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.

1. Rebonds

1.1. Utilisation d'un serveur SSH

Objectif :

Comprendre les fonctionnalités d'un serveur SSH, de son serveur Socks et des forwards de port.

Enoncé :

Copiez le fichier `id_rsa` que vous avez récupéré sur le serveur web et utilisez-le sur la machine `zeus.entreprise.net`.

Question 27 : Quelle information devez-vous avoir (et que vous avez trouvée!) pour utiliser cette clé ?

Question 28 : Quelles sont les permissions qui doivent être positionnées obligatoirement sur cette clé ?

Connectez-vous au serveur SSH que vous avez trouvé dans le domaine entreprise.net et rebondissez sur ce serveur pour continuer votre progression.

Question 29 : Quelle ligne de commande avez-vous utilisée pour vous connecter au serveur SSH ?

Question 30 : Quelle est son adresse IP ? Quel type de NAT est mis en place ?

Question 31 : Après voir réalisé l'environnement de cette machine, donnez l'adresse IP à partir de laquelle se connecte l'administrateur du serveur SSH ?

Question 32 : disposez-vous des droits d'administration sur cette machine ? Rencontrez-vous des limitations ? Pourquoi ?

Question Bonus : la gestion du cron semble être « perfectible ». Quelle action pouvez-vous réaliser pour récupérer un shell « `root` » ?

1.2. Utilisation du serveur Socks

Préparation :

Modifiez le fichier `/etc/proxychains.conf` pour lire à la dernière ligne :

```
socks4 127.0.0.1 1080
```

Enoncé :

Relancez votre session SSH et en démarrant cette fois-ci un serveur Socks sur le port 1080 (option `-D 1080` de SSH). Le serveur Socks vous permet maintenant d'encapsuler tous les flux réseaux TCP (et uniquement TCP) et de faire en sorte qu'ils soient émis par le serveur SSH distant.
Utilisez les modules auxiliaires de `Metasploit` à travers le serveur Socks pour continuer la découverte des nouveaux réseaux.
Commande :

```
proxychains4 msfconsole
```

2. Recherche de vulnérabilités

Objectif :

Sur la base d'une version de système d'exploitation ou d'une application d'une cible, identifier les vulnérabilités potentielles au travers de requêtes Google.

Enoncé :

A partir des informations que vous avez collectées lors de la réalisation de l'environnement réseau précédent, recherchez les potentielles vulnérabilités que vous pourriez exploiter pour continuer votre progression.
Question 33 : quels sont les vulnérabilités que vous avez identifiées et le nom des « exploits » que vous pensez utiliser pour continuer votre progression ?
Question 34 : essayez de créer un compte ou bien d'obtenir des accès sur des machines distantes sur le réseau.

Outils :

http://fr.0day.today
http://www.cvedetails.com/vulnerability-search.php

3. Metasploit : Exploitation de vulnérabilités

Objectif :

- Découvrir comment exploiter une vulnérabilité à partir de `Metasploit`

Enoncé :

Vous allez exploiter une vulnérabilité pour ajouter un compte sur une machine Windows distante.

Commandes :

- Exploit à privilégier : « `ms08_067_netapi` »
- Payload à utiliser : « `windows/adduser` »

Question 35 : Ajoutez un compte avec votre trigramme sur cette machine LA machine qui est vulnérable à cet exploit et essayez d'augmenter les privilèges de ce compte. Expliquez votre démarche.

Question 36 : Faites l'environnement de la machine à la recherche d'éventuels indices.

Question 37 : Ajoutez un compte sur la machine qui vous est attribuée (une fois que vous êtes arrivés ici !)

Question Bonus pour les pirates : expliquez la procédure pour accéder à cette machine en Terminal Server. C'est un bonus, c'est-à-dire que tu ce qu'il y a avant cette question doit être réalisé avant !