

SYSTEM MOYEN

- 1/ Accéder au site.
- 2/ Inspectez la page et récupérez le message caché.
- 3/ Déchiffrez le message en utilisant AES et la clé qui se trouve dans le message, obtenant ainsi le mot de passe : **Kikawa_9123**.
- 4/ Connectez-vous au serveur **FTP** en utilisant les identifiants : **john + Kikawa_9123**.
- 5/ Téléchargez le fichier **my_bio.txt** et construisez un dictionnaire à partir de son contenu.
- 6/ Utilisez l'outil Hydra pour effectuer une attaque par force brute sur **SSH** avec le mot de passe : **JoDoGGyFiF@1994**. Voici la commande : **hydra -l john -P passwordlist -t 6 ssh://localhost**.
- 7/ Récupérez le premier flag.
- 8/ Exécutez **sudo -l** pour voir les commandes que vous pouvez exécuter en tant que root.
- 9/ Effectuez une élévation de privilèges à l'aide de sudo et tar. La commande à saisir est : **sudo tar -cf /dev/null /dev/null --checkpoint=1 --checkpointaction=exec=/bin/sh**.
- 10/ Récupérez le dernier flag.