Rapport Pentest example.com :

Introduction :

Nous avons le plaisir de vous présenter le rapport de pentest réalisé pour [Nom du Client/Entreprise]. Ce rapport a été préparé par notre équipe d'experts en cybersécurité, avec l'objectif de fournir une évaluation complète et détaillée de la posture de sécurité de votre infrastructure informatique.

L'objectif principal de ce pentest était de détecter et d'évaluer les vulnérabilités potentielles au sein de votre environnement réseau et des applications. En simulant des attaques réalistes, nous avons pu identifier les faiblesses qui pourraient être exploitées par des acteurs malveillants et proposer des mesures correctives pour renforcer vos défenses contre de telles menaces.

Le rapport suivant détaille nos méthodologies, nos découvertes, les risques associés et fournit des recommandations stratégiques pour améliorer la sécurité de votre système d'information. Nous avons structuré le rapport pour offrir une vue d'ensemble claire dans la section "Synthèse", suivie de détails techniques dans les sections subséquentes.

Table des Matières

1. Introduction

- Présentation du rapport
- Objectifs du pentest

2. Synthèse

- Aperçu des résultats principaux

3. Détails des Vulnérabilités

- CVE Testées et Validées
- Description et impact des vulnérabilités

4. Tests Effectués

- Dirscan
- URLs relevées
- Scan Nmap
- Services Obsolètes
- CMS
- Plugins
- Utilisateurs Relevés
- SSH

5. Analyses et Recommandations

- Analyse des résultats
- Recommandations de sécurité

6. Conclusion

- Récapitulatif des découvertes
- Prochaines étapes

7. Annexes

- Données techniques supplémentaires
- Graphiques et tableaux

1. Synthèse

Le pentest automatisée effectué concerne le site example.com.

- Nous n'avons pas relevé de services sur le site.
- Il n'existe pas de services obsolètes sur le site.
- Nous avons relevé des PoCs publics sur le site.
- Nous avons validé une vulnérabilité connue sur le site.
- Nous n'avons pas relevé de CMS sur le site.
- Nous avons trouvé un port SSH sur le site.
- La connexion SSH est sécurisée.

2. CVE Testées Validées

- Pour chaque CVE :
    - Titre : Vulnérabilité dans Apache Struts
    - CVE : CVE-2017-5638
    - Catégorie OWASP : Injection
    - Description : Une vulnérabilité d'exécution de code à distance dans Apache Struts.
    - Risque : Élevé
    - Remédiation : Mise à jour vers la version x.x.x

3. Tests Effectués

- Dirscan :
    - URLs relevées :
        - Pages admin : url1, url2
        - Pages connexion : url3, url4
        - Pages backup : url5, url6
        - Pages API : url7, url8
        - Pages données txt : url9, url10
        - Pages dev : url11, url12

4. Scan Nmap

- Pour chaque résultat :
    - Port : 22
    - Nom du service : SSH
    - Version : OpenSSH 7.9p1 Debian 10+deb10u2

5. Services Obsolètes

- Pour chaque service :
    - Nom : Apache
    - Version : OpenSSH 7.9p1 Debian 10+deb10u2
    - Nombre CVE : 5
    - Nombre PoCs publics : 2
    - URLs PoCs publics : url_poc1, url_poc2

6. CMS

CMS :

Nom	Version	Nombre CVE	Nombre PoCs publics	URLs PoCs publics
WordPress	5.4	10	3	url_poc1, url_poc2, url_poc3

Thèmes :

Nom	Version	CVES
theme1	1.2	CVE-xxxx-xxxx, CVE-yyyy-yyyy

Plugins :

Nom	Version	CVES
plugin1	3.5	CVE-zzzz-zzzz, CVE-aaaa-aaaa

7. Utilisateurs Relevés

Utilisateurs relevés	admin

8. SSH

Nom du Service	Version	Root Disable	Password Connexion	Fail2Ban
OpenSSH	7.4	Activé	Oui	Non

Nous vous remercions pour la confiance que vous nous avez accordée pour effectuer cette évaluation critique. Votre engagement envers la sécurité de vos systèmes est un pas important vers la protection de vos actifs numériques et de la confiance de vos clients.

Nous restons à votre disposition pour toute question ou éclaircissement concernant ce rapport et nous sommes prêts à vous assister dans la mise en œuvre des recommandations.