DOCUMENTATION

Abderraouf METIDJI

Job 1

Afficher le manuel de la commande ls

Pour afficher le manuel de la commande ls il faut utiliser la commande "***man ls***" qui signifie tout simplement "***manuel ls***".

Cela nous affiche le manuel de la commande ***ls*** avec des indications tels que :

NAME
ls - list directory contents

SYNOPSIS
ls [OPTION]... [FILE]...

DESCRIPTION
List information about the FILEs (the current directory by default). Sort entries alphabetically if none of -cftuvSUX nor --sort is specified.

Mandatory arguments to long options are mandatory for short options too.

-a, --all
do not ignore entries starting with .

-A, --almost-all
do not list implied . and ..

--author
with -l, print the author of each file

-b, --escape
print C-style escapes for nongraphic characters

Afficher les fichiers cachés du home de votre utilisateur

Pour lister dans un terminal les éléments non-cachés du dossier en cours, entrez la commande : ***ls***

Pour afficher tous les éléments, y compris les éléments cachés, il suffit d'ajouter l'argument ***-a*** («all» en anglais) : ***ls -a***

Et pour n'afficher que les fichiers et dossiers cachés : ***ls -d .****

Si vous ajoutez /, vous ne voyez que les dossiers cachés : ***ls -d .*/***

Afficher les fichiers cachés plus les informations sur les droits sous forme de liste

Afin d'afficher les fichiers cachés nous réutilisons la commande "***ls -a***" comme indiqué ci-dessus.

Pour afficher le résultat en ligne nous ajoutons la commande ***-1***, cela donne "***ls -1 -a***".

Et enfin, pour afficher le détails des droits tout en préservant l'aspect liste nous utilisons la commande "***ls -1 -l***".

-l permettant d'afficher le détail des fichiers.

abdou@abdou-virtual-machine:~$ ls -1 -l
total 36
drwxr-xr-x 2 abdou abdou 4096 oct. 2 20:23 Desktop
drwxr-xr-x 2 abdou abdou 4096 oct. 2 20:23 Documents
drwxr-xr-x 2 abdou abdou 4096 oct. 2 20:23 Downloads
drwxr-xr-x 2 abdou abdou 4096 oct. 2 20:23 Music
drwxr-xr-x 2 abdou abdou 4096 oct. 2 20:23 Pictures
drwxr-xr-x 2 abdou abdou 4096 oct. 2 20:23 Public
drwx------ 4 abdou abdou 4096 oct. 3 10:09 snap
drwxr-xr-x 2 abdou abdou 4096 oct. 2 20:23 Templates
drwxr-xr-x 2 abdou abdou 4096 oct. 2 20:23 Videos

Comment ajouter des options à une commande ?

Prenons la commande ls en exemple. La syntaxe de la commande ls est la suivante :

ls [OPTION]... [FILE]...

Le 1er mot tapé est une commande. Les lettres tapées après un tiret, et les mots tapés après 2 tirets, sont des options. Le reste ce sont des paramètres.

Quelles sont les deux syntaxes principales d'écriture des options pour une commande ?

Certains utilitaires servent à en documenter d'autres : par exemple l'utilitaire info et l'utilitaire man.

info man : donne des infos sur la commande man
man info : donne le manuel de la commande info

Job 2

Lisez un fichier en utilisant une commande qui permet seulement de lire

La commande cat est une commande qui affiche le contenu d'un fichier dans la sortie du terminal.

C'est la façon la plus simple pour lire le contenu d'un fichier en ligne de commandes.

La syntaxe est simple puisqu'il suffit de spécifier le nom du fichier :

"***cat fichier.txt***"

La commande nl (*number lines*) fonctionne comme cat pour afficher le contenu d'un fichier dans le terminal.

La seule différence est qu'elle affiche les numéros de lignes.

