TP 2: Injection SQL

Consignes générales :

- Un compte-rendu par binôme
- Justifiez vos réponses mais soyez concis.

Objectifs

Injection SQL

Pré-requis

VirtualBox, SQL

Introduction

Ce TP a pour objectif de vous permettre de réaliser une attaque de type injection SQL sur un site web existant. L'ensemble des manipulations proposées dans le cadre de ce TP ne doit être réalisé que dans un environnement personnel, virtuel de préférence.

NE LES UTILISEZ PAS POUR ATTAQUER DES SITES WEB NE VOUS APPARTENANT PAS !!

Maintenant que ceci est dit, passons au TP ! Vous avez reçu deux VM, Kali Linux et Metasploitable2. Kali Linux embarque une large palette d'outils d'attaque. Metasploitable2 est une VM volontairement faillible. Importez-les dans VirtualBox et démarrez-les en mode pont.

- Kali Linux : root/toor
- Metasploitable2 : msfadmin/msfadmin

Récupérez les adresses IP de Metasploitable2 et Kali Linux.

Activités

Dans un premier temps, nous allons examiner le profil de Metasploitable2 que nous appellerons M. Kali sera dénommé K. Depuis la ligne de commande de K, exécutez la commande suivante :

nmap -p1-65535 <ip_de_M> -O --osscan-guess

Interprétez le résultat de la commande.

Sur M tourne un serveur web : à partir d'un navigateur sur K, vous pouvez accéder à l'interface du site hébergé. Cette page d'accueil vous présente un lien vers DVWA. Ce sigle signifie Damn Vulnerable Web Application. Il s'agit donc d'un site web truffé de failles, utile pour découvrir les différents types de risques encourus par le serveur. Vous allez donc vous mettre dans la peau d'un attaquant et essayer de soutirer un maximum d'informations au serveur. Commencez par vous connecter.

Une fois connecté, configurez le niveau de sécurité : dans le menu de gauche, cliquez sur l'item *DVWA Security* et choisissez *Low*. Après avoir validé, cliquez sur l'item *SQL Injection*.

Sur cette interface, vous disposez d'un champ dans lequel entrer un numéro d'utilisateur et d'un bouton de validation. Une fois ce bouton pressé, les informations relatives à l'utilisateur sélectionné sont affichées sur la page.

Dans un premier temps, testez manuellement les valeurs supportées pour l'UID. Combien existe-t-il d'utilisateurs dans cette base ?

En vous aidant des explications du cours et de la section « Rappels », répondez aux questions suivantes :

1. Quelle commande permet d'afficher tous les utilisateurs d'un coup?
2. Quelle est la version de la base de données ?
3. Quel est le compte utilisateur exécutant les commandes ?
4. Quel est le nom de la base de données ?
5. Combien de tables comporte cette base ?
6. Listez les tables dont le nom commence par "user".
7. Existe-t-il une tables users? Quelles données pouvez-vous en tirer?

Pour chacune des questions, vous fournirez la commande utilisée, les résultats obtenus et un bref commentaire de ces résultats.

Après toutes ces péripéties, vous avez pu récupérer le nom d'utilisateur et le mot de passe mais, sacrebleu ! Les mots de passe ont été passés au MD-5 !! Expliquez pourquoi.

- Récupérez les usernames et les mots de passe. Collez-les dans un fichier texte au format
- username:password
- Enregistrez sur K ce fichier sous dvwa_pss.txt
- Exécutez la commande suivante:
- john --format=raw-MD5 dvwa_pss.txt
- Interprétez la sortie.

Connectez-vous à présent à M. Naviguez au répertoire /var/www/dvwa/vulnerabilities/sqli/source
et lisez le fichier low.php
Comment modifieriez-vous ce fichier pour empêcher l'exécution de l'attaque précédente?

Rappels

- Pour concaténer les résultats de deux requêtes S1 et S2 : S1 union S2. Possible si les deux requêtes retournent le même nombre de colonnes
- version(), user()