Sujet IE Chef de projet Sécurité et administration (concours MI2)

Première Partie

Exercice 1. Système d'exploitation (notation sur 2 points)

- Quelles sont les différences entre un processus et un *thread* ?

- Quels sont les avantages et difficultés de développement et d'utilisation d'un programme *multi-thread* ?

Exercice 2. Serveur de *log* (notation sur 2 points)

Pouvez-vous citer les opérations et obligations légales à effectuer pour centraliser les *logs* de machines *linux* et *windows* sur un serveur de *log* ?
Quels sont les mécanismes permettant de le faire dans les environnements *linux* et *windows* ?
Connaissez-vous une solution pour regrouper les *logs* aussi bien des postes *windows* que ceux des postes *linux* sur un serveur de *logs* unique?

Exercice 3. Performances (answer in english) (notation sur 2 points)

A research team uses *unix* computers. Members complain about poor performance of their workstations.

- What unix commands will you use to diagnose this problem?
- How do you monitor a *unix* system over several days?

Deuxième Partie

Étude de cas 1. Serveur web (notation totale sur 7 points)

Dans une équipe de recherche, plusieurs personnes souhaitent contribuer à la mise à jour d'un site web. Un stagiaire installe dans le laboratoire une machine désignée comme serveur, car l'équipe souhaite rester autonome. Ce serveur fonctionne sous linux. Après quelques semaines, une douzaine de personnes se connectent régulièrement (1 à 3 fois par semaine), éventuellement depuis leur domicile ou en déplacement. Elles partagent toutes le même compte pour l'accès (identifiant et mot de passe). Elles utilisent des postes sous *windows*, *linux* ou *macosx*.
Trois mois plus tard, cette machine est compromise. Il est impossible de cerner depuis quelle adresse IP la machine a été compromise. Le directeur de l'équipe vous sollicite.

Question P1 (notation sur 1 point)
Quelles actions réalisez-vous immédiatement ?

Question P2 (notation sur 2 point)
Vous transmettez à votre responsable un compte-rendu de l'incident et le traitement proposé. Donner les éléments principaux de ce compte-rendu.

Question P3 (notation sur 2 point)
Comment limiter les intrusions et conserver une trace utile des accès ?

Question 4 (notation sur 2 points)
À quoi sert une Politique de Sécurité des Systèmes d'Information (PSSI) ?

Étude de cas 2. Projet Migration de parc (notation totale sur 7 points)

Le responsable d'une équipe de recherche informe le 1er juin qu'il souhaite confier au service informatique le renouvellement de son parc de PC portables. Votre responsable vous demande d'organiser et piloter ce projet.

- Le nouveau matériel est composé de 10 portables identiques. Il sera acheté sur le budget de l'équipe projet. Le fournisseur vous informe qu'il peut vous livrer à partir du 15 juin. Par ailleurs, vous disposez d'une machine similaire en réserve.
- Le système d'exploitation utilisé auparavant est *windows xp*. Dans une démarche nationale, une migration vers *windows vista* est souhaitée.
- Les chercheurs échangent entre eux des fichiers créés sous *open-office* et *latex*.
- Le service informatique propose des images disque *windows xp* et *windows vista* pour ces machines mises à jour en avril. Le constructeur des portables a publié de nouveaux pilotes le 15 mai.
- Les chercheurs ne seront pas tous présents au même moment. Ils passent au moins 2 fois par mois dans le centre.
- Toutes les machines doivent être renouvelées avant le 1er septembre.
- Un technicien des services généraux est disponible 2 jours par semaine pour installer les machines et voir les chercheurs. Il sera en congés du lundi 13 juillet au vendredi 31 juillet. Vous-même êtes en congés du lundi 20 juillet au 7 août.

Question 1 (notation sur 2 points)
Identifiez la liste des travaux à réaliser.

Question 2 (notation sur 2 points)
Proposez un planning et une organisation de ce projet.

Question 3 (notation sur 2 points)
Quel accompagnement proposez-vous pour les utilisateurs ?

Question 4 (notation sur 1 point)
Les agendas ne permettent pas la tenue de points d'avancement entre le 15 juin et le 15 août.
Quel compte-rendu proposez-vous au directeur du projet et à votre responsable ?