"***nl fichier.txt***"

A noter que cat sait aussi le faire avec l'option -n :

"***cat -n fichier.txt***"

Dans notre cas nous pouvons utiliser :

"***nl .bashrc***" / "***cat .bashrc***" / "***cat -n .bashrc***"

Afficher les 10 premières lignes du fichier ".bashrc"

La commande head est une autre façon de consulter un fichier texte, mais avec une légère différence.

Elle affiche les 10 premières lignes d'un fichier texte par défaut.

"***head fichier.txt***"

Dans notre cas nous utiliserons "***head .bashrc***"

Afficher les 10 dernières lignes du fichier ".bashrc"

La commande tail génère les dernières parties d'un seul fichier ou plusieurs fichiers.
Par défaut, la commande tail imprime les dix dernières lignes des fichiers d'entrée.

Enfin on peut aussi l'utiliser pour la lecture de fichiers journaux en temps réel.

“***tail fichier.txt***”

Dans notre cas nous utiliserons : “***tail .bashrc***”

Afficher les 20 premières lignes du fichier “.bashrc”

Ici on utilise également la commande head mais avec des options on peut choisir le nombre de lignes à afficher.

Ainsi, vous pouvez afficher les N premières lignes d’un fichier et même les N dernières lignes d’un fichier.

“***head -n 30 fichier.txt***” - cela affichera les 30 premières lignes du document fichier.txt

Dans notre cas nous utiliserons “***head -n 20 .bashrc***” ou “***head -20 .bashrc***”

Afficher les 20 dernières lignes du fichier “.bashrc”

Ici on utilise également la commande head mais avec des options, tout comme pour la commande head, on peut choisir le nombre de lignes à afficher.

“***tail -n 30 fichier.txt***” - cela affichera les 30 dernières lignes du document fichier.txt

Dans notre cas nous utiliserons “***tail -n 20 .bashrc***” ou “***tail -20 .bashrc***”

Job 3

Installer le paquet “cmatrix”

L'installation du package cmatrix sur Ubuntu est aussi simple que d'exécuter la commande suivante sur le terminal:

sudo apt-get update
sudo apt-get install cmatrix

Lancer le paquet que vous venez d’installer

Afin de lancer le paquet cmatrix il suffit d’écrire “***cmatrix***” dans le terminal.

Mettre à jour son gestionnaire de paquets

Pour mettre à jour le gestionnaire de paquets nous pouvons utiliser la commande

sudo apt update

Mettre à jour ses différents logiciels

Suite à cela nous pouvons utiliser la commande suivante : ***apt list --upgradable***

Cette commande nous permet de voir la liste des paquets que nous pouvons mettre à jour.

abdou@abdou-virtual-machine:~$ apt list --upgradable
Listing... Done
apt-utils/jammy-updates 2.4.7 amd64 [upgradable from: 2.4.6]
apt/jammy-updates 2.4.7 amd64 [upgradable from: 2.4.6]
dmidecode/jammy-updates 3.3-3ubuntu0.1 amd64 [upgradable from: 3.3-3]
evolution-data-server-common/jammy-updates,jammy-updates 3.44.4-0ubuntu1 all [upgradable from: 3.44.2-0ubuntu1]
evolution-data-server/jammy-updates 3.44.4-0ubuntu1 amd64 [upgradable from: 3.44.2-0ubuntu1]
fonts-opensymbol/jammy-updates,jammy-updates 2:102.12+LibO7.3.6-0ubuntu0.22.04.1 all [upgradable from: 2:102.12+LibO7.3.5-0ubuntu0.22.04.1]
fprintd/jammy-updates 1.94.2-1ubuntu0.22.04.1 amd64 [upgradable from: 1.94.2-1]
gir1.2-gnomedesktop-3.0/jammy-updates 42.4-0ubuntu1 amd64 [upgradable from: 42.2-0ubuntu1]
gir1.2-gtk-4.0/jammy-updates 4.6.6+ds-0ubuntu1 amd64 [upgradable from: 4.6.5+ds-0ubuntu1]
gjs/jammy-updates 1.72.2-0ubuntu1 amd64 [upgradable from: 1.72.0-3~ubuntu22.04.2]

