PROJET TEST D'INTRUSION AVEC PYTHON

INTRODUCTION

OWASP Broken Web Applications Project propose une collection de diverses applications web intentionnellement vulnérables, conçues pour aider les utilisateurs à pratiquer les tests de sécurité des applications web. Le projet peut être téléchargé sous forme de machine virtuelle.

PREREQUIS

1) Téléchargez l'environnement souhaité depuis le site correspondant ;
2) Importez la machine virtuelle dans votre logiciel de virtualisation préféré (VirtualBox, VMware, etc.) ;
3) Configurez le réseau de la machine virtuelle pour qu'elle soit accessible depuis votre réseau de test local ;

CONTENU DU TRAVAIL DEMANDE

Lancez la machine virtuelle et commencez vos tests d'intrusion en utilisant les outils Python sur les applications BWAPP et Wordpress.

Pour chacune des applications, il faut utiliser les phases de Test d'intrusion vu au cours :

1) Collecte d'informations (Reconnaissance) : Recueillir des informations sur l'application en utilisant des Outils comme *requests, BeautifulSoup*, etc, pour récupérer les pages web, analyser et extraire des informations des pages HTML, scanner les différentes pages pour identifier les points d'entrée possibles (formulaires, pages d'authentification, etc.), extraire les commentaires HTML, les scripts JavaScript, et les méta-informations, et bien d'autres choses ;
2) Analyse de vulnérabilités : Identifier les vulnérabilités potentielles dans l' application web en utilisant des outils tel que python-nmap, en développant des scripts par exemple pour effectuer du *fuzzing* sur les entrées de formulaires.
3) Exploitation : Exploiter les vulnérabilités identifiées pour accéder aux informations sensibles en utilisant des outils tels que *Pwntools* pour créer des exploits pour les vulnérabilités identifier (XSS, SQL Injection, etc), *requests* pour automatiser l'exploitation des failles afin d'obtenir un accès non autorisé.
4) Post-exploitation : Maintenir l'accès et extraire des informations sensibles en utilisant des outils tels que *Paramiko* pour maintenir l'accès en téléchargeant un reverse shell ou en configurant une connexion SSH et *Psuti*l pour collecter des informations système sensibles comme les fichiers de configuration ou les bases de données.

5) *Reporting* : Générer un rapport détaillé des découvertes et des exploits en utilisant des outils comme *Jinja2* pour générer des rapports HTML et *Matplotlib* pour visualiser les données

RESUME DES LIVRABLES DU PROJET :

1. Rapport de collecte d'informations : Détails sur les points d'entrée et les informations recueillies.
2. Rapport d'analyse de vulnérabilités : Liste des vulnérabilités trouvées et détails sur chaque vulnérabilité.
3. Preuve de concept d'exploitation : Scripts et résultats des exploits réalisés.
4. Rapport de post-exploitation : Détails sur les actions entreprises après la compromission du système.
5. Rapport final : Document HTML généré avec *Jinja2*, incluant des graphiques et des analyses visuelles des résultats.

N.B : Créer un dépôt github pour déposer vos livrables en plus de votre code source.

Deadline de soumission de votre projet : 21/08/2024 ; FAIRE PAR GROUPE DE 4 PERSONNES

CONCLUSION

Ce projet donne aux étudiants une expérience pratique et complète des tests d'intrusion en utilisant des outils Python. En s'appuyant principalement sur des scripts Python et en limitant l'utilisation de plateformes de formation, les étudiants apprendront les bases de la sécurité des applications web et développeront leurs compétences en programmation et en sécurité informatique.