Formation
sécurité réseau et Internet

Réalisation pratique d'un test d'intrusion

Comprendre l'attaque pour mieux se défendre

Enoncés des exercices

Présentation du TP

Le PDG de l'entreprise « entreprise.net » vous a mandaté pour réaliser un test d'intrusion sur son réseau. Il souhaite obtenir un rapport exhaustif comportant les actions que vous avez réalisées, accompagnées des informations que vous avez récupérées (configuration, mots de passe, preuves de votre passage…)
Vous travaillerez à partir d'un filiale de « entreprise.net » et serez connectés sur le WAN de la société.

L'objectif à atteindre est simple : compromettre le réseau de entreprise.net.

Contrainte : ne rien casser ! L'entreprise doit pouvoir continuer à travailler normalement.

Conseils :

- Conserver une vision globale de votre avancée ;
- Organisez vos données dès le début ;
- Définissez des objectifs à atteindre.

2. Attaque Web

2.1. Inclusion de fichier / directory traversal

Objectifs :

- Comprendre le mécanisme de d'inclusion de fichier local ou distant ;
- Trouvez une méthode pour exécuter un code malveillant (PHP) sur le serveur.

Préparation de l'exercice :

Vous allez configurer votre serveur web local et tester son bon fonctionnement. Démarrez le service apache2 de votre machine virtuelle `Kali` et vérifiez son bon fonctionnement en vous connectant dessus.

```
sudo service apache2 start
```

Créez un fichier `info.php` dans le répertoire `/var/www/html` :

```
<?php
phpinfo();
?>
```

Lancez votre navigateur et connectez vous à `http://127.0.0.1/info.php`

Enoncé :

Question 17 : Exploitez la LFI de la page « test_lrfi.php »pour afficher le contenu du fichier passwd du serveur. Quel est le nom login qui possède l'iid 1000 ?

Question 18 : Exploitez la RFI de cette page pour charger le code PHP que vous hébergez sur votre propre machine. Que constatez-vous ?

Question 19 : Faites la correction nécessaire pour récupérer le valeur du champ « Apache API Version » du serveur web. Quelle est cette valeur ?

2.2. Injection SQL

Objectifs :

- Exécutez des commandes SQL non légitimes sur la base de données
- Comprendre le principe de fonctionnement d'une architecture web classique

Enoncé :

Grâce à votre navigateur et ses plugins, exploitez les injections SQL les fichiers « identification.php » et identification_get.php ».

Question 20 : Quelles sont les URL et les paramètres que vous avez utilisés pour exploiter ces deux injections SQL ?

Passez à la vitesse supérieure en réalisant les challenges 1, 2 et 3.

Question 21 : Quelles sont les URL et les paramètres que vous avez utilisés pour exploiter ces deux injections SQL ?

A partir de l'injection que vous aurez trouvée au challenge3, uploadez un webshell sur le serveur. Nommez votre fichier de la forme « `_trigramme_.php` » (webshell fourni par le formateur). Vous pourrez utiliser l'application sqlmap pour automatiser le traitement. En cas de difficulté, l'option `–os-shell` pourrait s'avérer être utile.

Outils :

- extension `hackbar` pour `firefox` ou l'utilitaire `curl`.
- `sqlmap` uniquement pour l'upload du webshell
- webshell `B374k`

2.3. Investigations

Objectif :

Réaliser un « environnement » du serveur pour caractériser la machine (rôle, niveau de sécurité…) et récupérer les fichiers qui pourraient être intéressants pour la suite de votre progression.

Enoncé :

Grâce à votre webshell, vous êtes en mesure de passer des commandes et d'explorer simplement le serveur.

Question 22 : Quel est le nom du compte utilisé par l'administrateur du serveur ? A partir de quelle adresse IP se connecte-t-il pour l'administrer ?

Question 23 : Quel fichier très intéressant, qui n'est pas du tout à sa place, avez-vous trouvé lors de votre investigation ? Sur quelle machine comptez-vous l'utiliser ?

Outils :

- Commandes natives linux
- Webshell