Si nous souhaitons les mettres à jour nous pouvons utiliser les commandes suivantes :

sudo apt upgrade

upgrade : les paquets seront remplacés par des versions plus récentes, mais sans qu’aucun autre paquet ne soit ajouté ou supprimé. Par exemple, une nouvelle version de Firefox sera installée avec apt upgrade.

sudo apt full-upgrade

full-upgrade : même chose que apt upgrade, mais supprime des paquets si cela est nécessaire pour installer les nouvelles versions des paquets.

Télécharger les internets : Google

Installez wget si on ne l'a pas déjà. Il s'agit de l'outil qui vous permettra de télécharger le paquet de Chrome à partir de l'invite de commandes :

sudo apt install wget

Utilisez wget pour télécharger le paquet Chrome grâce à la commande :

wget https://dl.google.com/linux/direct/google-chrome-stable_current_amd64.deb

Installez le paquet Chrome que vous avez téléchargé grâce à la commande :

sudo dpkg -i google-chrome-stable_current_amd64.deb

Corrigez les erreurs qui sont apparues lors de l'installation :

sudo apt-get install -f

On peut ensuite utiliser ***google-chrome*** afin de lancer l'application.

Redémarrer votre machine

Pour redémarrer votre ordinateur en ligne de commande, exécutez les commandes suivantes dans votre terminal :

sudo reboot ou ***sudo shutdown -r now***

Éteindre votre machine

Pour l'éteindre :

sudo halt ou ***sudo shutdown -h now***

Job 4

Créer un fichier users.txt qui contiendra User1 et User2 séparé par un retour à la ligne

Pour créer un fichier et y ajouter User1 & User2 nous allons utiliser nano.

Pour cela nous devons d'abord l'installer grâce à la commande

sudo apt install nano

Une fois nano installé il suffit d'écrire

nano nomdufichier

Cela va créer un fichier directement dans le terminal, dans lequel nous pourrons effectuer plusieurs choses. Par exemple, nous pouvons écrire directement dans le terminal et cela sera ajouté au fichier.

Voici quelques commandes utiles :

Ctrl + O pour sauvegarder
Ctrl + X pour quitter nano
Ctrl + U pour coller
Alt + U pour annuler notre dernière action

Dans notre cas nous allons indiquer

nano users.txt

Dans ce fichier nous allons écrire

User1
User2

Et utiliser la commande ***Ctrl + O*** pour sauvegarder suivi de ***Ctrl + X*** pour quitter nano.

Nous pouvons également effectuer cela sans utiliser Nano. Pour cela nous utilisons la commande ***cat*** basique pour créer un fichier

Cat > users.txt

Puis, nous allons à la ligne pour écrire dans le fichier

User1
User2

Et il suffira de faire ***Ctrl Z*** pour arrêter l'écriture dans le fichier.

Il devrait y avoir un prompt qui indique *"[2]+ Stopped cat > users.txt"*

Voilà, votre fichier est créé et vous y trouverez le texte renseigné dans le terminal.

Créer un groupe appelé "Plateformeurs"

Pour créer un groupe, on utilise la commande groupadd

groupadd [nom du groupe à créer]

Dans notre cas nous utiliserons

groupadd Plateformeurs

Créer un utilisateur appelé "User1"

Pour créer un user on utilise la commande

useradd [nom de l'utilisateur]

Dans notre cas nous allons utiliser

useradd User1

Créer un utilisateur appelé "User2"

useradd User2

Ajouter "User2" au groupe Plateformeurs

Pour ajouter un user à un groupe, on utilise la commande usermod :

usermod -a -G [nom du groupe] [nom du user à ajouter]

