Mise en place MFA sur ssh

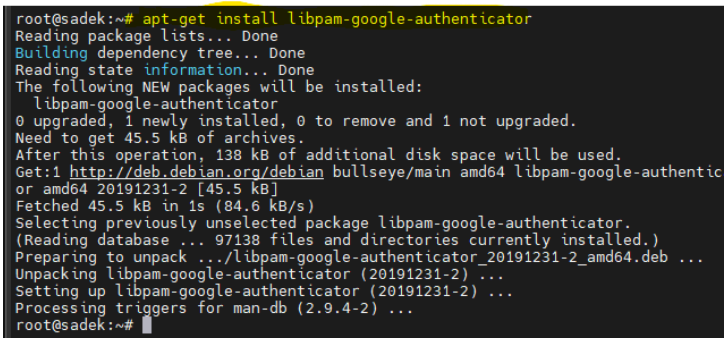
Introduction

Dans cette documentation on va mettre en place le MFA pour l'accès ssh sur un serveur Linux, sa permettra de garantir un haut niveau de sécurité, même si le mdp est trouvé il y'aura une autre barrière à fournir.

Mise en place

Sa sera du MFA google, en utilisant l'appli authenticator

On fait une petite update de la liste des paquets et on installe ce paquet qui est un module à PAM pour MFA selon son nom

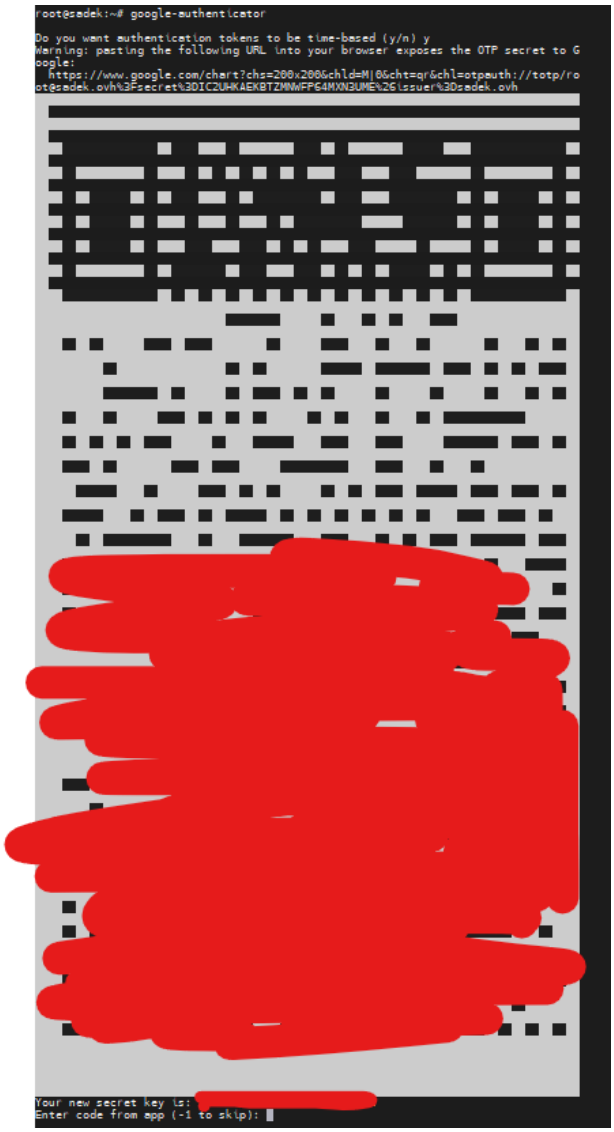


Ensuite exécuter cette commande : google-authenticator

Ensuite une question

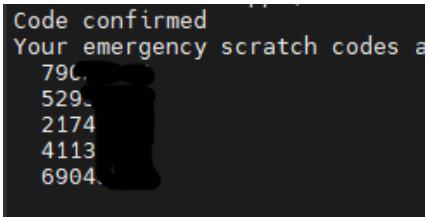
La première pour savoir si on veut que le mdp sois temporaire

Ensuite un QR code s'affiche qu'il faut scanner avec son appli



Le code temporaire qui s'affiche sur notre appli doit être saisi en bas

Ensuite un code de secours s'affiche au cas ou

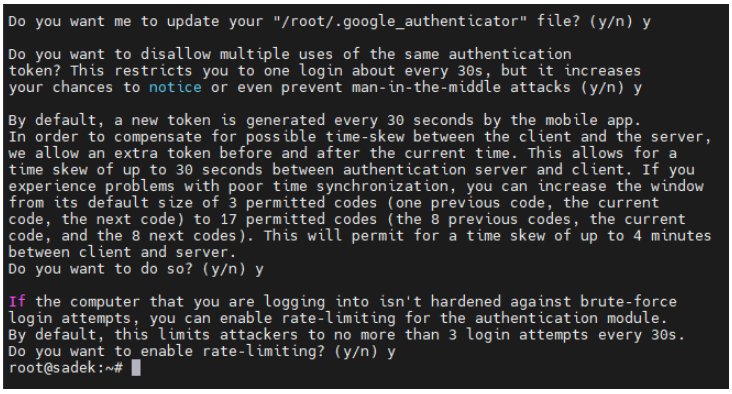


Ensuite on nous demande si on veut mettre à jour le fichier. google_authenticator , on dit oui.

Ensuite on nous demande si on veut désactiver l'authentification à plusieurs users avec le même token, on dit oui

Ensuie on dit oui pour un token toute les 30 sec c'est amplement suffisant

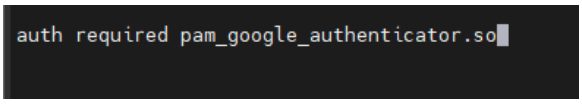
Ensuite on active le blocage pendant 30 sec en cas de tentative 3 fois non réussis



Ensuite il faut modifier ce fichier

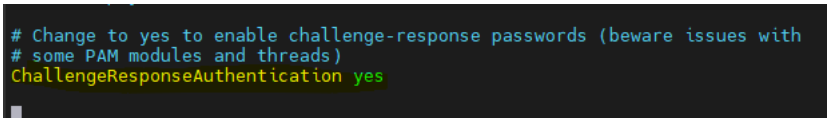
/etc/pam.d/sshd

Et on rajoute cette ligne à la fin du fichier



Ensuite il faut modifier le fichier de conf du serveur sshd

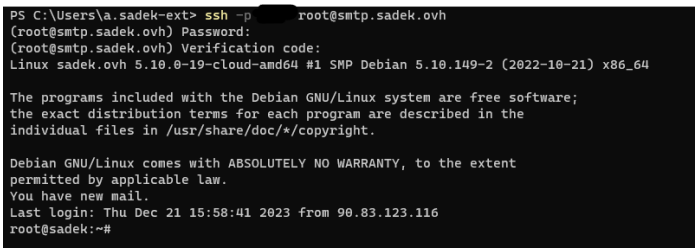
Ici il faut faire passer de « no » à « yes »



Test

Ensuite on redémarre le service ssh on garde notre connexion et on ouvre une nouvelle fenêtre de connexion

Et voila



Remarque

Avec mobaxterm sa ne fonctionne pas mais client ssh basique oui.