La Plateforme

Let's take control

Jarvis, il faut parfois savoir utiliser ssh avant de savoir utiliser Linux. Iron-man

Introduction

Aujourd'hui, vous allez pouvoir faire vos premières opérations d'administrateur système et sécurité. Effectuer des manipulations à distance sont des classiques pour administrer des serveurs.

Vous allez vous pencher sur les connexions à distance SSH et l'automatisation des tâches.
La configuration de SSH sur votre machine est un prérequis pour tous les projets suivants.

Job 1

Installez ou activez le service permettant de se connecter en SSH à vos machines primaires et secondaires. Depuis votre machine hôte, connectez-vous à votre machine primaire.

Faites en sorte que le message “Hello admin @ primary” soit affiché lorsque l'utilisateur “admin” se connecte sur le serveur.

Job 2

Est-ce suffisamment sécurisé ?

Changez le port du service et mettez en place une clé RSA. Pour ce faire, il faut générer un mode d’échange de clés (Privé et Public) comme pour une PKI.

Vous pouvez en outre paramétrer un mot de passe. Si vous ne souhaitez pas garder cette option, laissez-passer l’étape passphrase.

Copiez la clé publique sur le serveur distant pour la mettre dans le fichier authorized_keys.

Job 3

L’utilisateur “root” doit-il être autorisé à se connecter ?

Créez le groupe d’utilisateurs “sshusers”.

Modifier la configuration du serveur SSH de sorte que seuls les utilisateurs de ce groupe puissent se connecter.

Ajoutez l'utilisateur "assistant" dans le groupe sshusers

Job 4

La mission de votre équipe consiste à déployer des softs. La procédure sécurité selon ISO 2700x que vous avez arrêté est la suivante : test / validation avant mise en service.

Le serveur secondaire va servir aux tests.

Testez la procédure à l'aide de la commande scp :

Sur les deux serveurs, créez deux fichiers de configurations conf1.conf et conf2.conf dans le répertoire "/home/*utilisateur*/config".

Poussez conf1.conf à partir du serveur primaire vers le serveur secondaire.

Récupérez le fichier conf2.conf du serveur secondaire vers le serveur primaire.

Job 5

L'utilisateur assistant a abusé de ses attributions d'administrateur sur le serveur primaire et a ajouté des signatures de virus test. Il ne sait pas que c'est un virus inoffensif.

Connectez-vous avec le compte "assistant" et insérez ce texte dans conf1.conf.

X5O!P%@AP[4\PZX54(P^)7CC)7}$ERICA-STANDARD-A script linux -ILE!$H+H* :://

Poussez avec la commande adéquate le fichier du serveur secondaire vers le serveur primaire.

Job 6

En tant qu'administrateur système sécurité (root), vous vous connectez à distance pour réparer les dégâts.

Comment pouvez-vous afficher les modifications apportées aux fichiers ?

Enregistrez le rendu dans un fichier.

Détruisez le fichier malsain conf1.conf puis remplacez-le par conf2.conf en utilisant une fonction de copie.

Réfléchissez aux questions suivantes :

- Y a-t-il des outils permettant de faire des opérations à distance d'un serveur Linux vers des clients Windows ?
- Quels outils et commandes utiliseriez-vous si vous étiez dans un environnement Windows ?
- Comment transférer des fichiers de Windows vers Windows ?
- Quels outils se lancent à partir d'un navigateur ?
- Quels outils permettent de prendre le contrôle de la souris sur un poste client Windows ?

Job 7

Il va falloir prendre des mesures. Certainement, vous rapprochez de la DRH pour envisager de lui proposer quelques jours de repos.

En attendant, il faut d'abord mettre "assistant" hors d'état de nuire.

Bloquez ses droits sans désactiver le compte, car il a encore des tâches à finir sans danger pour le SI avant d'envisager de désactiver son compte ou supprimer son compte ?

Retirez tous les droits d'écriture sur les fichiers.

Job 8

Vu l'évènement, vous vous dites qu'il serait bien de sauvegarder les configurations dans un dossier spécifique "sauvegarde_deploiements".

