BreakingLab

PLATEFORME D'E-LEARNING INFORMATIQUE ET PENTESTING VIA DES DOCKERS

24/03/2020

PRÉSENTATION

1. Description du projet

Nom	**BreakingLab**
Description	Plateforme d'apprentissage de l'informatique et du pentest avec des dockers
Date	24/04/2020
Domaine	Informatique, Cybersécurité, Pédagogie
Module	Projet Informatique
Gitlab Project	PRO-8445-20-RAN-BreakingLab
Equipe	Adil AHMED Moustapha BARI Rémi BILLY Gaëtan GIANQUINTIERI Patience Noé EBONGUE NJOE

2. Objectif du projet

Notre projet a pour objectif de permettre aux gens d'apprendre l'informatique et la Cybersécurité de manière très simple. Nous souhaitons mettre à la disposition des gens une plateforme d'e-learning sur l'informatique et le pentest.

La grande majorité des personnes de notre société n'ont aucune notion en informatique et encore moins en cybersécurité bien qu'elles utilisent des objets numériques tous les jours dans leur quotidien.

Notre projet a pour but de les sensibiliser à l'informatique et à la Cybersécurité de manière simple afin qu'ils découvrent un nouveau domaine et pour qu'ils adoptent les bons gestes de cybersécurité dans leur quotidien.

Il est important de noter que notre objectif n'est pas de former des gens à devenirs des pirates informatiques mais à les sensibiliser à la cybersécurité et d'initier, pourquoi pas, une vocation dans la sécurité informatique.

3. Fonctionnalités détaillées de notre projet

- Création d'un serveur web et donc d'un site web pour le e-learning.
- Inscription de chaque utilisateur sur notre site.
- Base de données avec diverses informations à définir (utilisateurs, date de connexion, ip, etc.)
- Pages web offrant un apprentissage de langages de programmation, du bon comportement de sécurité informatique à adopter, des failles informatiques existant et dangereuses, etc.
- Possibilité pour l'utilisateur de cliquer sur un bouton « Pratiquer » permettant de pratiquer ce qu'il a appris.
- Lorsque le bouton Pratiquer est cliqué, une instance de docker est créée contenant seulement les types de failles que l'utilisateur souhaite tester.
- Cette instance de docker est isolée du serveur web hôte contenant notre site web.
- L'utilisateur est libre sur ce docker, il peut le « reset » s'il y a un problème.
- Chaque utilisateur différent lance une instance de docker différente, il n'y a pas de conflit entre les dockers.

4. Composantes du projet

Développement Web	Tutoriel Informatique	Programmation des failles
Site web principal sur le serveur	Langage Bash (bases)	Injection SQL, HTML, PHP
Page de login avec base de données	Langage Python	Reverse Shell
Page sommaire et webs	Outils de scans	Session Hijacking
Mise en place des DOCKER	Outils de brute-force	Local File Inclusion
	Exploitation des failles web	Injection HTTP

5. Exigences

Notre projet doit permettre à nos utilisateurs de :

- Apprendre l'informatique ainsi que la cybersécurité
- Pratiquer directement sur notre site ce qu'ils ont appris via des dockers

- Faire du pentest dans un docker spécialement conçu pour l'utilisateur
- Avoir un suivi de ses cours

6. Public ciblé

Nous visons les personnes de tout horizon.

Cependant, nous pensons qu'un tel projet serait un très bon outil pour introduire/former les gens à la cybersécurité. Ainsi nous pourrions mettre cet outil à disposition des clubs de cybersécurité afin de former leurs nouveaux arrivants.

De plus, conscient de la difficulté de l'apprentissage des langages de programmation à l'IMTBS, notre projet pourrait leur permettre d'apprendre facilement les bases d'un langage.

7. Compétences mobilisées

- Langages de programmation : Bash, Java, Python, SQL
- Développement web : HTML, CSS3, PHP
- Base de données : MySQL ou PostgreSQL
- Connaissances sur les Dockers et les serveurs web
- Connaissances en Cybersécurité : injections SQL/PHP/HTML, reverse shell, session hijacking, LFI, brute-force, outils de scan, utilisation de proxy pour du Man In The Middle, web shell…
- Gestion de projet et d'équipe

8. Outils à notre disposition

- Google drive pour la gestion des documents de projet et documents techniques
- Gitlab de TSP pour une gestion intelligente de nos codes
- OpenProject pour la gestion de notre projet
- Messenger, Discord ou Skype pour des réunions visio à distance
- Serveur web