ISTY - Université de Versailles – St Quentin en Yvelines
IATIC5
Module " Administration Système Unix / Linux "

Franck TALBART

Examen : module " Administration Système Unix / Linux " IATIC5 2015/2016

(Date : vendredi 13 novembre 2015 – Durée : 3h00 – Seul le support de cours est autorisé)

Lisez attentivement et en entier les énoncés des exercices avant de les commencer, afin de bien assimiler ce qui est attendu. Faites les exercices dans l'ordre et laissez de l'espace si besoin. Justifiez TOUTES les réponses tout en vous limitant à ce qui est pertinent (une recopie du cours sur un sujet donné ne constitue pas une réponse). Les réponses non justifiées ne rapportent pas de point.

Partie I : Sauvegardes (5 points)

On dispose d'un serveur comprenant plusieurs systèmes de fichiers :

- systèmes de fichiers occupés par le système (`/`, `/usr`, `/var`, etc) occupant 4 Go ;
- un système de fichiers de 50 Go contenant les données des utilisateurs (dont environ 5% est modifié chaque jour).

On dispose de 10 cartouches de sauvegarde d'une capacité de 10 Go chacune, et on souhaite mettre en place un système de sauvegardes.

Question 1 – *4 point(s)*

En prenant en compte les questions de redondance de sauvegardes, de facilité de sauvegarde, de facilité de restauration, proposer une politique de sauvegarde en détaillant :

- les informations à sauvegarder ;
- la fréquence de sauvegarde des diverses informations ;
- la méthode de sauvegarde (complète, incrémentale) liée aux différentes informations.

Justifier les choix effectués.
Décrire les outils utilisés et leurs paramétrages.
Si des opérations sont automatisables, décrire l'outil utilisé et sa mise en œuvre.

Question 2 – *1 point(s)*

Votre datacenter est en Californie, un Etat subissant des tremblements de terre, inondations, et incendies simultanément. Comment se prémunir des risques de perte de données dans ce contexte ? Décrire une solution automatisée et donner les inconvénients s'il y en a.

Partie II : Problème (2 points)

Un administrateur système maladroit efface le programme `/bin/bash` avant d'éteindre une machine Linux.

Question 3 – *2 point(s)*

- Lorsqu'on tentera de rallumer la machine, que va-t-il se passer ?
- Comment corriger cette erreur ? Détailler la solution.

Partie III : Utilisateurs (2 points)

L'administrateur ouvre le fichier /etc/passwd:

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/bash
bin:x:2:2:bin:/bin:/bin/bash
sys:x:3:3:sys:/dev:/bin/bash
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/bash
man:x:6:12:man:/var/cache/man:/bin/bash
igor:x:0:0::/home/igor:/bin/sh
mysql:x:116:124:MySQL Server,,,:/nonexistent:/bin/false
franck:x:15:15:franck:/home/franck:/bin/bash
bob:x:16:16:eponge:/home/bob:/bin/bash
```

Question 4 – *0.5 point(s)* A quoi sert l'utilisateur dont l'uid est 116 ? Justifier son existence.

Question 5 – *0.5 point(s)* Comment empêcher Bob de se connecter ?

Question 6 – *1 point(s)* L'administrateur s'aperçoit qu'une intrusion a eu lieu sur son système. Retrouver l'indice qui permet d'en venir à cette conclusion.

Partie IV : Mise en place de l'infrastructure réseau (6 points)

Vous êtes responsable d'un réseau d'adresse 132.45.0.0/16 et souhaitez mettre en place des sous-réseaux.

Question 7 – *2 point(s)* Découper en 8 sous-réseaux le réseau. Indiquer la plage d'adresse attribuable pour les deux premiers sous-réseaux, puis proposer deux adresses IP pour les machines **A** et **B**, connectées respectivement sur les premier et deuxième sous-réseaux.

Question 8 – *0.5 point(s)* Indiquer la commande à invoquer sur la machine **A** afin de lui attribuer statiquement l'adresse IP de la réponse à la première question.

Question 9 – *1 point(s)* Quelle commande utilise t-on pour afficher la table de routage ? Indiquer les tables de routage nécessaires à la communication de **A** et de **B**.

Question 10 – *0.5 point(s)* Comment vérifier le bon fonctionnement du routage ?

Question 11 – *0.5 point(s)* Que signifie l'acronyme TTL ?

Question 12 – *0.5 point(s)* Décrire le processus de recherche dans la table.

Question 13 – *1 point(s)* Qu'est-ce qu'une attaque par dictionnaire ? En supposant que les machines **A** et **B** soient accessibles via le protocole SSH, donner deux solutions pour protéger votre réseau contre ce type d'attaque.

Partie V : Services (4 points)

Vous venez de rejoindre l'entreprise ISTY Corp. qui possédait une administration vieillissante, et vous a embauché pour la mise en place d'un nouveau système. Vous devrez remettre en place tous les services informatiques pour répondre aux besoins suivants :

1. Les 13 employés doivent disposer de stations de travail autonomes et pouvoir accéder à leurs documents depuis n'importe quelle station.
2. On souhaite disposer d'un système d'authentification centralisé pour faciliter la création de comptes lors de l'arrivée de nouveaux employés.
3. L'entreprise aura besoin d'un d'un webmail et service de publication d'informations sur l'entreprise, tous deux accessibles depuis internet.
4. Les employés doivent pouvoir disposer d'un moyen sécurisé pour accéder ponctuellement à leurs fichiers à distance.
5. On souhaite mettre en place un DHCP qui affecte les adrese IP aléatoirement entre 128.93.62.2 et 128.93.62.224, que le broadcast soit en 128.93.62.225 et qu'en cas de panne il redirige ses requête ailleurs.
6. La résolution des noms d'hôtes est également nécessaire.

Question 14 – *4 point(s)* Proposer une organisation adéquate des machines (en schématisant) et décrire les différents services (nommer les logiciels employés) à mettre en place ainsi que leur localisation sur le réseau. Sans entrer dans les détails de leur configuration, mentionner les liens qui existent entre ces services et les aspects de sécurité associés.

Partie VI : Question pour un champion (1 point)

On exécute les instructions suivantes:

```
ftalbart@alkan:~$ mkdir mon_rep
ftalbart@alkan:~$ > mon_rep/a
ftalbart@alkan:~$ > mon_rep/b
ftalbart@alkan:~$ ln -s mon_rep/a a
ftalbart@alkan:~$ ln mon_rep/b b
ftalbart@alkan:~$ chmod a+rw-x *
```

Question 15 – *1 point(s)* Qu'affiche la commande "cat a b" ? Justifier.