Dans notre cas nous allons utiliser

usermod -a -G Plateformeurs User2

Nous pouvons également utiliser

usermod -aG Plateformeurs User2

Copier votre “users.txt” dans un fichier “droits.txt”

Pour copier un fichier nous utiliserons la commande ***cp*** qui signifie tout simplement copie/copy

Donc cela donne

cp users.txt droits.txt

Copier votre “users.txt” dans un fichier “groupes.txt”

cp users.txt groupes.txt

Changer le propriétaire du fichier “droits.txt” pour mettre “User1”

La commande ***chown*** permet de changer le propriétaire et/ou le groupe

chown nouvel_utilisateur unfichier

Nous allons donc utiliser

chown User1 droits.txt

Changer les droits du fichier “droits.txt” pour que “User2” ai accès seulement en lecture

Pour ajouter des droits de lecture à un utilisateur nous utilisons la commande

chmod o+r nomdufichier

Dans ce mode d'utilisation, il faut se rappeler que :

u signifie : user (propriétaire) ;

g signifie : group (groupe) ;

o signifie : other (autres) ;

... et que :

+ signifie : « Ajouter le droit » ;

- signifie : « Supprimer le droit » ;

= signifie : « Affecter le droit ».

Dans notre cas nous allons utiliser

chmod o+r droits.txt

Nous pouvons également utiliser 0/1/2/4/7 afin de donner des droits à un utilisateur, un groupe ou le propriétaire du fichier.

Ainsi, rwx « vaut » 7 (4+2+1), r-x « vaut » 5 (4+1) et r-- « vaut » 4. Les droits complets (rwxr-xr--) sont donc équivalents à 754.

Changer les droits du fichier “groupes.txt” pour que les utilisateurs puissent accéder au fichier en lecture uniquement

Nous donnons le droit de lecture aux utilisateurs grâce à la commande vue plus haut

chmod o+r nomdufichier

Dans notre cas nous allons utiliser

chmod o+r groupes.txt

Il faut également enlever le droit d’écriture des utilisateurs pour que l’accès soit uniquement en lecture

chmod o-w nomdufichier

Dans notre cas nous utiliserons

chmod o-w groupes.txt

Changer les droits du fichier pour que le groupe “Plateformeurs” puissent y accéder en lecture/écriture.

Afin d’ajouter le droit d’écriture et de lecture au groupe Plateformeurs il faut utiliser la commande chmod mais en indiquant groupe à la place de other

chmod g+rw nomdufichier

Dans notre cas nous utiliserons

chmod g+rw groupes.txt

Job 5

Ajouter un alias qui permettra de lancer la commande “ls -la” en tapant “la”

Pour ajouter un alias nous utilisons la commande alias. Par exemple, si vous voulez utiliser provisoirement un alias pour supprimer les copies de paquets installés avec l'outil apt-get, vous pouvez saisir:

alias agc='sudo apt-get clean'

Dans notre cas nous utiliserons

alias la=’ls -la’

Ajouter un alias qui permettra de lancer la commande “apt-get update” en tapant “update”

alias update='apt-get update'

Ajouter un alias qui permettra de lancer la commande “apt-get upgrade” en tapant “upgrade”

alias upgrade='apt-get upgrade'

Ajouter une variable d’environnement qui se nommera “USER” et qui sera égale à votre nom d’utilisateur

Afin de créer la variable USER égale à votre nom d’utilisateur il suffit simplement d’écrire dans notre cas

USER=abdou

Grâce à la commande

echo $TEST_VAR

Nous pourrons tester notre variable afin de voir si la valeur qu’on lui a accordé est celle souhaitée

Dans notre cas nous écrivons

echo $USER

Cela donne bien abdou

Mettre à jour les modifications de votre bashrc dans votre shell actuel

Afin de mettre à jour les modifications de notre bashrc dans le shell nous utiliserons la commande

cp .bashrc bashrc-bak

Il est important de l'utiliser avant de modifier le fichier BashRC

Afficher les variables d’environnement

Pour afficher les variables d’environnement nous pouvons utiliser deux commandes

printenv ou ***env***

Ajouter à votre Path le chemin "/home/'votre utilisateur'/Bureau"

Pour ajouter un chemin spécifique à notre Path nous utiliserons

export PATH=$PATH:/chemin/vers/le/repertoire

Dans notre cas nous utilisons

export PATH=$PATH:/home/abdou/Bureau

Job 6

Vous devez télécharger l’archive suivante et la désarchiver seulement avec le terminal.

