INSA
CENTRE VAL DE LOIRE

Projet CTF : challenge Réseau

Les 4 Coquins

Table des matières

1 Scénario

Pour ce challenge, nous avons une entreprise qui veut que nous fassions un test d'intrusion sur leur système pour savoir s'il est suffisamment sécurisé. L'entreprise a mis au point des systèmes de détection d'intrusion qui se déclenche régulièrement. Si nous parvenons à récupérer des documents sensibles de l'entreprise sans se faire repérer, elle va nous proposer un post pour faire la maintenance et la sécurisation de leur système informatique.

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.