INSA
CENTRE VAL DE LOIRE

Projet CTF : challenge Réseau

Les 4 Coquins

1 Scénario

Une entreprise pharmaceutique à eux une fuite de documents qui était secrète. Cette entreprise possède des systèmes de sécurité qui aurait pu permettre de garder une trace du passage de l'attaquant, mais malgré ces protections, aucune trace n'a étais gardé. C'est là que vous intervenais, cette entreprise vous a chargé de reproduire cette attaque pour savoir si cette fuite de documents a pue être menée à distance ou alors si c'est un employer qui aurait fait cela. Vous deviez donc essayer de récupérer un document qui est présent sur une machine de la pharmacie tous en suppriment vos traces de passages pour pouvoir apaiser les tensions qui sont maintenant présente dans l'équipe. De plus si vous parvenais à réaliser l'attaque, la pharmacie vous proposeras un second contrat pour renforcer leurs systèmes de protection et de détection de leur infrastructure.

2 Objectif

Pour mener a bien ce challenge, vous aller disposé d'une adresse IP. Avec celle-ci vous devrez trouver un moyen de prendre possession de la machine, puis prendre possession d'une seconde machine. Dans ce scénario, vous aller devoir trouver neuf flags. Chaque flag trouver délimite une étapes, mais une étapes peut êtres constituer de plusieurs manipulation. Le challenge est fait pour laisser les utilisateurs assez libre sur les méthodes de procédé même si les directions sons orientées. Le plus important, il est fait mention qu'il fallait supprimer ces traces sur la premier machine. Il y a un certain nombre de vérification faite, ces vérifications permettent de vérifier comme un administrateur pourrais le faire pour contrôler les activité sur la machine a vous de les trouver pour vous rendre invisible. Comme c'est vous qui déterminerais le moment d'on vous estimez avoir réussie les étapes, nous avons implémenté un commande sur la machine qui va faire les vérifications de manière automatisé. Bien sûr vous pourriez récupérer l'executable pour l'analyser, et potentiellement trouver le flag, mais des système de protection on étais ajouté pour rendre cette manipulation plus compliqué bien sûr nous ne pouvons pas la rendre impossible, mais le plus important serait de

respecter le fait de ne pas tenter ou alors de le faire après avoir fini le challenge pour s'exercer. Pour utiliser la commande vous devrait faire :

```
root@groupe1-machine1 : / # traceCheck
/!\WARNING :
        Pour realiser cette etapes du challenge, vous avez la possibilte de recuperer ce fichier
        binaire pour faire du reverse ingenering mais cela n'est pas l'objectif.
        Des points de securite on etais ajoute pour ralentir la possibilite d'effectuer le
        reverse. Le plus judicieux serais d'essayer de realise cette etapes normalement.

        De plus pour faire cette partie du challenge, il vous faut penser
        a l'integralite des etapes qui vous on conduit ici pour pouvoir
        effacer ces trace methodiquement.

Felicitation, vous avez reussie a effacer les traces necessaire :
< CENSURED >
root@groupe1-machine1 : / #
```

Cette affichage correspond a ce que vous devriez obtenir si vous parvenez a bien supprimer les traces que ce programme vérifie.