INSA
CENTRE VAL DE LOIRE

Projet CTF : challenge Réseau

Les 4 Coquins

Table des matières

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 Idée primaire

Nous avons l'adresse IP d'une machine qui est un serveur de l'entreprise. Sur ce serveur, nous pouvons identifier un service Wev. Nous devons exploiter une fail sur ce site pour pouvoir récupérer un accès sur la machine. Une fois introduit dans cette machine, et trouvé le moyen de passé root, nous devrons trouver un moyen pour envoyer Nmap dans cette machine pour pouvoir scanner le réseau et pouvoir identifier la seconde machine. Cette seconde machine posséderas un service FTP non-sécurisé car l'entreprise pensais que ce services ne pouvais pas créer une vulnérabilité, car elle n'avais pas d'access a internet. Une fois connecté sur le service, nous devrons trouver un moyen de faire une backdoor. Comme avec NetCat. Mais comme cette machine n'a pas d'access a internet, nous devons avoir l'obligation de transmettre NetCat a partir de la machine qui contient le service Web. Une fois l'access sur cette seconde machine, nous devrions faire une élévation de privilaige pour pouvoir récupérer les fichiers secret contenue dans le /root/. Une fois les documents récuperer, nous devrons pour optenir les derniers flags, supprimer toute trace de l'intrution et lancer une commande qui va vérifier si la machine a étais infiltrée. En cas de bonne suppresion des trace, la commande va nous tranmettre un flag. La suppression des trace devrat s'effectuer sur les deux machines. Nous aurrons donc deux flags avec la suppressions des traces de sont passage.