JOB 1

Afficher le manuel de commandes ls
man ls, ls –help

Afficher les fichiers cachés du home
ls -a

Liste de tous les fichiers, y compris les fichiers cachés, avec plein de caractéristiques ; les droits, la date, etc
ls -lisa

Comment ajouter des options à une commande ?
Pour ajouter une option à une commune il suffit juste de mettre un tiret - devant la commande
Quelles sont les deux syntaxes principales d'écriture des options pour une commande ?
Les deux syntases principales d'écritures sont un tiret (-) ou deux (--)

JOB 2

Lire seulement un fichier = readonly (nom du fichier)
- afficher les 10 premières lignes du fichier ".bashrc" = head .bashrc
- afficher les 10 dernières lignes du fichier ".bashrc" = tail .bashrc
- afficher les 20 premières lignes du fichier ".bashrc" = head -20 .bashrc
- afficher les 20 dernières lignes du fichier ".bashrc" = tail -20 .bashrc

JOB 3

Pour installer le paquet cmatrix = sudo apt-get install cmatrix
Mettre à jour son gestionnaire de paquets = apt (full-)upgrade
Mettre à jour ses différents logiciels = sudo apt-get update
Télécharger les internets : wget (mettre le lien google chrome)

JOB 4

J'ai pu trouver deux moyens de faire ça

Le premier moyen :
Créer un fichier qui contient user1 et user2 = nano users.txt
Créer un groupe = groupadd Plateformeurs
Créer deux utilisateurs = adduser user1 adduser user2
Ajouter user2 dans le groupe = sudo adduser user2 Plateformeurs
Copier votre users.txt dans un fichier droits.txt = touch droits.txt cp users.txt droits.txt
Copier votre "users.txt" dans un fichier "groupes.txt" = touch groupes.txt cp users.txt groupes.txt

Changer le propriétaire du fichier “droits.txt” pour mettre “User1”= chown user1 droits.txt
Changer les droits du fichier “droits.txt” pour que “User2” ai accès seulement en lecture = chmod ou+rx droits.txt
Changer les droits du fichier “groupes.txt” pour que les utilisateurs puissent accéder au fichier en lecture uniquement = chmod au+rx groupes.txt
Changer les droits du fichier pour que le groupe “Plateformeurs” puissent y accéder en lecture/écriture = chmod

Et le deuxième moyen :
Créer un fichier = nano (nom du fichier).txt
Créer un groupe = groupadd (nom du groupe)
Créer un utilisateur dans le groupe = gpasswd -a User2 PLATEFORMEURS
Ajouter quelqu’un au groupe = sudo adduser nom_utilisateur nom_groupe
Copier votre “users.txt” dans un fichier “droits.txt” = cp /home/alyssa/documents/
Copier votre “users.txt” dans un fichier “groupes.txt” = /
Changer le propriétaire du fichier “droits.txt” pour mettre “User1”= chown user1 droits.txt
Changer les droits du fichier “droits.txt” pour que “User2” ai accès seulement en lecture = chmod o+r (nom du fichier)
Changer les droits du fichier “groupes.txt” pour que les utilisateurs puissent accéder au fichier en lecture uniquement = chmod o+r groupes.txt
Changer les droits du fichier pour que le groupe “Plateformeurs” puissent y accéder en lecture/écriture = chmod g+wr groupes.txt

JOB 5

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

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
export User=’al’
pour le supprimer unset User

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

Afficher les variables d’environnement
printenv

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

- cd
- PATH=' /home/alyssa/Bureau'

JOB 6

Vous devez télécharger l'archive suivante et la désarchiver seulement avec le terminal. Cette manipulation vous permettra d'accéder à la suite du sujet.

wget https://drive.google.com/file/d/1s9ZhRhjo0FXcBNRB5khAGK1jVxkZj6Uk/view?usp=sharing.tar.gz
Pour la décompresser = tar -xzvf Ghost-in-the-Shell.tar.gz
ou alors,

- tar -xf Ghost\in\the\shell.tar.gz
- ls

JOB 7

Pour réunir toutes les commandes en haut on va utiliser le fameux ">" ce qui va donner :
echo je suis votre fichier texte > une_commande.txt ; wc -l /etc/apt/sources.list > nb_lignes.txt > cat /etc/apt/sources.list > save_sources

JOB 8

sudo apt-get install tree && tree& / > tree.save.txt ; tree -a && wc -l tree.save.txt && upgrade

BONUS

Installer SSH = apt-get install ssh, apt-get install openssh-server
Générer une clé SSH = ssh-keygen -t rsa (on fait ensuite "entrée" sans rien marquer)

Se connecter à une VM ou l'ordinateur d'un camarade via SSH
ssh <nom_utilisateur>@<ipaddress>

Configurer SSH pour empêcher le login root (root ne peut pas se connecter en SSH)
nano /etc/ssh/sshd_config et ensuite sur la ligne PermitRootLogin et écrire no et ensuite redémarrer = service ssh restart

Modifier le port de connexion de SSH (autre que 22)
La même manip à faire que pour le permitrootlogin mais avec la ligne "port 22" qu'on devra remplacer par un nombre entre 1024 et 65536

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

Uploader un fichier avec SSH (de votre pc ou VM vers le pc ou VM d'un camarade)
scp /users/dondada/desktop/root@alyssa:/home/alyssa/bureau/test.txt

Télécharger un fichier avec SSH (de votre pc ou VM vers le pc ou VM d'un camarade)
scp root@alyssa:/home/alyssa/bureau/exemples.txt users/dondada/desktop

Limiter l'utilisation de SSH à un groupe particulier nommé "Plateforme_ssh" ___
nano etc/ssh/ssh_config et ensuite à la ligne allowgroups plateforme_ssh

Quel est l'intérêt d'utiliser SSH ?
SSH (Secure Socket Shell) est un protocole réseau qui permet aux administrateurs d'accéder à distance à un ordinateur, en toute sécurité.

Est-ce que les clés générées par SSH par défaut sont assez sécurisées ?
Comme son nom l'indique, Secure Shell, le protocole de connexion impose un échange de clé de chiffrement en début de connexion. Les clés privées générées par le SSH seront donc chiffrées. C'est-à-dire ? Le message sera chiffré, mélangé, incompréhensible pour une personne qui intercepte en plein milieu, à part pour la personne qui reçoit ce message, elle ne peut pas le lire à moins donc de posséder la clé privée.

Citez d'autres protocoles de transfert ? Quelles sont les différences entre ses protocoles ?
FTP, FTPS, SFTP, HTTPS, SMB (mais très souvent victime d'attaques informatiques)…
Pour FTP, il y a les ports 21 et 20. Le port 20 permet de transférer des fichiers tandis que le 21 permet de contrôler le trafic et de pouvoir effectuer des requêtes pour télécharger des éléments sur le port 20
Tandis que par exemple pour HTTP celui-ci utilise uniquement le port 80, etc en fonction des protocoles de transfert…
Hormis la différence du port, il y aussi celle de l'url, pour la nature de leur utilité c'est à dire HTTP est utilisé pour les sites web tandis que FTP pour transférer un fichier d'un hôte à l'autre.