ausyscall

Mappage des noms en numéro syscall

ausyscall affiche le mappage des noms syscall en numéro et inversement pour l'architecture donnée. Il peut être utilisé pour vérifier les numéros syscall dans une plateforme pour optimiser les règles.

Supposons une règle auditctl :
-a always, exit -S open -F exit=-EPERM -k fail-open
Pour vérifier que les programmes 32 et 64 bits sont audités, lancer
ausyscall i386 open
et
ausyscall x86_64 open
Et regarder les numéros retournés. S'ils sont différents, il faut écrire 2 règles pour obtenir une couverture complète :
-a always,exit -F arch=b32 -S open -F exit=-EPERM -k fail-open
-a always,exit -F arch=b64 -S open -F exit=-EPERM -k fail-open

OPTIONS

–dump Affiche tous les syscalls pour l'architecture donnée

–exact Match exact (au lieu de partiel) du nom syscall