ksu

Version kerberisé de su

ksu est une version Kerberisé du programme su qui a 2 objectifs : sécuriser les changements d'ID d'utilisateur réel et effctifs, et de pouvoir créer de nouveaux contextes de sécurité.

Authentification

ksu opère en 2 phases : l'authentification et l'autorisation. Résoudre le nom du principal de la cible est la première étape de l'authentification. L'utilisateur peut soit spécifier sont nom de principal avec -n, ou un nom de principal par défaut sera assigné en utilisant l'heuristique. Le nom de l'utilisateur cible doit être le premier argument du ksu ; si non spécifié, root est le défaut. Si **.** est spécifié, l'utilisateur cible sera l'utilisateur source, Si l'utilisateur source est root ou l'utilisateur cible est l'utilisateur source, aucune authentification est aucune autorisation ne sera effectuée. Sinon, ksu recherche un ticket Kerberos approprié dans le cache de la source.

Ce ticket peut être soit pour un serveur final, ou un TGT pour le domaine du principal cible. Si le ticket pour le serveur final est déjà dans le cache, il est déchiffré et vérifié. S'il n'est pas dans le cache mais que le TGT l'est, le TGT est utilisé pour obtenir le ticket. Si aucun de cet tickets n'est présent, et ksu est compilé avec **GET_TGT_VIA_PASSWD**, l'utilisateur devra entrer son mot de passe qui sera ensuite utilisé pour obtenir un TGT. Si l'utilisateur est loggé à distance et n'a pas de canal sécure, le mot de passe peut être exposé. Si ni le ticket ni **GET_TGT_VIA_PASSWD** ne sont présent, l'authentification échoue.

Autorisation

Cette section décris l'autorisation de l'utilisateur source quand ksu est appelé sans l'option **-e**.Une fois l'authentification réussie, ksu vérifie que le principal cible est autorisé pou accéder au compte cible. Dans le home de l'utilisateur cible, ksu tente d'accéder à .k5login et .k5users Pour vérifier les autorisations.

Si le nom du principal cible est trouvé dans le .k5login, l'utilisateur source, est autorisé à accéder au compte cible. Sinon, ksu recherche le fichier .k5users. Si le nom de principal cible est trouvé sans commandes ou suivi uniquement par *, l'utilisateur source est autorisé. Si les 2 fichiers ne sont trouvés mais qu'aucune entrée appropriée pour le principal cible n'existe, l'accès est refusé. Si les 2 fichiers n'existent pas le principal aura accès au compte en accord avec la règle de mappage aname->lname. Sinon l'autorisation échoue.

Exécution du shell cible

Une fois l'autorisation réussie, ksu se comporte comme su. L'environnement n'est pas modifié sauf **USER**, **HOME**, et **SHELL**. Si l'utilisateur cible n'est pas root, **USER** est l'utilisateur cible. Sinon **USER** reste inchangé. La variable d'environnement **KRB5CCNAME** est définie au nom du cache de la cible. L'ID utilisateur réel et effectif sont changés à l'utilisateur cible. Une fois le shell terminé, ksu supprime le cache cible, sauf si -k.

Créer un nouveau contexte de sécurité

ksu peut être utilisé pour créer un nouveau contexte de sécurité pour le programme cible (soit le shell, soit la commande spécifiée avec -e). Le programme cible hérite d'un jeu d'accréditifs de l'utilisateur source. Par défaut, ce jeu inclue tous les accréditifs dans le cache source, plus tout type d'accréditifs obtenus durant l'authentification. L'utilisateur source est capable de limiter les accréditifs dans le jeu avec les options -z ou -Z. -z restreins la copie des tickets du cache source dans le cache cible aux seuls tickets où le client == le nom principal cible. -Z fournis à l'utilisateur cible un cache neuf, sans accréditifs. Noter que pour des raisons de sécurité, quand l'utilisateur source est root et l'utilisateur cible non-root, -z est le mode par défaut.

Note : durant l'authentification, seul les tickets qui pourraient être obtenus sans fournir de mot de passe sont cachés dans le cache source.

OPTIONS

-n target_principal_name Spécifie un nom de principal cible. non spécifié, un nom de principal par défaut est assigné via les cas suivant :

Cas 1 : l'utilisateur source est non-root Si l'utilisateur cible est l'utilisateur source, le nom de principal par défaut est définis au principal par défaut du cache source. Si le cache n'existe pas, le nom de principal par défaut est **target_user@local_realm**. Si les utilisateurs source et cible sont différent et que .k5users et .k5login n'existent pas, le nom de principal est **target_user_login_name@local_realm**. Sinon, en commençant avec le premier principal listé ci-dessous, ksu vérifie si le principal est autorisé à accéder au compte cible et s'il y a un ticket pour ce principal dans le cache source.

a. Principal par défaut du cache source

b. target_user@local_realm

c. source_user@local_realm

Cas 2 : l'utilisateur source est root Si l'utilisateur cible est non-root, le nom de principal par défaut est **target_user@local_realm**. Sinon, si le cache source existe, le nom est un principal par défaut du cache source. Si le cache source n'existe pas, le nom est **root\@local_realm**.

-c source_cache_name Spécifie le nom du cache source. Non spécifié, utilise **KRB5CCNAME**, ou définis à krb5cc_<target uid>.(gen_sym()).

-k Ne supprime pas le cache cible à la sortie du shell ou de la commande.

-d mode debug

-z Restreins la copie de tickets du cache source dans le cache cible aux seuls tickets où client==le nom du principal cible.

-Z Ne copie aucun tickets du cache source dans le cache cible.

-q mode silencieux

-l lifetime (chaîne time_duration) Spécifie la durée de vie pour les tickets demandés. défaut 12 heures.

-r time (chaîne time_duration) spécifie l'option renewable à demander pour les tickets.

-p Spécifie que l'option proxiable devrait être demandé pour le ticket

-f Spécifie que l'option forwardable devrait être demandé pour le ticket

-e command [args ...] Exécute la commande spécifiée au lieu d'exécuter le shell cible.

Le fichier .k5users a le format suivant : Une seul entrée par ligne qui peut être suivie par une liste de commandes que le principal est autorisé à exécuter. Un nom de principal suivi par un ***** signifie que l'utilisateur est autorisé à exécuter une commande. Ainsi, l'exemple suivant :

jqpublic@USC.EDU ls mail /local/kerberos/klist
jqpublic/secure@USC.EDU *
jqpublic/admin@USC.EDU

La première ligne autorise à exécuter ls, mail et klist. La deuxième ligne autorise à exécuter toute commande, et la troisième autorise uniquement à exécuter le shell cible, tout comme la deuxième ligne, mais pas la première.

-a args Spécifie les arguments à passer au shell cible. cette option peut être utilisé pour simuler l'option -e avec : **-a -c[command [arguments]]**.

Instructions d'installation

ksu peut être compilé avec les flags suivant :

GET_TGT_VIA_PASSWD Si aucun ticket approprié n'est trouvé dans le cache source, demande à l'utilisateur son mot de passe.

PRINC_LOOK_AHEAD Durant la résolution du nom de principal par défaut, permet à ksu de trouver les noms des principaux dans le fichier .k5users.

CMD_PATH Spécifie une liste de répertoires contenant les programmes que les utilisateur sont autorisés à exécuter (via le fichier .k5users)

HAVE_GETUSERSHELL Si l'utilisateur source est non-root, ksu insiste pour que le shell de l'utilisateur invoqué soit un shell légal.

ksu devrait être possédé par root et avoir le set user bit mis.