Je s'appelle G root

Bienvenue sur la page pour vous expliquer comment va se dérouler le jeu de piste sur l'infrastructure du GInfo.

Vous allez ici utiliser l'ensemble de vos compétences sur linux.

Première pierre de l'infinité : LE SSH

CLIENT KSI FORTUNE - Bonjour, monsieur le hackeur, j'aimerais que vous preniez le contrôle de la cible dénommée ginfo.xyz . Si vous avez besoin d'aide vous allez voir le respo réseau ou suivre la formation réseau et linux.

FORMATEUR BRUN TENEBREUX ET SEXY (JERRY DES TOTALLY SPIES) - Ah ! je vois pour cela vous aurez besoin de savoir vous connecter à un serveur à distance grâce au protocol SSH dans un terminal. Dites-moi vous savez ouvrir un terminal sur votre ordinateur ?

FORMATEUR BRUN TENEBREUX ET SEXY (JERRY DES TOTALLY SPIES) - OK, maintenant que vous avez ouvert un terminal, je vais essayer de trouver des infos sur la cible.

[5 minutes passent]

STAGIAIRE CHIANT DES SERVICES SECRETS (entre dans la pièce) - C'est bon monsieur, j'ai des infos sur la cible, mais c'est une mauvaise nouvelle, la cible s'appelle Sirroco c'est un serveur du service ultra secret : le GInfo je pense que ça être compliqué pour entrer dans le serveur pq ils ont un respo réseau incroyable (vory) il va falloir cracker un mot de passe ultra complexe, je vais chercher le super calculateur quantique !

FORMATEUR BRUN TENEBREUX ET SEXY (JERRY DES TOTALLY SPIES) - Essayer de vous connecter en ssh au serveur ginfo.xyz avec l'utilisateur ginfo, il sont peut-être totalement con ...

La commande type est :

```
ssh user@adresse_IP_serveur_ou_nom_serveur_si_DNS
```

[Allez voir la section solution si vous n'y arrivez pas]

La solution

La première ligne de commande devrait ressembler à :

```
ssh ginfo@ginfo.xyz
```

Seconde pierre de l'infinité : NAVIGUER DANS UN SERVEUR

FORMATEUR AVEC DES LUNETTES PQ IL FAUT ETRE INTELLIGENT : OK maintenant que nous avons infiltré l'ordinateur cible, il va falloir faire de l'escalade de privilège. En effet actuellement tu est connecté en tant que user = ginfo or cette utilisateur n'a pas tout les droits. Donc nous allons devoir changer d'utilisateur avec la commande :

```
su nom_utilisteur
```

Maintenant votre mission est de fouiller dans les fichiers pour trouver si des données très très bien cachées contiennent les identifiant nécessaires à escalader vers le niveau 2 de privilège. (Regardez dans la boîte à outils pour trouver des commandes utiles)

Boîte à outil

Vous pourrez avoir besoin de ces commandes :

```
ls
cd
touch
chmod
grep
```

Pour avoir des infos sur ce que font ces commandes et quels arguments peuvent être utilisés, faites :

```
 man <commande>
```

Indice

Tu peux regarder ce que fait les commandes suivantes, ça t'aidera :

```
ls -la
grep -n
```

Troisième pierre de l'infinité : LES TOKENS JWT

FORMATEUR SUPER COOL : Bien joué ! Nous nous sommes infiltré dans le niveau 2 de cette forteresse ! Nous ne sommes plus qu'à un échelon de devenir l'administrateur système de ce serveur ! Un dernier effort ! Comme nous avons gagné un niveau de privilège nous avons donc maintenant la possibilité de changer les droits d'un fichier cela pourrait t'être utile. Tu peux regarder dans notre base de données comment on peut utiliser cela, tu peux la consulter en allant à cette adresse : www.google.fr

CHEF DES SERVICES SECRETS (passe la tête par la porte) : N'oublie d'effacer tes traces en supprimant toutes traces de ton passage, cela nous éviterait un conflit avec le GInfo et nous ne

pouvons pas nous permettre de nous brouillés avec NICOLAS BERT !

STAGIAIRE CHIANT (entre encore dans la salle) : Le service cybersécurité de l'agence (allez voir le club cyber du GInfo) as réussi à trouver une faille et en exploitant nous avons découvert qu'une API était héberger sur ce serveur on pourrait bruteforce la route ou bien on pourrait essayer de trouver un indice sur la session actuelle ! (FORMATEUR NE DOIT PAS OUBLIER DE METTRE EN PLACE L'API)

Solution

Tu dois chercher frère c'est pas à moi de tout faire Sinon il y a un indice dans le titre de la partie !
Tu peux utiliser un navigateur internet “Formateur doit se connecter en root et lancer :

```
node vory-API/index.js"
```

Cherche sur internet pour décoder le token

From:
https://wiki.centrale-med.fr/ginfo/ - **Wiki GInfo**

Permanent link:
https://wiki.centrale-med.fr/ginfo/formations:jeu_de_piste_reseau

Last update: **25/10/2021 13:58**