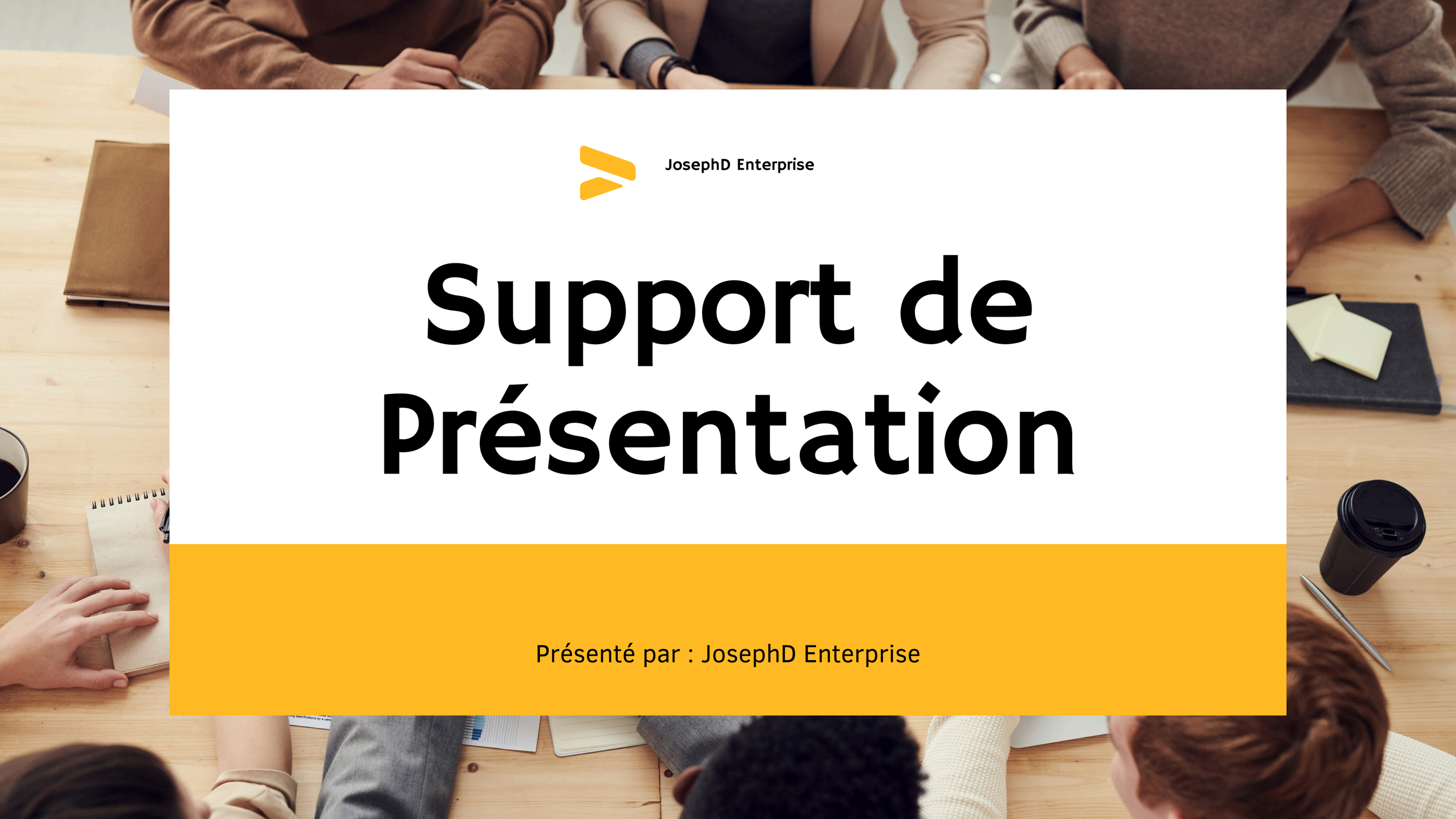

JosephD Enterprise

Support de Présentation

Présenté par : JosephD Enterprise

Sommaire

Audit de Sécurité de FramaFTP

Contexte de l’audit

En tant que consultant en sécurité, nous avons été chargés de mener un audit de sécurité sur leur infrastructure pour identifier et corriger les vulnérabilités potentielles.