Pour télécharger un fichier à partir de google drive il faut utiliser

wget “https://drive.google.com/uc?export=download&id=” en ajoutant l’id du fichier à la suite de id=

Dans notre cas nous utiliserons

wget "https://drive.google.com/uc?export=download&id=1s9ZhRhjo0FXcBNRB5khAGK1jVxkZj6Uk"

La commande tar est capable d’extraire (décompresser) ainsi que de compresser une archive.

–c : crée un archive.
–z : compresse l’archive avec gzip.
–v : mode verbeux, affiche la progression.
–f : permet de spécifier le nom du fichier d’archive.

Par exemple, pour extraire le contenu du fichier archive.tar.gz dans le répertoire courant, entrez la commande suivante :

tar -xzvf archive.tar.gz

Il s’agit en fait de la même commande que celle pour créer une archive, sauf que l’on remplace l’option -c par -x qui indique à tar d’extraire une archive au lieu d’en créer une.

Pour extraire le contenu de l’archive dans un répertoire spécifique, il faudra ajouter l’option -C. Par exemple, pour extraire le contenu du fichier archive.tar.gz dans le répertoire /tmp, entrez la commande suivante :

tar -xzvf archive.tar.gz -C / tmp

Dans notre cas nous utilisons

tar -xf 'Ghost in the Shell.tar.gz'

Cela va extraire le fichier tar.gz dans le répertoire de travail actuel. Dans notre cas, cela a extrait le fichier dans le répertoire Downloads.

Job 7

Créer un fichier “une_commande.txt” avec le texte suivant “Je suis votre fichier texte”

Pour créer un fichier avec du texte nous pouvons utiliser la commande echo

echo "votretexte" > nomdufichier.txt

Dans notre cas nous utiliserons

echo “Je suis votre fichier texte” > une_commande.txt

Nous pouvons également utiliser la commande cat vue plus haut

cat > une_commande.txt

“Je suis votre fichier texte”

Ctrl + Z

Compter le nombre de lignes présentes dans votre fichier de source apt et les enregistrer dans un fichier nommé “nb_lignes.txt”

Dans un premier temps il faut localiser le fichier sources. Dans notre cas le fichier sources.list se situe dans /etc/apt

Pour compter les lignes d’un document il faut utiliser

wc -l nomdudocument ou ***wc -l emplacement/nomdudocument***

Dans notre cas nous utiliserons donc la commande

wc -l /etc/apt/sources.list

Pour créer le fichier texte qui contient le nombre de ligne nous combinons les deux commandes vu précédemment

wc -l /etc/apt/sources.list > nb_lignes.txt

Afficher le contenu du fichier source apt et l'enregistrer dans un autre fichier appelé "save_sources"

Pour afficher le contenu du fichier nous utilisons la commande cat vu précédemment. A cela nous ajoutons la commande de création de fichier.

Dans notre cas nous utiliserons

cat /etc/apt/sources.list > save_sources

Faites une recherche des fichiers commençant par "." tout en cherchant le mot alias qui sera utilisé depuis un fichier

Pour faire une recherche de fichier commençant par '.' nous utiliserons la commande find

find -name .*

Pour rechercher les alias il suffit d'utiliser la commande

alias

Pour effectuer les deux recherches ensembles nous pouvons utiliser

find -name .* && alias

Le ***&&*** permettra d'associer les deux recherches

Pour aller plus loin…

Installer la commande tree

Pour installer la commande nous utilisons

apt-get install tree

Lancer la commande tree en arrière-plan qui aura pour but d'afficher toute l'arborescence en de votre / en enregistrant le résultat dans un fichier "tree.save"

Pour lancer la commande tree tout en enregistrant le résultat dans le fichier tree.save nous utilisons la commande

tree > tree.save

Cela va créer un fichier 'tree.save' qui contiendra le résultat de la commande tree

Cependant, si nous souhaitons lancer tree en arrière plan nous devons ajouter "nohup" à la commande.