Faites un script qui automatise la copie de nouveau fichiers de configuration vers "sauvegarde déploiements" tous les jours à 12 h 01 et regroupez les toutes les semaines un 1 seul archive protégé par un mot de passe.

Job 9

L'école s'est dotée d'une charte, mais à la suite de vols par effraction, elle vient vous consulter pour le renforcement des clauses de sécurité. Que voyez-vous à ajouter, notamment pour le respect des accès physiques, concernant l'introduction de tiers non autorisés ? Le respect et la responsabilité dus au matériel IT prêté ?

Par ailleurs, pensez-vous que la charte suffit pour faire respecter les barrières usages privés et usages scolaires ?

Charte Informatique du Collège et Lycée Charles HERMITE

La présente charte a pour objet de définir les règles d'utilisation des moyens informatiques du lycée-collège Charles Hermite.

Champ d'application de la charte

Les règles et obligations ci-dessous énoncées s'appliquent à toute personne, (élève, professeur, personnels administratifs ou techniques) autorisée à utiliser les moyens informatiques du lycée-collège Charles Hermite.

Conditions d'accès au réseau de l'établissement

Chaque utilisateur se voit attribuer un identifiant, (nom de login) et un mot de passe qui lui permettront de se connecter au réseau de l'établissement, à son répertoire privé, pédagogique et autre répertoire de service. Ce compte informatique est strictement personnel. Chaque utilisateur est responsable de l'utilisation qui en est faite et s'engage à ne pas communiquer son mot de passe à une tierce personne.

Respect des règles de la déontologie Informatique

Chaque utilisateur s'engage à respecter les règles de la déontologie et notamment à ne pas effectuer des opérations qui pourraient avoir pour conséquence :

- de masquer sa propre identité,
- de s'approprier le mot de passe du compte d'autrui,
- d'altérer les données ou d'accéder a des informations appartenant à d'autres utilisateurs du réseau sans leur autorisation,
- de porter atteinte à l'intégrité d'un utilisateur ou à sa sensibilité, notamment par l'intermédiaire de messages, textes ou images provocants,
- de mettre en péril le fonctionnement normal du réseau ou d'un des systèmes connectés au réseau,
- de modifier ou de détruire des Informations sur un des systèmes connectés au réseau,
- de se connecter ou d'essayer de se connecter sur un site sans y être autorisé.

La Réalisation d'un programme informatique ayant de tels objectifs est également interdite.

Utilisation de logiciels

Les administrateurs installeront les logiciels à la demande des utilisateurs après vérification de la nature de ceux-ci et l'usage qui en sera fait. Ils ont la possibilité de détruire tout élément paraissant contraire à l'esprit de la charte. L'utilisateur ne devra en aucun cas :

- faire des copies de logiciels n'appartenant pas au domaine public,
- faire une copie d'un logiciel commercial,
- installer des logiciels
- contourner les restrictions d'utilisation d'un logiciel,
- développer au introduire un des programmes qui s'auto dupliquent ou s'attachent à d'autres programmes (virus informatiques).

Protection des mineurs et droit au respect de la vie privée

Chacun a droit au respect de sa vie privée, toute personne peut interdire la diffusion de données nominatives le concernant, et en particulier de son image sans accord préalable. S'agissant de mineurs, ce droit à l'image et au respect de sa personne est d'application stricte. Le non respect de cette protection est sanctionné par les art. 226-1 à 226-7 du code pénal.

L'utilisateur qui contreviendrait aux règles précédemment définies s'expose aux sanctions administratives prévues par le règlement de l'établissement, ainsi qu'aux sanctions et poursuites pénales prévues par les textes législatifs et réglementaires en vigueur dont il reste soumis.

Rendu

Une soutenance aura lieu afin de présenter les différentes compétences vues durant la semaine.

Compétences visées

- Administration système

Base de connaissances

- Comment installer SSH ?
- Comment générer une clé SSH ?
- Mettre en place une Authentification pour SSH
- Changer sa clé SSH en cas de perte
- Créer un nouvel utilisateur SSH
- Sauvegarde automatique
- Contrôle à distance
- Mettre en place des Cron
- Mettre en place des Cron
- Mettre en place des Cron
- Debian Handbook