestion signée Ed25519 anti-rejeu, journal d'audit chaîné HMAC, client d'administration OIDC/PKCE, CI JaCoCo/PMD/SonarCloud.

Java 21 JavaFX gRPC PostgreSQL