Nous utiliserons donc

nohup tree > tree.save

Lister les éléments présents dans le dossier courant est utilisé directement le résultat de votre première commande pour compter le nombre d'éléments trouvés

Afin de compter le nombre d'éléments contenu dans le répertoire courant nous allons utiliser la commande

ls -1A |wc -l

Cette commande indiquera le nombre d'éléments contenus dans le dossier utilisé lors de l'exécution.

Lancer une commande pour updater vos paquets, si l'update réussi alors, vous devrez lancer un upgrade de vos paquets. Si l'update échoue, votre upgrade ne se lancera pas

Pour lancer l'update des paquets il faut utiliser la commande

apt-get update

Pour lancer l'upgrade de ces derniers il faut utiliser

apt-get upgrade

Bonus

Installer SSH

Pour installer SSH nous utiliserons la commande

apt-get install

Dans notre cas nous utiliserons

sudo apt-get install openssh-server

Générer une clé SSH

Pour générer une clé SSH nous pouvons utiliser la commande suivante

ssh-keygen

Il faudra ensuite choisir le fichier ou l'on souhaite enregistrer la clé ainsi qu'une passphrase pour protéger la clé en question

Il est également possible de sauter ces 2 étapes en appuyant sur entrer et en laissant l'input vide

Se connecter à une VM ou l'ordinateur d'un camarade via SSH

Pour se connecter à une VM via SSH nous pouvons utiliser la commande

ssh -p <port> user@<ip-address-or-hostname>

Voici un exemple avec une adresse IP publique

ssh -p 22 user@128.128.128.128

Configurer SSH pour empêcher le login root (root ne peut pas se connecter en SSH)

Pour modifier SSH afin d'empêcher le login root il faut suivre les étapes suivantes

Ouvrir le fichier de configuration SSH

nano /etc/ssh/sshd_config

Modifier la ligne

#PermitRootLogin yes

Pour :

PermitRootLogin no

Sauvegarder le fichier avec ***Ctrl + O***

Modifier le port de connexion de SSH (autre que 22)

Pour modifier le port de connexion SSH il faut suivre les étapes suivantes

Ouvrir le fichier de configuration SSH

nano /etc/ssh/sshd_config

Modifier la ligne

Port 22

Pour :

Port XXXX

Sauvegarder le fichier avec ***Ctrl + O***

Ensuite se connecter en SSH sans avoir à renseigner de mot de passe

Pour pouvoir nous connecter sans mot de passe nous allons devoir générer une clé

ssh-keygen -t rsa

Il faut ensuite copier la clé publique, il existe plusieurs manières de procéder

Méthode 1 : Utilisation de la commande ssh-copy-id

La syntaxe de base pour utiliser cette commande est la suivante :

ssh-copy-id utilisateur_distant@adresse_IP_distante

Méthode 2 : Copier la clé privée en utilisant SSH

La méthode suivante utilise SSH pour copier la clé privée. Cette méthode peut être utilisée lorsque vous avez un accès SSH au serveur basé sur un mot de passe. La commande ci-dessous s'occupe de la procédure. Il vous suffit d'entrer le nom d'utilisateur de l'utilisateur distant et l'adresse IP de la machine.

cat ~/.ssh/id_rsa.pub | ssh utilisateur_distant@adresse_IP_distante "mkdir -p ~/.ssh && cat >> ~/.ssh/authorized_keys"

