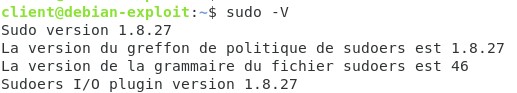
Wiederkehr

Julien

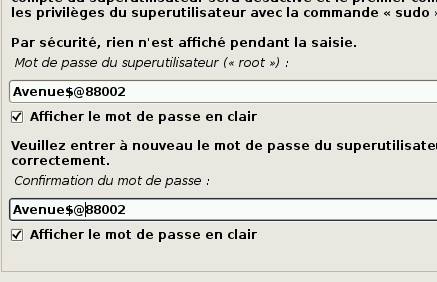
Exploit sudo Bypass Debian 10 Explication



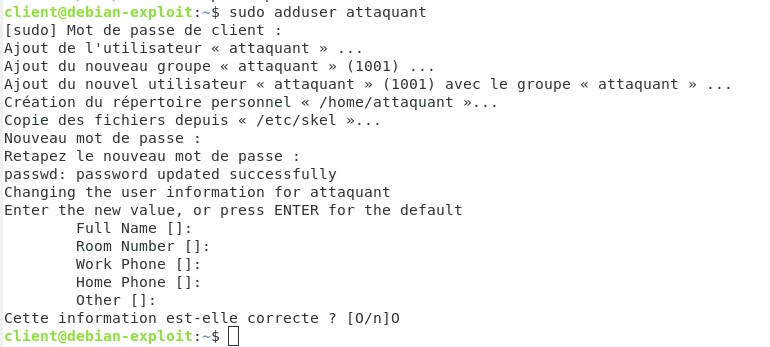
J’ai utilisé une debian 10 qui dispose d’une version de sudo qui à des failles de sécurité.



Le but de cette faille c’est d’obtenir les privilèges root pour pouvoir lire les fichiers qui ne sont pas accessible depuis un utilisateur normal.



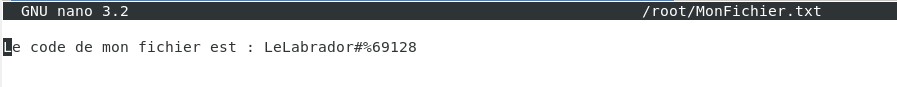
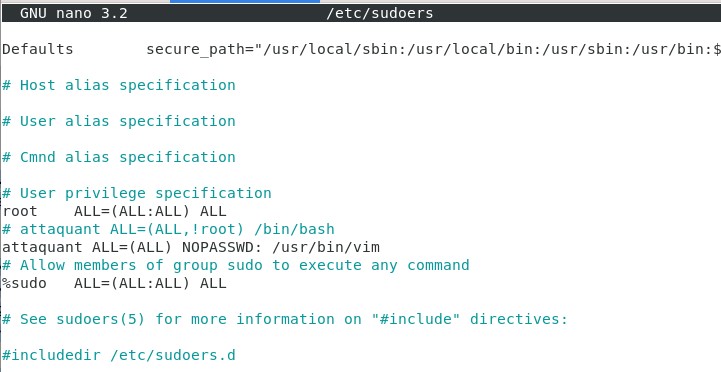
En installant la debian, j’ai mis comme mot de passe celui-ci mais il n’est pas utile pour l’épreuve.



Pour ceux j’ai créé un nouvelle utilisateur « attaquant » qui n’a pas les droits admins sur la machine.



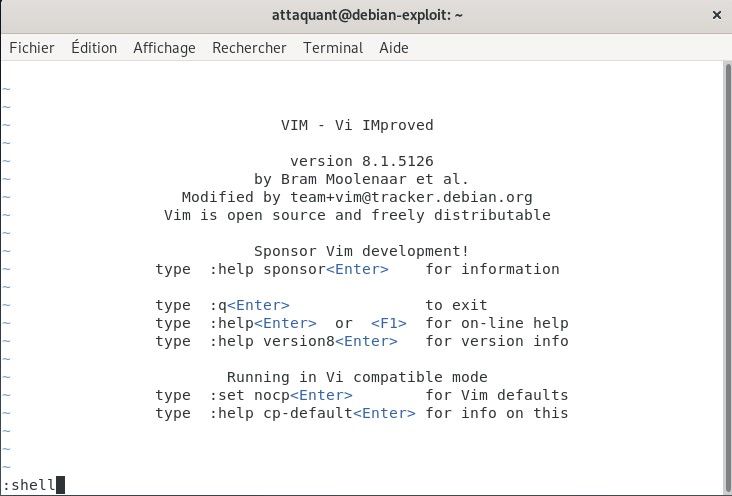
J’ai créé un fichier dans le dossier root qui sera le flag à trouver.

Le flag est ceci uniquement accessible en étant root.

Ensuite dans ce fichier j’autorise l’utilisateur à avoir les droits sur le fichier VIM qui sera par la suite notre faille.

Et c’est terminer pour la mise en place de l’épreuve. On va se connecter en tant qu’attaquant dont le mot de passe est « attaquant ».



L’attaque se passe comme ça, on tape la commande « sudo vi » dans l’invite de commmande.

On arrive sur cette page de configuration de ViM et il suffira de taper « :shell » et cela nous fera retourné automatiquement dans l’invite de commande cette fois en tant que root.



Et Hop, challenge terminer, on à accès un fichier qui contient le flag.

Ce qui était prévu de base :

Lien du site : <https://www.exploit-db.com/exploits/47502>

C’était prévu que la commande « sudo -u#-1 /bin/bash » ou un code python qu’on pouvait exécuter par l’utilisateur « attaquant » nous permettait de passer en root grâce à la faille de sécurité de la version de sudo.

Mais pour une raison que je pense vient d’un patch de sécurité de linux sur la debian 10 ne fonctionne plus.