

PROJET DE TEST D'INTRUSION AVEC PYTHON

Membres du groupe :

Noms et prénoms	Etablissement	Filière et Niveau
Ouattara Amangoua Ismael	UPB	SAS / Master 1
Ouattara Yenipo Shalom	UPB	SAS / Master 1

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 Psutil 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

REPONSES :

Nous avons utilisé dans notre cas OWASP BWA Project en tant que client-serveur nous avons utilisé une machine Windows comme notre client.

Après télécharger OWASP BWA Project et installer sur notre VMware nous allons passer maintenant au travail demander :

Téléchargement de notre environnement : OWASP BWA sur le lien
<https://sourceforge.net/projects/owaspbwa/>

Nous allons passer maintenant à l'installation de notre VM OWASP

Login : root

Mot de passe : owaspbwa

```
owaspbwa login: root
Password:
Last login: Wed Aug 21 17:38:47 EDT 2024 on tty1
You have new mail.

Welcome to the OWASP Broken Web Apps VM

!!! This VM has many serious security issues. We strongly recommend that you run
    it only on the "host only" or "NAT" network in the VM settings !!!

You can access the web apps at http://192.168.8.135/

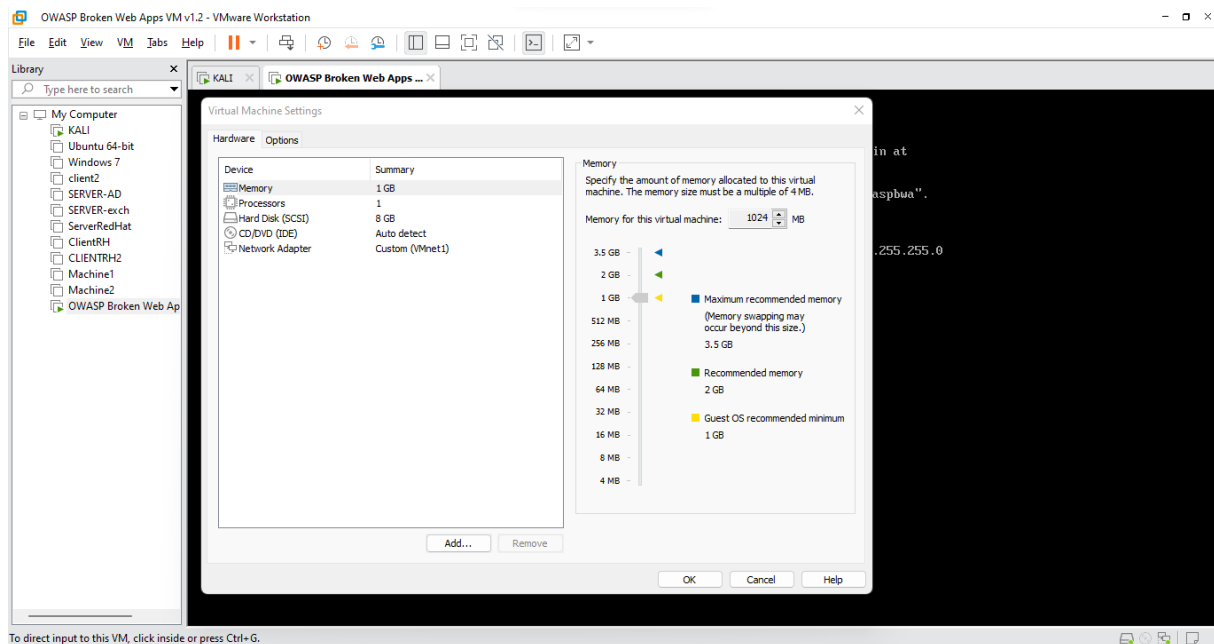
You can administer / configure this machine through the console here, by SSHing
to 192.168.8.135, via Samba at \\192.168.8.135\\, or via phpmyadmin at
http://192.168.8.135/phpmyadmin.

In all these cases, you can use username "root" and password "owaspbwa".

root@owaspbwa:~# _
```

Logiciel : VMware


Configuration du réseau : voir schéma ci-dessous



Ensuite voir l'interface de notre OWASP BWA

Non sécurisé 192.168.8.135

iTube Maps




owaspbwa

Projet OWASP sur les applications Web défectueuses

Version 1.2

machine virtuelle du projet [Broken Web Applications de l' Open Web Application Security Project \(OWASP\)](#) . Elle contient de nombreuses applications Web très vulnérables, ci-dessous. Vous trouverez plus d'informations sur ce projet dans le [guide de l'utilisateur](#) et [la page d'accueil](#) du projet .

détails sur les vulnérabilités connues dans ces applications, consultez https://sourceforge.net/p/owaspbwa/tickets/?limit=999&sort=_severity+asc .



!!! Cette machine virtuelle présente de nombreux problèmes de sécurité graves. Nous vous recommandons vivement de l'exécuter uniquement sur le réseau « hôte uniquement » ou « NAT » dans les paramètres de la machine virtuelle !!!

DEMANDES DE FORMATION	
WebGoat de l'OWASP	OWASP WebGoat.NET
OWASP ESAPI Java SwingSet interactif	OWASP Mutillidae II
OWASP RailsChèvre	Briques OWASP
Berger de sécurité OWASP	Fantôme
Injection de code magique arc-en-ciel	bWAPP

- Avec BWAPP

← → ↻ Non sécurisé 192.168.8.135/bWAPP/login.php

Gmail YouTube Maps



une application web extrêmement bugguée !

[Se connecter](#)
[Nouvel utilisateur](#)
[Informations](#)
[Conférences et formations](#)
[Blog](#)


/ Se connecter /

Entrez vos identifiants (*abeille/insecte*) .

Se connecter:

Mot de passe:

Définir le niveau de sécurité :



bWAPP est uniquement à des fins éducatives / Suivez @MME_JIT sur Twitter et demandez notre aide-mémoire, contenant toutes les solutions ! / Besoin d'une formation ? / © 2014 MME BVBA

- Avec WordPress