Méthode 3 : Copier manuellement la clé publique

La troisième méthode est un peu plus difficile car elle est entièrement manuelle. Cependant, dans certains cas où les autres méthodes ne fonctionnent pas, vous pouvez utiliser celle-ci ! Vous devrez ajouter manuellement le contenu du fichier id_rsa.pub au fichier

~/.ssh/authorized_keys du serveur distant

Sur la machine source, vous pouvez afficher le contenu du fichier id_rsa.pub en utilisant l'éditeur vi ou la commande cat :

cat ~/.ssh/id_rsa.pub

Une fois la clé copiée il faudra la coller sur le serveur distant (si nous souhaitons nous connecter à une VM sans mot de passe dans ce cas)

mkdir -p ~/.ssh

Vous pouvez de la même manière créer le fichier authorized_keys. Ajoutez la clé publique SSH copiée au fichier vide comme indiqué ci-dessous :

echo SSH_public_key >> ~/.ssh/authorized_keys

SSH_public_key est la clé publique que vous avez copiée de la machine source. Elle commencera par ssh-rsa

Une fois la clé copiée, vous pouvez fournir les autorisations requises au répertoire .ssh des serveurs distants en utilisant la commande chmod

chmod -766 ~/.ssh

On peut ensuite tester pour voir si la connexion est possible sans mot de passe

ssh utilisateur_distant@adresse_IP_distante

Uploader un fichier avec SSH (de votre pc ou VM vers le pc ou VM d'un camarade)

Envoi d'un fichier via SSH en utilisant SCP

scp /home/usersurlequeljesuis/data/Ficher2 root@192.168.10.131:/var/www/

Dans ce cas on utilise “Secure Copy (scp)” pour envoyer un fichier vers un autre PC, une VM ou un serveur. Il faut bien entendu modifier l’adresse IP et le répertoire en fonction de la machine principale et de la machine ciblée.

Télécharger un fichier avec SSH (de votre pc ou VM vers le pc ou VM d’un camarade)

Téléchargement d'un fichier via SSH en utilisant SCP

scp root@192.168.10.131:/var/www/Fichier2 /home/usersurlequeljesuis/data/

Dans ce cas on utilise Secure Copy pour télécharger un fichier qui se situe sur un PC, une VM ou un serveur. Ici on indique d’abord l’emplacement du fichier que l’on souhaite téléchargé suivi de l’emplacement ou l’on souhaite enregistrer le fichier

Limiter l’utilisation de SSH à un groupe particulier nommé “Plateforme_ssh”

Afin de limiter l’utilisation de SSH à un seul groupe il faut éditer le fichier SSH avec nano par exemple

nano /etc/ssh/sshd_config

On va ensuite ajouter une ligne à la fin de ce document qui modifiera l’accès de SSH

AllowGroups nomdugroupe <login>

Une fois cette ligne ajoutée uniquement le groupe en question aura accès à SSH

Bien entendu, il faudra avoir créé le groupe au préalable sur Linux

Dans notre cas nous utiliserons

AllowGroups Plateforme_ssh <login>

Nous pouvons également limiter l’utilisation à des utilisateurs plutôt que des groupes avec la commande

AllowUsers User1 User2 User3 <login>

Bonus suite

Quel est l’intérêt d’utiliser SSH ?

SSH permet d’accéder et d’effectuer des modifications à un PC ou une machine virtuelle tout en étant à distance. Elle permet par exemple de créer des fichiers, uploader ou télécharger des fichiers.

L’intérêt principal de SSH reste l'utilisation de cryptage pour assurer un transfert d'informations sécurisé entre le client et le serveur.

Est-ce que les clés générées par SSH par défaut sont assez sécurisées ? Justifier votre réponse

Les clés générées par SSH sont sécurisées par défaut pour 2 raisons. La principale étant que ce sont des clés volumineuses qui restent difficiles à contourner.

