Rapport d'Audit de Pentest

Table des Matières

Introduction

Cet audit de pentest a été réalisé dans le cadre d'un entretien d'embauche pour le poste de pentesteur chez Orange Cyber Defense. L'objectif principal est de démontrer mes compétences en matière de sécurité informatique et d'évaluation des vulnérabilités. Cet audit est une simulation pratique visant à identifier et évaluer les vulnérabilités au sein d'une infrastructure prédéfinie. Les résultats obtenus permettront de mettre en évidence mes capacités à mener des tests de pénétration et à fournir des recommandations de sécurité pertinentes.

Objectifs de l'Audit

Décrivez les objectifs principaux de l'audit de pentest, par exemple :

- Identifier et évaluer les vulnérabilités de sécurité présentes dans l'infrastructure.
- Fournir des recommandations pour remédier aux vulnérabilités identifiées.

Méthodologie

L'audit de pentest s'est déroulé en plusieurs phases, chacune ayant un objectif spécifique et utilisant des outils appropriés.

Reconnaissance (Reconnaissance Active et Passive)

La phase de reconnaissance a pour but de recueillir des informations sur la cible de manière passive et active. Pour la reconnaissance passive, nous avons utilisé des outils comme `Whois` pour obtenir des informations sur le domaine, et avons effectué une analyse de DNS et une recherche sur Google Dorking. Ensuite, la reconnaissance active a impliqué l'utilisation d'outils tels que `Nmap` pour scanner les ports ouverts et les services actifs, ainsi que `Dirbuster` pour identifier les répertoires et fichiers cachés sur le serveur cible.

Analyse de Vulnérabilités

Cette phase vise à identifier les vulnérabilités présentes dans les systèmes et les applications de la cible. Nous avons employé des scanners de vulnérabilités comme `Nessus` et `OpenVAS` pour effectuer un balayage complet des systèmes, tandis que `Burp Suite` a été utilisé pour analyser les applications web et détecter des vulnérabilités spécifiques telles que les injections SQL, XSS et LFI.

Exploitation

L'objectif de la phase d'exploitation est d'exploiter les vulnérabilités identifiées pour accéder aux systèmes de la cible. Nous avons utilisé `Metasploit` pour exploiter les vulnérabilités critiques, `SQLmap` pour automatiser les injections SQL, et `Hydra` pour mener des attaques par force brute sur les services exposés.

Post-Exploitation

Une fois les systèmes compromis, la phase de post-exploitation se concentre sur le maintien de l'accès et l'extraction d'informations sensibles. Nous avons utilisé `Mimikatz` pour extraire les informations d'identification de la mémoire, ainsi que `Powersploit` pour effectuer diverses tâches de post-exploitation sur les systèmes Windows.

Rapport

Enfin, la phase de rapport consiste à documenter toutes les vulnérabilités identifiées, les méthodes d'exploitation utilisées, et les recommandations de sécurité. Cette documentation est réalisée en utilisant des outils comme Markdown, LaTeX ou Microsoft Word, et inclut des captures d'écran, des descriptions détaillées et des recommandations de remédiation.

Outils et Techniques Utilisés

Pour mener cet audit, plusieurs outils et techniques ont été utilisés. `Nmap` a servi à identifier les ports ouverts et les services actifs. `Dirbuster` a été utilisé pour découvrir des fichiers et répertoires cachés. `Burp Suite` a été essentiel pour l'analyse approfondie de l'application web. Pour l'exploitation des vulnérabilités, nous avons utilisé `pwncat`, et `SQLmap` pour les injections SQL. `Hashcat` a été employé pour tester la robustesse des identifiants d'accès par force brute.

Résumé Exécutif

Fournissez un résumé des principales découvertes de l'audit. Cette section devrait donner une vue d'ensemble des vulnérabilités critiques et des recommandations clés.

Faire tableau recap des faille

Critique	Moyenne	Faible
SQL		
LFI		
.git		

Scénario d'exploitation

Compromission de la machine

> Nmap, dirbuster,Sqlmap, SQLI, Uploads de fichier (RCE),git log git status git show ⇒ trouver compte admin ⇒ RCE ⇒ leenpeas ⇒ USER ⇒ ROOT

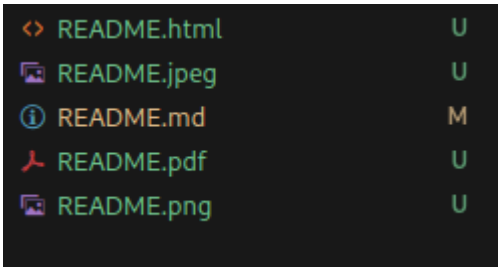
Nous avons commencé par un scan `Nmap` sur l'ip de la machine. Celui-ci nous a permis de constater que les ports 80 (Web HTTP), 443 (Web HTTPS) sont ouverts. Nous avons donc de suite lancer une énumération de dossiers sur le serveur web avec `Dirbuster`.

`Expliquer le cheminement global. (Ne pas hésiter a faire des réference)`

Vulnérabilités Elevées

SQLI

Nous avons trouvé une injection SQL su le paramêtre <>



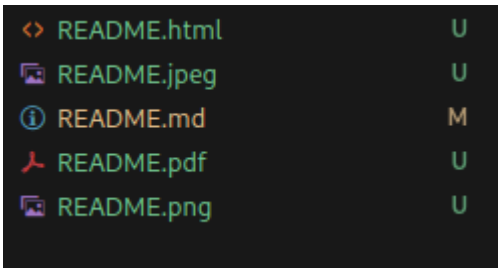
Remédiation

Il faudrait utilisé les PDO et faire des requêtes preparées

Exposition de l'historique du code source

Nous avons trouvé dans l'application Web le dossier .git qui contient l'ensemble des commits github du code source.

Ce dossier contenait des Secrets utilisateurs

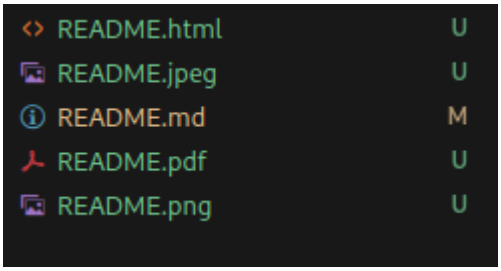


Remédiation

Ne pas deployer le .git dans les fichiers accèssible en production.

LFI

En ce qui concerne la faille LFI,



Remédiation

Vulnérabilités Moyennes

Même structure que pour les vulnérabilités critiques.

Vulnérabilités Faibles

Même structure que pour les vulnérabilités critiques.

Conclusion

Résumez les principales conclusions de l'audit et réitérez les recommandations clés. Mentionnez les prochaines étapes possibles pour l'organisation.

Annexes

Incluez ici toute information supplémentaire pertinente, comme des logs, des scripts utilisés, des diagrammes de réseau, etc.