Projet Sécurité

Les scénarios:

1. **<u>Challenge facile</u>: Web Directory Enumeration, Web Command Line and Steganography.**

   1.1. Création du challenge:

   Une machine avec server web qui contient les vulnérabilités:

   - **Hoster server web**
   - **Création d'un fichier txt contenant le premier flag.**
   - **Création d'une page login pour authentifier utilisateur pour test.php**
   - **Création d'une page test.php contenant une inputbox qui reçoit une commande et renvoie le résultat sous forme de chaînes**
   - **Insertion du 3eme flag dans une image.**

   1.2. Les étapes de résolution:

   1.2.1. Le premier flag: Reconnaissance

   Découvrir le serveur Web, effectuer Web Directory numeration, trouver le premier flag et le page test.php

   1.2.2. Le deuxieme flag: Brute Forcing login

   Brute Force le login et mot de pass dans le page login pour gagner d'acces de test.php été conçu par les développeurs pour des tests uniquement.

   Utiliser la ligne de commandes pour trouver le deuxième flag sous forme de fichier texte et le lire.

   1.2.3. Le troisieme flag:

   Utiliser la ligne de commande pour recuperer un fichier png qui cache le troisieme flag avec le chemin /home/user1.

2. **<u>Challenge moyen/difficile</u> :**
   a. **Les étapes de création du challenge**
      - **Création de deux machines 1 et 2:**
        Machine 1 est héberge un site de web avec base de donnees et un site blog wordpress que le developeur a oublié à le déhéberger. Le site de web est vunerable au SQL Injection et le site de blog partage le mot de pass de admin login avec le site, qui peut être piraté par SQLi. Dans la machine 1, nous cachons les flags de 1 à 3, et aussi l' information nécessaire pour acceder à la machine 2.

        Machine 2 IP peut être obtenu dans le fichier known_hosts de Machine 1 avec mot de pass dechiffré. Dans cette machine, il existe plusieurs utilisateurs, respectivement existe le flag.

   b. **Les étapes de résolution:**
      - **Reconnaissance:**
        Trouver flag1.txt et small-word-list.txt.
        Gobuster avec la nouvelle word-list pour accéder au site Wordpress.
      - **SQL Injection:**
        Pour trouver le login et mdp(et un autre utilisateur : flag 2 comme login et Flag comme mdp)
      - **Wordpress:**
        Trouver flag 3 dans la page admin du site Wordpress.
        Modifier le thème de la page 404.php pour lancer un reverse shell et acceder a la première machine.

      **** Dans Machine 1 :**
      - **Trouver un fichier user1file.txt qui n'est accessible que par user1 et qui contient flag 4 et le mdp de la deuxième machine(user1).**
      - **Trouver un autre fichier backup-mdp.txt qui contient le mdp de user1 encrypté(md5).**

- **Chercher dans known_hosts pour passer à la deuxième machine via SSH.**

  **** Dans Machine 2 :**

- **Flag 5: User2**

  Lire le contenu de crontab, un cron qui fait une sauvegarde de /home/user2(qui contient flag5.txt) vers une autre directory avec cp
  Modifier le PATH pour cp vers notre script cp(qui est une cat) pour lire le contenu du flag 5.

- **Flag 6: Root**
  Chercher un fichier SUID pour droits d'accès.
  Le exploiter pour accéder à un terminal en tant que root et chercher le dernier flag.