La deuxième raison est que les clés SSH sont divisées en 2 parties. Une première clé privée qui est générée en local et qui reste stockée en local sur notre machine et une deuxième clé publique, aussi générée en local, qui est communiquée aux serveurs. C’est donc cet aspect "pair" qui permet une bonne sécurisation de notre / nos systèmes.

Citez d’autres protocoles de transfert ? Quelles sont les différences entre ses protocoles ?

FTP

Premier protocole de transfert de fichiers, FTP est une méthode populaire de transfert de fichiers mise en place depuis des décennies. FTP échange les données via deux canaux séparés : le canal de commande (qui authentifie l’utilisateur) et le canal de données (qui transfère les fichiers).

Aucun des deux canaux FTP n’étant crypté, les données transmises via ces canaux peuvent être détournées. L’accès FTP nécessite toutefois un nom d’utilisateur et un mot de passe.

FTPS

FTPS est un protocole FTP via SSL/TLS (Secure Sockets Layer/Transport Layer Security). Ce protocole de transfert de fichiers sécurisé vous permet de transférer des fichiers en toute sécurité avec vos partenaires commerciaux, clients et utilisateurs. Les transferts peuvent être authentifiés par le biais de méthodes prises en charge via FTPS, comme des certificats clients, des certificats serveurs et des mots de passe.

SFTP

SFTP est un protocole FTP sécurisé par SSH (Secure Shell). Il constitue une alternative intéressante aux outils FTP non sécurisés et aux scripts manuels. Le SFTP échange les données via une connexion SSH et fournit aux organisations une protection élevée des transferts de fichiers entre leurs systèmes, partenaires commerciaux et employés, ou encore dans le cloud.

SCP (que nous avons vu précédemment)

SCP (Secure Copy Protocol) est un ancien protocole réseau qui prend en charge les transferts de fichiers entre plusieurs hôtes sur un réseau. Assez proche de FTP, SCP prend cependant en charge des fonctions de cryptage et d'authentification.

HTTP et HTTPS

Épine dorsale du WWW (World Wide Web), le protocole HTTP (Hyper Text Transfer Protocol) constitue la base même de la communication de données. Il définit le format des messages via lesquels les navigateurs et les serveurs Web communiquent, et définit la façon dont un navigateur Web doit répondre à une requête Web. HTTP est un protocole sans état qui utilise TCP (Transmission Control Protocol) comme couche de transport. En d'autres termes, chaque commande est exécutée de façon indépendante et aucune information de session n'est conservée par le destinataire.

Il existe encore d'autres protocoles mais nous n'allons pas tous les citer.

Différences entre certains protocoles

Prenons par exemple SFTP et FTPS. SFTP a besoin d'un seul port pour toutes les communications SFTP, ce qui permet de le protéger facilement. FTPS utilise plusieurs ports, ce qui représente une différence essentielle avec SFTP. Le premier port pour le canal de commande est utilisé pour l'authentification et la transmission des commandes. Cependant, chaque fois qu'une demande de transfert de fichiers ou une demande de liste des répertoires est effectuée, un autre port doit être ouvert pour le canal de données.

En ce qui concerne SCP et SFTP, SFTP est un protocole plus robuste et fournit des fonctionnalités de gestion de fichiers telles que la liste des répertoires, le renommage des fichiers, la suppression de fichiers, etc. En cas de problèmes de connectivité, SFTP prend en charge la reprise du transfert. De plus, SFTP dispose de contrôles d'intégrité au niveau des paquets, qui offrent plus de fiabilité, mais peuvent ralentir les transferts de fichiers. SCP est un algorithme de transfert plus simplifié et plus efficace, ce qui le rend plus rapide que SFTP, en particulier sur les réseaux à latence élevée. Cependant, SCP ne permet pas de répertorier les répertoires, de renommer les fichiers ou d'autres fonctionnalités de gestion de fichiers. Il ne reprend pas non plus les transferts en cas de problèmes de connectivité.