

Introduction :

CTF (Capture The Flag) sont des challenges liés au domaine de la sécurité informatique. La création de ces challenges est l'un des sujets proposés, comme projet en sécurité de 4A, par les professeurs afin de mettre à l'épreuve nos connaissances et compétences dans des domaines liés à la sécurité.

CTF1 : Easy Peasy

Dans la catégorie des challenges faciles, on a choisi un challenge avec une seule machine Debian et contient trois flags. Le but principal de ce challenge est de découvrir un site web hébergé dans la machine Debian et qui contient des flags dans le serveur. Ce challenge permet à l'hacker d'utiliser des outils de sécurité basique et traditionnelle comme Hydra pour une brute force sur une page de login, reconnaissance en utilisant nmap ainsi que l'utilisation des commandes de linux dans une ligne de commande en ligne

Lors de ce challenge, vous allez mettre en pratique plusieurs méthodes et outils afin de résoudre le challenge. Parmi ces méthodes, on a ; reconnaissance qui permet à l'hacker d'interagir avec le système cible pour collecter des informations sur ses vulnérabilités, d'énumération pour lister les différents répertoires et fichiers au niveau du port http en créant une connexion active avec le système cible.

Brute Forcing login qui va être utilisée pour trouver un mot de passe ou une clé. Il s'agit de tester, une à une, toutes les combinaisons possibles. Ce type d'attaque fait en utilisant plusieurs outils comme Hydra.

La création du challenge :

La création de ce challenge s'est basée sur un ensemble des étapes cohérents :

1. Choix d'une machine Debian avec une adresse privé et une autre flottante qui est disponible sur l'open stack fournis par les professeurs.
2. Hébergement dans apache 2 d'un serveur et site web développés en Node JS et MongoDB en utilisant un clonage d'un site web qui contient une ligne de commande accessible par un login de développeur (la brute force le login par hacker pour avoir l'accès.).
3. La récupération du premier flag par une Reconnaissance et une énumération (@ip/robots.txt). Ainsi que la création d'un compte de développeur (Admin) qui contient un fichier.txt contenant le deuxième flag.
3. L'insertion du troisième flag dans une photo en utilisant la stéganographie.

Explication de install1.sh :

On a généré un mot de passe lors de l'exécution de ce fichier. Ensuite, on a fait l'installation de tous les services nécessaires pour le challenge et les mettre au démarrage de la machine (lignes 8 - 17). On a utilisé le cmd disponible sur le git hub suivant : https://github.com/Oumaimaelh/command_line.git.

Après, on a utilisé wget afin de télécharger le contenu du fichier du server et configurer le fichier de configuration de notre site qui va contenir notre cmd (lignes 22-36). Ensuite, on a désactivé le contenu du site par défaut et on a activé notre site (lignes 37-39).

Les flags

Flag 1 en MD5 (Yes! You get it) = 3c7abd78f0f92410afc66fc00c0adcc4

Flag 2 en MD5 (That is great!) = 61a0a824765dc715d0af0f65dddbdf915

Flag 3 en MD5 (You did it) = a98b5ce98ad49e5dba91a17652f49f4f