Institut Universitaire de Technologie
Aix*Marseille Université

Réseaux & Télécoms

TP – Initiation aux réseaux d'entreprise

Accès au routeur
"Crack" du mot de passe administrateur

1 Mise en place d'une configuration

L'idée de cette première partie est d'installer dans le routeur une configuration écrite par exemple sous packet-tracer. Pour cela, commencez par récupérer le fichier de configuration détenu par votre chargé de TP. Puis, démarrez votre routeur.

Une fois le routeur démarré, vérifiez que votre prompt est bien `Routeur>` **et si ce n'est pas le cas, appelez le chargé de TP**.

Passez administrateur et entrez la commande `show version`.

> Quelle est la valeur du registre de configuration ?
> A quoi sert le registre de configuration?

Passez en mode de configuration et injecter par un copier-coller le fichier configuration récupéré précédemment.

Redevenez administrateur

> Quel est le prompt du routeur ?

Au moyen de la commande `copy running-config startup-config`, sauvegardez la configuration active dans la configuration de démarrage, et relancer alors le routeur au moyen de la commande `reload`.

Une fois le routeur redémarré, essayez à nouveau de passer administrateur.

> Y arrivez-vous ?
> Si non pourquoi ?
> Dans quel fichier était stocké le mot de passe administrateur qui vous est inconnu ?
> Si nous n'avions pas chargé le fichier de configuration de démarrage, aurions-nous pu devenir administrateur ?

2 Crack du routeur (ou comment prendre le pouvoir)

Vous allez donc maintenant mettre en œuvre une procédure de changement du mot de passe administrateur alors même que vous ne pouviez pas passer administrateur. Pour cela

1. éteignez votre routeur
2. redémarrez-le et interrompez la séquence d'amorçage en appuyant simultanément sur les touches `Ctrl` et `Pause`

Si tout se passe bien, votre routeur affiche l'invite `rommon 1>.`

Vous allez maintenant modifier le registre de configuration de telle sorte que le routeur ne charge pas le fichier de configuration de démarrage lors du prochain démarrage. Pour cela :

1. tapez la commande `confreg 0x2142` suivi de la touche `Entrée` ;
2. tapez la commande `reset` pour relancer le routeur.

Attendez que le routeur soit réamorcé. Tapez `no` lorsqu'une invite vous propose d'entrer le dialogue de configuration. Appuyez sur la touche `Entrée` pour afficher l'invite `Router>.`

Devenez administrateur.

Pourquoi aucun mot de passe n'est requis ?

Quelle commande permet de voir la valeur du registre de configuration ?
Quelle est la valeur du registre de configuration ?

Vous allez maintenant rechargez manuellement le fichier de configuration de démarrage du routeur en entrant la commande

```
Routeur#copy startup-config running-config
```

(ATTENTION DE NE PAS FAIRE L'INVERSE !!!)

Quel est le prompt affichée maintenant par le routeur ?
Pourquoi avons-nous réalisé cette manipulation ?

Passez en mode de configuration et saisissez un nouveau mot de passe administrateur. Puis rétablissez la valeur du registre de configuration à sa valeur normale (`0x2102`). Pour cela, entrez la commande `jld(config)#config-register 0x2102`.

Sortez du mode de configuration, et moyen de la commande `show version` vérifiez quelle sera la valeur du registre au prochain redémarrage.

3 Fin

Effacer la configuration de démarrage, mettez hors tension le routeur et remettez le câble console à sa place.