Éléments de Configuration Cisco

Notes :

* Les commandes précédées de "$" signifient que vous devez exécuter la commande en tant qu'utilisateur général - et non en tant qu'utilisateur root.
* Les commandes précédées de "#" signifient que vous devez travailler en tant qu'utilisateur root.
* Les commandes comportant des lignes de commande plus spécifiques (par exemple "rtr>" ou "mysql>") signifient que vous exécutez des commandes sur des équipements à distance, ou dans un autre programme.
* Si une ligne de commande se termine par "\", ceci signifie que la commande se poursuit sur la ligne suivante et que vous devez la traiter comme une seule ligne.

Exercices Partie I

0. Travail en équipe

Pour cet exercise, nous allons travailler en groupe. Une personne dans chaque groupe sera désignée pour entrer les commandes au clavier.

Rappel: Groupe 1: pc1-4, Groupe2: pc5-8, etc.

Si vous n'êtes pas certain du groupe auquel vous appartenez, référez vous
au Diagramme Réseau sur http://noc.ws.nsrc.org/

1. Connectez-vous à votre routeur

Loguez-vous à votre image vm/pc et installez Telnet :

```
$ sudo apt-get install telnet
```

Connectez-vous au routeur de votre groupe. En cas de doute, pensez à consulter le schéma du réseau de classe :

http://noc.ws.nsrc.org/wiki/wiki/Diagram

Maintenant connectez-vous à votre routeur

```
        $ telnet 10.10.N.254
        username: cisco         Password: cisco
```

Affichez les informations concernant votre routeur

```
        rtrN>enable                                 (mot de passe par
défaut "cisco")
        rtrN#show run                               (espace pour
continuer)
        rtrN#show int FastEthernet0/0
        rtrN#show ?                                 (liste toutes les
options)
        rtrN#exit                                   (déconnexion du
routeur)
```

2. Configurez votre routeur pour utiliser uniquement SSH

Ces étapes vous permettront d'effectuer les opérations suivantes :

* Créer une clé ssh pour votre routeur
* Créer un mot de passe chiffré pour l'utilisateur Cisco
* Chiffrer le mot de passe (Cisco)
* Désactiver l'accès telnet (non chiffré) à votre routeur
* Activer l'accès SSH (version 2) à votre routeur

Vous devez travailler par groupe de 4. Réunissez-vous avec les membres de votre groupe routeur et désignez une personne pour entrer les commandes. Pour commencer, connectez-vous à l'un des PC utilisés par votre groupe. À partir de ce PC lancez une connexion telnet vers votre routeur :

```
        $ telnet rtrN.ws.nsrc.org       (ou "telnet 10.10.N.254")

        username: cisco
        Password: cisco

        rtrN> enable                                    (en)
        Password: cisco
        rtrN# configure terminal                (conf t)
```

Commençons par donner un nom de domaine à notre routeur, au cas où:

```
rtrN(config)# ip domain-name ws.nsrc.org

rtrN(config)# aaa new-model
rtrN(config)# crypto key generate rsa

How many bits in the modulus [512]: 2048
```

Attendez que la clé soit générée. Vous pouvez maintenant spécifier les mots de passe et ils seront chiffrés. Supprimons d'abord provisoirement notre utilisateur Cisco, nous allons le recréer par la suite :

```
rtrN(config)# no username cisco
rtrN(config)# username cisco secret 0 <MOT DE PASSE DONNÉ EN CLASSE>
```

Maintenant le mot de passe de l'utilisateur Cisco (le mot de passe donné en classe) est chiffré.

