Rapport Exécutif – Test d’Intrusion

Client : [non spécifié]

Période d’intervention : [non spécifiée]

Consultant en cybersécurité : [non spécifié]

# 1. Contexte et Objectif

Un test d’intrusion a été mené sur les systèmes associés aux domaines comme openmrs.org, trailskills.org, etc., dans un cadre légal.  
L’objectif : identifier les failles de sécurité exploitables par un attaquant, évaluer les risques, et proposer des actions concrètes pour renforcer la sécurité.

# 2. Résumé des Résultats

- Technologies obsolètes détectées : certains serveurs web utilisent des versions anciennes de logiciels comme Apache ou OpenSSH, connues pour contenir des failles de sécurité.  
- Absence de protections de base : plusieurs sites n’intègrent pas les en-têtes de sécurité HTTP standards, ce qui les rend vulnérables à des attaques simples (ex : usurpation, vol de session).  
- Utilisation de WordPress : détecté sur plusieurs sites. Ce CMS est souvent la cible d’attaques, surtout si les plugins ne sont pas à jour.  
- Services sensibles accessibles : le service SSH (accès distant) est exposé publiquement, ce qui représente un risque important si mal configuré.

# 3. Principaux Risques

- Risque d’intrusion : via des failles connues sur des services non mis à jour.  
- Vol ou altération de données : notamment si un CMS comme WordPress est compromis.  
- Dégradation de l’image de l’entreprise : en cas d’exploitation publique ou défacement de site.  
- Responsabilité légale : en cas d’exposition de données personnelles.

# 4. Recommandations Clés

- Mettre à jour les logiciels : appliquer les correctifs de sécurité sur les serveurs et CMS.  
- Renforcer les configurations web : intégrer des protections comme HTTPS strict, en-têtes de sécurité, pare-feu applicatif.  
- Réduire la surface d’attaque : fermer les accès inutiles, protéger les interfaces d’administration.  
- Effectuer des audits réguliers : pour garantir la conformité et anticiper les nouvelles menaces.

# 5. Conclusion

Le test a permis de détecter plusieurs failles techniques exploitables. Si elles ne sont pas traitées, elles exposent l’organisation à des attaques.  
Un plan d’action rapide est recommandé pour corriger les vulnérabilités identifiées et sécuriser durablement les systèmes.