🔐 TP – Mise en place d'une authentification multifactorielle (MFA)

Un atelier pratique pour sécuriser l'accès à vos services internes avec une authentification renforcée

1️⃣ Objectif du TP

Sécuriser l'accès

Protéger un site interne avec une authentification renforcée appelée MFA (Multi-Factor Authentication)

Protection renforcée

Empêcher l'accès même si le mot de passe est connu ou compromis

Double facteur

Combinaison de deux méthodes d'authentification pour garantir la sécurité

2️⃣ Contexte de sécurité

Infrastructure classique

L'accès repose souvent uniquement sur un **login + mot de passe**. Ce mécanisme est aujourd'hui **insuffisant** face aux menaces modernes.

1

Vol

Exfiltration de données d'identification

2

Bruteforce

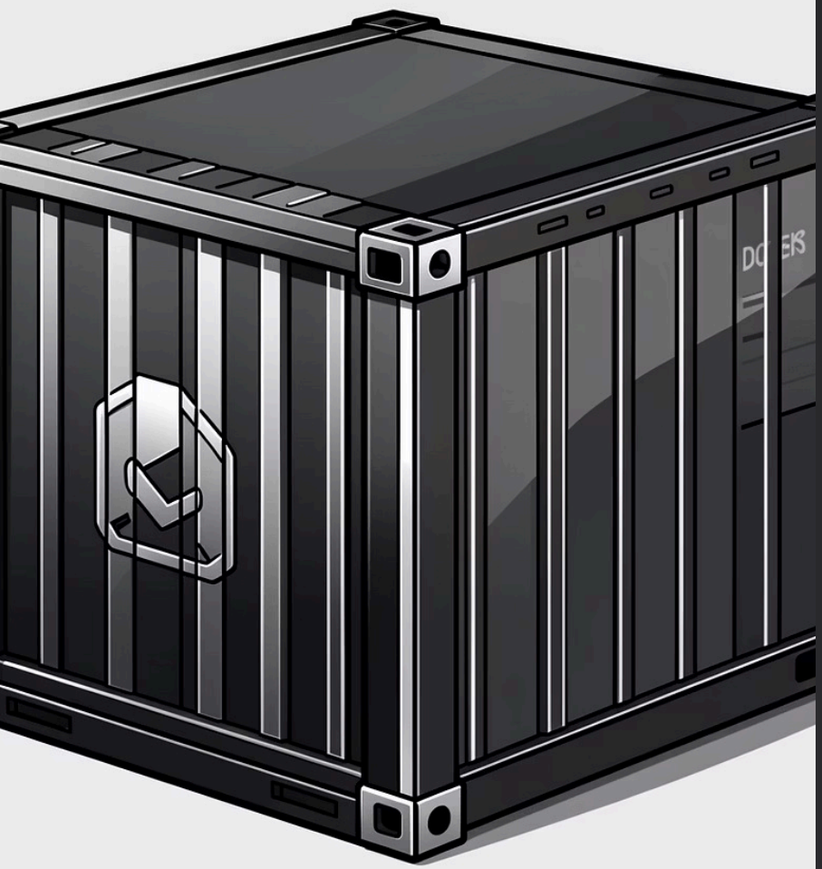
Tentatives répétées pour deviner le mot de passe

3

Réutilisation

Utilisation du même mot de passe sur plusieurs services

Il est donc **nécessaire d'ajouter un second facteur de sécurité** pour garantir l'authenticité de l'utilisateur.



3️⃣ Solution retenue : Authelia

1

Open-source

Code source libre et auditable par la communauté

2

Authentification centralisée

Gestion unique des identifiants pour plusieurs services

3

Support MFA intégré

Implémentation native de l'authentification à double facteur

4

Déploiement Docker

Installation et gestion simplifiées avec conteneurs

4️⃣ Architecture mise en place

L'infrastructure repose sur **2 machines virtuelles Ubuntu** communiquant entre elles :

VM 1 : Authentification

- Authelia (serveur d'authentification)
- Docker & Docker Compose
- Gestion des utilisateurs

VM 2 : Service

- Site web interne : intranet.local
- Service protégé
- Accès conditionnel

Schéma de fonctionnement

1

Utilisateur

Demande d'accès

2

intranet.local

Redirection vers Authelia

3

Authelia

Authentification MFA

4

Autorisation

Accès accordé ou refusé

5 Création des utilisateurs

Fichier users.yml

Les utilisateurs sont définis dans un fichier de configuration YAML structuré.

Compte créé

Identifiant : admin

Mot de passe : Admin123!

01

Hashage bcrypt

Mot de passe haché avec l'algorithme bcrypt

02

Stockage sécurisé

Jamais stocké en clair dans la configuration

03

Validation

Vérification du hash lors de chaque connexion

6 Mise en place du MFA

Le MFA utilisé repose sur le **code temporaire à 6 chiffres** généré par une application mobile compatible TOTP (Time-based One-Time Password).

Identifiants

Saisie du login et mot de passe

Code MFA

Saisie du code à 6 chiffres de l'application

Accès autorisé

Validation et accès au service

Sans le code MFA, l'accès est systématiquement refusé, même avec le bon mot de passe.

7️⃣ Règles de sécurité

Configuration des règles

Des règles sont définies dans Authelia pour contrôler l'accès aux différents services.

- Accès par défaut **bloqué**
- Domaine intranet.local **protégé**
- Politique de sécurité personnalisée

two_factor

MFA activé : authentification à double facteur obligatoire pour accéder au service

one_factor

MFA désactivé : accès autorisé avec uniquement le mot de passe (moins sécurisé)

8️⃣ Tests réalisés

Plusieurs scénarios ont été testés pour valider l'efficacité du MFA :

❌ Test 1

Accès sans authentification

Résultat : Accès refusé

Le système bloque automatiquement toute tentative sans identifiants

❌ Test 2

Accès avec mot de passe seul

Résultat : Accès refusé

Le MFA est requis, le mot de passe ne suffit pas

✅ Test 3

Accès avec mot de passe + code MFA

Résultat : Accès autorisé

Authentification complète réussie

Ces tests démontrent l'**efficacité du MFA** dans la protection des accès.

9️⃣ Désactivation du MFA (test comparatif)

Modification de la configuration

Le MFA peut être désactivé en modifiant la règle dans la configuration :

```
policy: one_factor
```

Cette modification change la politique de sécurité du service.

Configuration initiale

policy: two_factor (MFA activé)

1

Modification

Changement de la règle de sécurité

2

Résultat

Accès possible avec mot de passe seul

3

Comparaison claire

Cette manipulation permet de comparer visiblement la différence entre une configuration **avec MFA** et **sans MFA**, illustrant l'importance de la double authentification pour la sécurité.