Chiffrez ensuite également le mot de passe enable :

```
rtrN(config)# enable secret 0 <MOT DE PASSE DONNÉ EN CLASSE>
```

Nous allons maintenant demander à notre routeur d'autoriser uniquement
des connexions SSH sur les 5 consoles définies (vty 0 à 4):

```
rtrN(config)# line vty 0 4
rtrN(config-line)# transport input ssh
rtrN(config-line)# exit
```

Nous quittons ainsi le mode de configuration "ligne" pour revenir au mode de configuration général. Nous allons maintenant indiquer au routeur d'enregistrer les événements liés au protocole SSH et de n'autoriser que les connexions SSH version 2 :

```
rtrN(config)# ip ssh logging events
rtrN(config)# ip ssh version 2
```

Quittez maintenant le mode de configuration :

```
rtrN(config)# exit
```

Et, enregistrez ces changements dans la configuration permanente du routeur :

```
rtrN# write memory                                    (wr mem)
```

Ok. C'est fait. Vous ne pouvez plus utiliser Telnet pour vous connecter à votre routeur. Vous devez vous connecter en SSH avec l'utilisateur "cisco" et le mot de passe donné en classe. Le mot de passe
Enable est également celui donné en classe - Naturellement, dans une situation
réelle, vous utiliseriez des mots de passe beaucoup plus sûrs.

Avant de quitter votre session Telnet, testez la connectivité SSH depuis
un autre PC dans votre groupe, ou bien depuis une autre fenêtre de terminal.
Nous faisons ceci au cas ou nous aurions fait une erreur de configuration qui
nous laisserait vérouillés hors de notre routeur!

Tout d'abord, essayez à nouveau de vous connecter avec Telnet :

```
$ telnet rtrN.ws.nsrc.org
```

Que se passe-t-il ? Vous devriez voir s'afficher un message du type :

```
Trying 10.10.N.254...
telnet: Unable to connect to remote host: Connection refused
```

Maintenant essayez de vous connecter en SSH :

```
$ ssh cisco@rtrN.ws.nsrc.org
```

Vous devriez voir le message suivant :

```
The authenticity of host 'rtr2.ws.nsrc.org (10.10.2.254)' can't be
established.
RSA key fingerprint is 93:4c:eb:ad:5c:4a:a6:3e:8b:9e:
4f:e4:e2:eb:e4:7f.
Are you sure you want to continue connecting (yes/no)?
```

Tapez "yes" et appuyez sur ENTREE pour continuer ...

L'écran affiche maintenant :

```
Password: <MOT DE PASSE DONNÉ EN CLASSE>
rtrN>
```

Tapez "enable" pour nous permettre d'exécuter des commandes

privilégiées :

```
rtrN> enable
Password: <MOT DE PASSE DONNÉ EN CLASSE>
rtrN#
```

Affichons maintenant la configuration courante du routeur :

```
rtrN# show running                                          (sh
run)
```

Appuyez sur la barre d'espace pour continuer. Regardez les entrées suivantes :

```
enable secret 5 $1$p4/E$PnPk6VaF8QoZMhJx56oXs.
.
.
.
username cisco secret 5 $1$uNg1$M1yscHhYs..upaPP4p8gX1
.
.
.
line vty 0 4
 exec-timeout 0 0
 transport input ssh
```

Vous pouvez voir que le mot de passe Enable et le mot de passe de l'utilisateur Cisco ont été chiffrés. C'est parfait.

Maintenant, vous devez quitter l'interface du routeur pour terminer cet exercice:

```
rtrN# exit
```

Si vous avez toujours une fenêtre avec Telnet ouvert sur votre routeur,
n'oubliez pas de fermez celle-ci également.

NOTES :

1.) Si vous ne pouvez plus accéder à votre routeur après cet exercice,
    informez-en votre instructeur afin qu'il puisse réinitialiser la
    configuration de votre routeur à son état d'origine.

2.) Veuillez n'effectuer cet exercice qu'une seule fois. Si

plusieurs
    personnes effectuent cet exercice, il est très probable que
l'accès
    au routeur soit bloqué.

3.) Au cours de la semaine, vous allez configurer des éléments tels
    que SNMP, NetFlow, etc. sur le routeur de votre groupe. A partir
    de maintenant vous pouvez vous connecter au routeur en SSH
directement,
    depuis votre ordinateur portable ou votre PC.