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

Franck TALBART, Vincent PALOMARES (Californie)

Examen : module " Administration Système Unix / Linux " IATIC5 2016/2017

(Date : mardi 3 janvier 2017 – Durée : 1h30 – 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 : Infrastructure réseau (8 points)

La Picardie du Nord a récemment fait sécession sous l'égide d'un nouveau gouvernement autoritaire. Son dictateur organise un système de censure dans son QG. Les contraintes sont les suivantes:

- Comme internet est une source désapprouvée d'information, les sites suivants ne doivent pas être accessibles par le personnel: cannele.fr, isty.uvsq.fr, zombo.com.
- Les PCs du dictateur et de ses conseillers ne doivent pas être censurés.

Question 1 – *1 point(s)* Le dictateur vous nomme chef du service IT. Comment faites-vous pour mettre en place ces contraintes? (Proposez 2 solutions en utilisant des outils vus en cours, ainsi que leurs avantages et inconvénients respectifs.)

Question 2 – *1 point(s)* Vous commencez à avoir des remords, et les rebelles picardiens vous approchent avec un gros chèque. Cela vous convainc de changer de bord, et d'aider les rebelles à contourner le système de censure que vous avez créé. Quelles techniques proposez-vous ?

Question 3 – *2 point(s)* Vous devez maintenant mettre en place le réseau des rebelles. Son adresse IP est le 132.45.0.0/16. Découpez ce réseau en 8 sous-réseaux. Indiquez la plage d'adresses des deux premiers sous-réseaux.

Question 4 – *0.5 point(s)* Quelle est l'adresse de diffusion du sous-réseau n°3 ?

Question 5 – *0.5 point(s)* Explicitez brièvement la raison d'être d'un serveur DHCP et d'un serveur DNS.

Question 6 – *0.5 point(s)* Les services DHCP et DNS du réseau allié ont été mis hors de service par une attaque informatique. Vous suspectez le gouvernement, mais comment pouvez-vous le vérifier ?

Question 7 – *1 point(s)* Comment vous connectez-vous au réseau sans ces services ? Donnez les fichiers de configuration si besoin, et / ou les commandes.

Question 8 – *0.5 point(s)* Il s'agit d'une attaque de type brute force. Comment vous protégez-vous de cette attaque ?

Question 9 – *1 point(s)* Peut-on faire cohabiter plusieurs serveurs DHCP sur un même réseau ? Si oui, donnez les fichiers de configurations, si non, expliquez la raison. Quel en serait l'intérêt ?

Partie II : Services (4.5 points)

Le réseau allié doit se développer et répondre aux besoins suivant:

- Les membres doivent pouvoir s'échanger des documents depuis n'importe quelle station.
- Un webmail doit être accessible et les accès doivent être chiffrés.
- Un système d'authentification centralisé est nécessaire.
- Les horloges des PCs doivent être synchronisées pour coordonner d'éventuelles attaques.

Question 10 – *2 point(s)* Proposez une organisation adéquate des machines en schématisant et décrivez les différents services (nommez-les). Mentionnez les liens qui existent entre ces services et les aspects sécuritaires nécessaires compte tenu du contexte.

Question 11 – *1 point(s)* Le service web qui héberge le webmail doit être exécuté automatiquement lors du démarrage du serveur. Expliquez les étapes nécessaires.

Question 12 – *1 point(s)* Pourquoi est-ce une mauvaise idée de se connecter en root via SSH en mode 'mot de passe'? Comment l'interdire ?

Question 13 – *0.5 point(s)* Quel est l'intérêt de sudo ?

Partie III : Sauvegardes (5 points)

Un système de sauvegarde doit être mise en place compte tenu des contraintes suivantes:

- Les sauvegardes doivent se faire très rapidement
- Elles doivent être distribuées afin de réduire les risques de perte en cas d'attaque (les données circulant devant évidemment être chiffrées)

Question 14 – *1 point(s)* Citez quelques systèmes de fichiers adaptés pour des exigences critiques et donnez les différences.

Question 15 – *1 point(s)* Quels sont les composants que vous devez installer sur le système pour gérer ce nouveau type de système de fichiers ?

Question 16 – *2 point(s)* Quelles politiques adopteriez-vous (scripts shells, fréquence, ...) pour mettre en place la sauvegarde distribuée ? Donnez le fichier de configuration de l'utilitaire cron correspondant.

Question 17 – *1 point(s)* Pourquoi a-t-on /bin ET /usr/bin ? Quel en est l'intérêt ?

Partie IV : Utilisateurs (1.5 points)

Le gouvernement a saisi le serveur d'authentification centralisé, et vous décidez d'utiliser le système classique de gestion d'utilisateurs.

Question 18 – *1 point(s)* Vous souhaitez obtenir la liste des comptes utilisateurs inactifs sur le serveur web depuis 2 semaines pour les désactiver. Comment procéder ? Comment désactiver ces comptes ?

Question 19 – *0.5 point(s)* Comment forcer les utilisateurs à changer de mot de passe toutes les 2 semaines ?

Partie V : Question pour un champion (1 point)

On exécute les instructions suivantes:

```
hackeur@picardie ~ $ echo "Bob l'éponge" | sudo tee  /root/titi
Bob l'éponge
hackeur@picardie ~ $ sudo ls /root/ti*
ls: impossible d'accéder à /root/ti*: Aucun fichier ou dossier de ce type
```

Question 20 – *1 point(s)* Pourquoi la dernière commande ne fonctionne-t-elle pas ? Proposez une solution.