Rapport Technique de Test d’Intrusion

Client : [non spécifié]

Période d'intervention : [non spécifiée]

Pentester : [non spécifié]

# 1. Objectif

Évaluer la sécurité d’un ou plusieurs systèmes appartenant à des domaines cibles tels que `openmrs.org`, `trailskills.org`, etc., dans le cadre d’un test d’intrusion légal. Le but est d’identifier les vulnérabilités techniques et de fournir des recommandations d’atténuation.

# 2. Méthodologie

La méthodologie s’est basée sur les phases suivantes :  
- Collecte d’informations passive et active : via WHOIS, DNS, HTTP headers.  
- Fingerprinting : WhatWeb, nmap.  
- Scanning de ports/services : nmap.  
- Reconnaissance Web : curl, WhatWeb.  
- Tentatives d’énumération ou d’exploitation non incluses dans le fichier mais potentiellement prévues.

# 3. Résultats

## 3.1. Collecte d'informations

WHOIS - Exemple openmrs.org :  
- Domaine enregistré via GoDaddy.  
- Adresse administrative et email : domainabuse@service.com.  
- Aucun nom de serveur personnalisé détecté.

## 3.2. Fingerprinting Web (WhatWeb)

Exemple https://openmrs.org :  
- Technologies détectées : WordPress, Google Analytics, jQuery  
- HTTP/2 activé  
- Aucun en-tête de sécurité détecté (X-Frame-Options, Content-Security-Policy, etc.)  
  
Exemple http://trailskills.org :  
- Redirection vers HTTPS (301).  
- WordPress détecté (version non identifiée).

## 3.3. En-têtes HTTP (curl -I)

trailskills.org :  
HTTP/1.1 301 Moved Permanently  
Server: Apache  
Location: https://trailskills.org/  
  
openmrs.org :  
HTTP/2 200  
Content-Type: text/html  
Server: nginx

## 3.4. Scan Nmap

IP : 104.248.113.199 (associée à trailskills.org) :  
PORT STATE SERVICE VERSION  
22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.3  
80/tcp open http Apache httpd 2.4.29 ((Ubuntu))  
443/tcp open ssl/https?  
  
- OpenSSH vulnérable si mal configuré.  
- Apache 2.4.29 : des CVE connues.  
- Pas de bannières complètes sur SSL.

# 4. Vulnérabilités potentielles identifiées

|  |  |  |  |
| --- | --- | --- | --- |
| Élément | Vulnérabilité potentielle | Gravité | Recommandation |
| Absence de headers de sécurité | Clickjacking, XSS | Moyenne | Implémenter CSP, HSTS, X-Frame-Options |
| Apache 2.4.29 (Ubuntu) | Multiples CVE (RCE, Priv Esc) | Élevée | Mettre à jour Apache |
| WordPress détecté | Attaques connues via plugins | Moyenne | Scanner avec WPScan, restreindre accès admin |
| OpenSSH 7.6p1 | Vulnérabilités connues | Moyenne | Vérifier les patchs, désactiver root login |

# 5. Recommandations générales

- Mettre à jour tous les logiciels à leurs dernières versions stables.  
- Mettre en place des en-têtes HTTP de sécurité.  
- Auditer les configurations WordPress, y compris les plugins et thèmes.  
- Restreindre les services exposés au strict nécessaire (ex : SSH).  
- Effectuer un audit complet des CMS détectés.