TP analyse de configuration Basique

NOTE : Un test d'audit ne sort que des erreurs et un programme par test ! me rendre prenom_nom_tp1.tar.gz

Routeur (router.unix)

TEST1 : Ecrire un programme qui vérifie que « service password-encryption » est configuré.

TEST2 : Ecrire un programme qui vérifie que chaque configuration implémente pour « snmp-server » avec une « access-list » et un droit d'accès uniquement « RO » (ne pas vérifier si l'access-list est définie, on le fera en test 5 :-).

TEST3 : Ecrire un programme qui vérifie que chaque « line » implémente une « access-class xx in » et une « access-class xx out ».

TEST4 : Ecrire un programme qui vérifie que toute interface ayant une adresse ip effective/valide implémente un « access-group ».

TEST5 : Ecrire un programme « générique » qui contrôle les ACLs définies mais pas appliquées et les ACLs appliquées, mais pas définies.

a. ACLs définies de type « access-list » « ip access-list extended »
b. ACLs appliquées de type « access-class », « access-group », « snmp-server … »

Catalyst (cat[1-3].unix)

TEST6 : Ecrire un programme qui vérifie que toute interface en « mode trunk » implémente :

c. Implémente « trunk encapsulation »
d. Implémente « native vlan »
e. Implémente « allowed vlan »
f. N'implémente pas « port-security »
g. N'implémente pas « mode access »

TEST7 : Ecrire un programme qui vérifie que toute interface en « mode access » implémente :

h. Implémente « port-security »
i. Implémente « mode access »
j. N'implémente pas « trunk encapsulation »
k. N'implémente pas « native vlan »
l. N'implémente pas « allowed vlan »

Routeur && Ipsec (conf[1-4].unix)

TEST8 : Ecrire un programme qui vérifie que chaque configuration implémente une « access-list 110 » contenant que des adresses en source et destination appartenant à la classe A 192.

TEST9 : Ecrire un programme qui vérifie que chaque configuration implémente :

La définition d'une « crypto-map » contenant au minimum un peer, une politique ipsec (« transform_set) et un filtrage sur les adresses ip (« match *access-list-number*). La définition de la dite devra être contrôlée.

L'application d'une « crypto map » pour toutes les interfaces de type « FastEthernet ». Ne pas confondre dans la configuration ***^crypto[ ]map*** versus ***^[ ]crypto[ ]map*** en accroche regex.