Training: Warchall - The beginning

Création de compte ssh

Pour pouvoir créer notre compte ssh nous devons y entrer le mot de passe qu'on a préalablement choisi. Il nous dit alors notre hostname (@warchall.net) et le port (-p 19198) sur lequel nous devons nous connecter.

Level 0

Comme le fichier WELCOME. md le dit, nous trouverons les solutions dans /home/level ou /home/user/yournick/level.Pour entrer dans un dossier, on utilise la commande "cd" et pour y afficher son contenu "ls -al". La solution 0 se trouve donc dans /home/level/00_welcome puis on exécute la commande 'cat README. md'.

Level 1

/home/level/01_choice_tree/blue/hats/grey/solution/patience cat SOLUTION.txt

Level 2

/home/level/02/.porb cat .solution

Level 3

/home/level/03 cat .bash_history

Level 4

/home/user/yournick/level/04_kwisatz Afin de pouvoir lire le fichier README2. md, il nous faut changer ses droits d'accès. On execute alors 'chmod a+rx README2. md'. A présent, tout le monde peut y accéder et suffit d'éxécuter la commande 'cat README2. md'.

Level 5

/home/level/05_privacy cat README. md

Py-Tong

ETAPE 1:
Créer deux fichiers dans /home/user/yournick. Par exemple "code" et "03".Le fichier "code" va alors contenir un script,en language python, qui ajoute indéfiniment un mot ou groupe de mot au fichier "03".

ETAPE 2:
Pour que le fichier "code" soit éxécutable, il faut lui en donner les droits et donc 'chmod +x code'. Maintenant, vous pouvez excécuter le fichier en faisant './code'.

ETAPE 3:
Ouvrir un autre terminal car l'autre n'est plus utilisable (mais ne le fermer quand meme pas). Allez dans /home/level/12_pytong/

ETAPE 4:

Exécuter le fichier "pytong" en utilisant le chemin du fichier qu'on a modifié comme argument. Exemple: ./pytong /home/user/yournick/03 Cela devra alors retourner le mot de passe qui validra notre challenge.

Warchall: Live LFI

Contexte: Notre page page web a des problèmes de sécurité appelés Local File Inclusion(LFI)dans le cadre de php.

Url initial: https://lfi.warchall.net/index.php?lang= Url final: https://lfi.warchall.net/index.php?lang=php://filter/convert.base64-encode/resource=solution.php

Comment est-on arrivé à cette url ?

- 'php://': est une enveloppe que permet d'appliquer des fonctionnalités tel que 'filter'.Donc ici 'filter' nous permet de manipuler et traiter les données de manière plus flexible.
- Maintenant, on veut préciser comment on le filtre.'convert.base64-encode': cela encode en base64 le contenu du fichier.
- Enfin 'resource=solution.php' correrspond au fichier que l'on veut lire.

Et là en tombe sur une suite de lettre, comme elle est en base64, il faut la décoder dans https://www.base64encode.org/ . Il suffit d'y coller notre solution et appyuer sur décoder.

Warchall: Live RFI

Notre problème de sécurité est cette fois un Remote File Inclusion(RFI), mais comme précedemment le principe est le meme. Url initial: https://rfi.warchall.net/index.php?lang= Url final: https://rfi.warchall.net/index.php?lang=php://filter/convert.base64-encode/resource=solution.php Comme tout à l'heure, tout est pareil et on soumet simplement la suite de lettre à https://www.base64encode.org/ pour le décoder.