Périmètre de test

Le périmètre de ce test d'intrusion inclut l’adresse IP suivante :

- 172.16.239.10

Objectifs principaux

L'objectif principal du test d'intrusion est de découvrir et démontrer un maximum de failles de sécurité présentes dans l'infrastructure de FramaFTP.

Évaluation du Niveau de Risque

Vulnérabilités critiques et hautes identifiées

- Identification et Authentification Failures (Critique)
  - Mots de passe faibles acceptés lors de l'enregistrement.
- Broken Access Control (Haut)
  - Accès et modification de fichiers via FTP sans restriction adéquate.

Risques potentiels pour FramaFTP

- Perte de confiance des clients
- Potentiel impact financier
- Dommages à la réputation

Impact sur la confidentialité, l'intégrité et la disponibilité des données

- Confidentialité : Exposition des données sensibles des utilisateurs
- Intégrité : Altération ou suppression des données critiques
- Disponibilité : Interruption des services, rendant FramaFTP inaccessible

Principales vulnérabilités

Point clés

- Mots de passe faibles (Critique)
- Accès FTP non restreint (Haute)
- Faille LFI (Critique)
- Changement non autorisé de mot de passe via SSH (Critique)

Conséquences Métier des Vulnérabilités

Risques d'accès non autorisé aux données sensibles

Les vulnérabilités permettent à des attaquants d'accéder à des fichiers sensibles, compromettant la confidentialité des utilisateurs.

Perturbation possible du service

Les failles peuvent être exploitées pour interrompre le service, provoquant une déni de service et rendant FramaFTP inaccessible.

Perte de confiance des utilisateurs

La découverte de ces failles peut nuire à la réputation de FramaFTP, entraînant une perte de confiance et une baisse du nombre d'utilisateurs.

Recommandations Clés

Implémenter une politique de mots de passe forts

Restreindre l'accès FTP et utiliser des connexions sécurisées

Auditer régulièrement les permissions des utilisateurs

Mettre en place des contrôles de validation pour prévenir les inclusions de fichiers (LFI)

Détails Techniques des Vulnérabilités

Vulnérabilité	Description	Méthode d’exploitation	**Criticité**
Faiblesse des mots de passe	Les mots de passe des utilisateurs sont faibles et faciles à deviner.	Utilisation de Patator pour effectuer un brute-force des mots de passe.	Critique
Accès FTP non restreint	Le service FTP permet un accès non restreint et non sécurisé.	Connexion FTP non sécurisée avec possibilité de transférer des fichiers.	Haute
Faille LFI	Inclusion de fichiers locaux via des paramètres d'URL.	Exploitation de la faille pour accéder à des fichiers sensibles via l'URL.	Critique
Changement non autorisé de mot de passe via SSH	Utilisateur Michel capable de changer son mot de passe SSH sans autorisation.	Utilisation de la commande chsh -s /bin/sh michel pour obtenir un shell root.	Critique
Possibilité de commande via navigateur	Exécution de commandes système via des scripts PHP injectés.	Injection de scripts PHP pour exécuter des commandes système via le navigateur.	Critique

Méthodologie de test

Recherche sur internet d'information sur FramaFTP

Scan des ports avec Nmap

Tests d'injection (XSS, CSRF, SQL, LFI)

- Exploitation des failles LFI
- Tentatives de brute-force

Exemples Concrets

Accès à /etc/passwd via LFI

Exécution de commandes système via Burp Suite

Changement de mot de passe de l'utilisateur michel via SSH après l’avoir bruteforce

Recommandations Techniques

- Renforcement des politiques de sécurité des mots de passe
- Mise en place de connexions sécurisées pour les services FTP et SSH
- Validation et nettoyage des entrées utilisateurs pour éviter les inclusions de fichiers
- Configuration des accès et des permissions de manière restrictive

Merci !

N'hésitez pas à nous poser des questions.