Sécuriser un routeur Cisco

Sécurisation d'un routeur Cisco sous IOS

BILLET ANATOLE

02 novembre 2015
Version: 1.0

Sécuriser un routeur Cisco

Sécurisation d'un routeur Cisco sous IOS

Avant de commencer…

Objectif :

Le but de ce tuto est de permettre la configuration d'un routeur de façon sécuriser.

Prérequis :

-Un routeur sous IOS

Code couleur :

-Bleu pour les commandes Debian

-Vert pour les noms des fichiers de configurations

-Italic pour les descriptions et anecdotes.

Table des matières

AVANT DE COMMENCER… 1
OBJECTIF : 1
PREREQUIS : 1
CODE COULEUR : 1

1. Désactivation des services inutiles

Pour sécuriser un routeur la première étape est de désactiver les services pouvant fournir une faille ou un « way in » à d'éventuels intrus.

Nous désactiverons donc les services suivants :

-Les services IP (small servers)

-Le Bootp

-Le service finger

-Le SNMP

-Le service http

-Le service CDP

-Le service de configuration à distance

Nous allons donc en premier lieu désactiver les **services IP** « Small Servers » grâce aux commandes suivantes :

no service tcp-small-servers

no service udp-small-servers

Désactivation du **bootp :**

No ip bootp server

Désactivation du **service finger :**

No ip finger

Désactivation du **SNMP :**

No snmp-server

Désactivation du **http** :

No ip http server

No ip http secure-server

No ip http active-session-modules WEB_EXEC

No ip http secure-active-session-modules WEB_EXEC

Désactivation du **service CDP :**

no cdp run
no cdp advertise-v2

Désactivation des **services de configuration à distances :**

Line vty 0 4 puis **transport input none**

Désactivation de **l'ip sans classe :**

No ip classless

Désactivation de La recherche **DNS** :

No ip domain-lookup

Désactivation des **requêtes TFTP** :

No service config

Désactivation des **broadcast dirigés :**

A réaliser dans les interfaces désirées :

No ip directed-broadcast

Désactivation **Le routage des redirections ICMP :**

A réaliser dans les interfaces désirées :

No ip redirect

Désactivation du **routage par la source :**

No ip source-route

Désactivation de l'**ip unreachable :**

A réaliser dans les interfaces désirées :

No ip unreachables

2. Ajout de mot de passe

Tout d'abord vérifié que le **chiffrement des mots de passes** est bien activé :

service password-encryption

Puis on applique le mdp du **mode privilégié** :

enable password [mot de passe]

ensuite le mot de passe d'**accès à la console** :

line con 0

password [mot de passe]

et finalement le mode de passe de **l'accès telnet et SSH :**

line vty 0 4

password [mot de passe]

3. Ajout d'une bannière au login

Utilisé la commande :

banner motd {caractère}[banner Text]{caractère}

Ou le caractère est une lettre délimitant le texte.

4. Ajout de commentaires aux interfaces

Pour ajouter une description aux interfaces entrez dans la configuration de celle-ci la commande suivante :

Description [commentaire]

5. Sauvegarde et restauration

On utilise sous notre client windows l'application **TFTPD64** pour récupérer les conf à distance.

/!\ *pensez à couper votre pare-feu et à attribuer une adresse ip à l'interface du routeur utilisé* /!\

Puis sur le routeur entrez la commande suivante :

Copy running-config

Puis il vous sera demandé l'ip du server TFTP ainsi que le nom sous lequel le fichier sera enregistré.

Pour copier le fichier flash de configuration identifier son nom grâce à :

Show flash

Puis copié le fichier en TFTP comme cela :

Copy flash : tftp

Puis il vous sera demandé l'ip du server TFTP ainsi que le nom du fichier source et celui sous lequel le fichier sera enregistré.

End