

# PASSWORD CISCO

## *Récupération et suppression*

Le but de ce cours est d'apprendre à récupérer le mot de passe d'un équipement Cisco

SALMON Nicolas

21/12/2009



# PASSWORD CISCO

## Récupération et suppression

### **I) CHANGER LE MOT DE PASSE SUR UN ROUTEUR :**

Pour changer le mot de passe actuel sans perdre la configuration, vous pouvez suivre la procédure suivante. Les interfaces vont passer en mode shutdown, il faudra les repasser en up.

- 1) Éteindre et rallumez le routeur
- 2) Pendant le démarrage appuyez sur *Ctrl + Pause* (sous Windows, pour les autres OS voir le document Standard Break) ou pour arriver au prompt ">"
- 3) Entrez la commande : *confreg 0x2142*
- 4) Entrez la commande : *reset*
- 5) Au re-démarrage, le routeur va ignorer le fichier de configuration :
  - ▶ Répondre "*no*" aux questions qu'il va vous poser.
- 6) Entrez en mode enable par la commande : *enable*
- 7) Tapez la commande : *wr*
- 8) Passez en mode configuration : *configure terminal*
- 9) Changez le mot de passe enable secret : *enable secret nouveau-mot-de-passe*
- 10) Supprimez le mot de passe enable simple s'il existe : *no enable password*
- 11) Passez en mode configuration du port Console : *line con 0*
- 12) Changez le mot de passe du port Console : *password nouveau-mot-de-passe*
- 13) Quittez le mode configuration du port console : *exit*
- 14) Configurez le routeur pour un démarrage normal via la commande : *config-register 0x2102*
- 15) Quittez le mode de configuration : *exit*
- 16) Enregistrez la configuration : *wr*
- 17) Relancez le routeur par la commande : *reload*

## II) CHANGER LE MOT DE PASSE D'UN SWITCH :

Pour changer le mot de passe sans perdre la configuration d'un Switch vous pouvez utiliser cette technique :

- 1) Éteindre
- 2) Appuyez sur le bouton en façade et allumez le Switch tout en restant appuyé sur le bouton
- 3) Une fois que le Switch est démarré en mode rommon
- 4) tapez : `flash_init`
- 5) Puis : `load_helper`
- 6) Ensuite : `dir flash:` pour afficher le contenu de la mémoire flash
- 7) Enfin tapez : `rename flash:config.text flash:config.old` pour renommer le fichier qui contient le mot de passe
- 8) Pour recharger l'IOS : `boot`
- 9) Le Switch va ignorer le fichier de configuration :
  - ▶ Répondre "no" à la question qu'il va vous poser.
- 10) Passez en mode `enable` : `enable`
- 11) Renommez le fichier config.old en config.text : `rename flash:config.old flash:config.text`
- 12) Chargez le fichier config.text : `copy flash:config.text system:running-config`
- 13) Passez en mode configuration : `configure terminal`
- 14) Changez le mot de passe enable secret : `enable secret nouveau-mot-de-passe`
- 15) Supprimez le mot de passe enable simple s'il existe : `no enable password`
- 16) Passez en mode configuration du port Console : `line con 0`
- 17) Changez le mot de passe du port Console : `password nouveau-mot-de-passe`
- 18) Quittez le mode de configuration : `end`
- 19) Enregistrez la configuration : `wr`
- 20) Relancez le routeur par la commande : `reload`