INSA
CENTRE VAL DE LOIRE

Projet CTF : challenge Réseau

Les 4 Coquins

1 Informations sur les indices

Les indices pour ce challenges ont étais fait sous forme de mini challenges car nous avons estimé que, puisque notre challenge étais de niveau difficile, les challenges ne devait pas trop simplifié la difficulté, donc pour avoir de l'aide les utilisateurs doivent réalisé un mini challenge. Nous avons essayer de faire des mini challenges qui soit proportionner au indice qu'il révèle mise a par le dernière indice qui a une complexité qui permet de révéler un indices qui ne donne pas vraiment de solution mais simplement une impressions sur ce qu'il faut faire. Nous avons aussi décider de mettre les indices dans ce fichier au cas ou les indices soit trop compliqué a obtenir.

Si les indices qui doivent être donner sont les mini challenges, ils sont classifié par étapes dans le dossier /doc/hints/ dans le repos GitHub. Il suffit de transférer le fichier qui est dans le dossier de la bonne étapes avec le numéro de l'indice souhaité (pour l'indices 2 de la troisième étapes, il se trouve sur le GitHub : /doc/hints/step_3/hint_02_step_03.txt).

2 Indices

Étape 1	
hint 1	Sur les trois pages de ce site, il n'y en un une seule qui permet l'exploiter de ce site
hint 2	La page a exploiter nous permet de transférer un WebShell
hint 3	Il faut camoufler le WebShell en fichier PNG : le chat des fichiers est supérieur au camouflageWebShell.php

hint 4	Nous devons trouver le dossier qui contient les fichiers envoyés. Il faut s'inspirer de l'URL qui permet d'upload le fichier pour trouver son nom
hint 5	Nous devons trouver le dossier qui contient le flag. Ce dossier contient aussi le site
Étape 2	
hint 1	Il vous faut une connexion sur un service et n'oublié pas les informations que vous avez pue trouvé au même endroit que le flag precedent
Étape 3	
hint 1	Pour faire une élévation de privilège, vous devez trouvé un programme qui possède le SUID
hint 2	https ://gtfobins.github.io/ va vous permettre de trouver des exploitation des programmes qui contiennent de SUID
hint 3	Notre grand objectif serrait de créer un nouvelle utilisateur avec une des commande qui possède le SUID (bien évidement, cette étapes dois êtres réalisé en faisant attention car nous pouvons facilement changeais des configuration système et de possiblement rendre indisponible la machine)
Étape 4	
hint 1	Avec le doigth, il faut savoir a quoi il sert et aussi comment vous pouvez l'exploiter.
hint 2	Avec les information trouver par le doight, il nous faut surment utiliser hydra comme créature.
Étape 5	
hint 1	Cette étapes peut etre facile ... Nope, je croit que pour cette étape je vais étre BoF.
Étape 6	
hint 1	Se débarrasser de la baleine bleue
Étape 7	
hint 1	Comprendre comment le site fonction peut être important pour supprimer ces traces
Étape 8	
hint 1	Un service apache doit sûrement laisser des logs
hint 2	Si il n'y a plus de logs, elles sont peut être sauvegarder automatiquement dans un autres emplacement il va falloir crontacter l'internet
Étape 9	(Bonus)
hint 1	C'est un bonus donc le seul indice que j'ai c'est bon courage et bien réfléchir a toute les étapes faite pour bien supprimer les traces qui aurait pue être laisser