Scénarios CTF 1

Cyprien Leschi, Hugo Sarazin, Jérémy Richard, Haroune Samouche, Steven Jaman

9 décembre 2021

1 CTF 1

Initialement l'attaquant se trouve sur un site de prise de rendez-vous pour se faire vacciner. Sa première mission est d'exécuter un **bind shell** à l'aide d'une **injection SQL** sur un serveur *postgreSQL*. A ce stade l'attaquant est dans le système en tant que *postgres*. Le flag user se trouvera dans */var/lib/postgresql/11/main/user.txt*.

Pour obtenir le flag root, l'objectif est de **modifier l'uid de l'utilisateur avec lequel l'attaquant est connecté à 0** dans */etc/passwd* ou **modifier le mot de passe root** dans */etc/shadow*. Seule la commande *tee* sera autorisée sans mot de passe dans */etc/sudoers*. Le flag root se trouvera dans */root/root.txt*.