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

Franck TALBART, Vincent PALOMARES (Californie)

Examen : module " Administration Système Unix / Linux " IATIC5 2017/2018

(Date : mardi 19 décembre 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 : Sécurité (3 points)

Vous êtes Johnson, un agent de la Picardie du Sud infiltré en tant qu'expert technique dans le réseau ultra sécurisé du nouveau gouvernement autoritaire de la Picardie du Nord. Votre rôle est de récolter certaines informations critiques et les envoyer à votre organisation sans être soupçonné.

Question 1 – *1 point(s)* Vous souhaitez éviter que vos données soient interceptées. Comment se nomme ce type d'attaque ? Expliquez son principe. Comment s'en prémunir ?

Question 2 – *1 point(s)* Comment procéderiez-vous pour mettre en place rapidement une solution permettant de chiffrer TOUTES les données (emails, chats, ...) envoyées vers picardie-leaks.com ?

Question 3 – *1 point(s)* Bien que les données soient chiffrées et en petites quantités (ce qui n'est pas anormal en soi), l'administrateur a quand même pu détecter une activité suspecte en regardant les logs des services réseau. Quel est le service qui l'a mis sur la piste ? (ce n'est pas du monitoring)

Partie II : Démarrage (6.5 points)

Vous êtes Bob, agent loyaliste du régime Nord-Picardien. Votre collègue, l'agent Johnson, est soupçonné d'être une taupe à la solde de la Picardie du Sud. Plutôt que de l'arrêter, vous décidez de profiter de cette situation : Jonhson ne sait pas que des soupçons pèsent sur lui. Vous souhaitez intercepter ses communications à son insu.

Johnson étant en charge de la surveillance de la salle des serveurs, il serait difficile d'obtenir un accès (physique ou distant) aux machines sans lui mettre la puce à l'oreille. En revanche, vous pouvez aisément accéder à son bureau, et vous décidez de trafiquer son poste.

Le but est de modifier les logiciels de communications tel que le client mail. Ces modifications doivent être complètement invisibles pour Johnson. Le système d'exploitation (GNU/Linux) est installé localement sur toutes les machines du réseau.

Question 4 – *1 point(s)* Vous voulez effectuer une sauvegarde de la machine avant toute tentative de modification de manière à restaurer le disque en cas de mauvaise manipulation. Quel environnement vous permettrait de le faire en O(1) ? Outre la rapidité, quel est l'avantage d'un tel procédé par rapport à la création complète d'une archive ?

Question 5 – *0.5 point(s)* Vous souhaitez envoyer une copie du système sur un serveur NFS et faire démarrer la machine directement dessus, l'intérêt étant de maintenir un contrôle total (et distant) du système sur le long terme (il existe bien sûr de meilleures stratégies ;)). Expliquez les principes du NFS.

Question 6 – *1.5 point(s)* Comment procéderiez-vous pour partager un système d'exploitation complet sur le NFS ? Donnez les grands points, et écrivez le fichier /etc/export correspondant. Quel est l'inconvénient principal d'une telle architecture ?

Question 7 – *0.5 point(s)* Vous souhaitez modifier la procédure de démarrage de sa machine pour maintenant exécuter le système d'exploitation depuis le NFS. Expliquez les grandes étapes du démarrage du système GNU/Linux.

Question 8 – *1 point(s)* Qu'est ce qu'un initramfs ? Quel en est l'avantage par rapport à la compilation en dur dans le noyau ?

Question 9 – *1 point(s)* Donnez la commande complète permettant de changer la racine du système de fichier, et ainsi prétendre avoir booté sur l'OS distant du NFS sur la machine locale. On suppose que le point de montage NFS est déjà présent dans /tmp/os.

Question 10 – *1 point(s)* A ce stade, le processus init prend la main. Quel est son rôle ? Quel devrait être son PID ? Pourquoi cette contrainte n'est-elle pas respectée dans le cas présent ?

Partie III : Réseau (9.5 points)

Johnson est finalement arrêté pour haute trahison et l'administrateur réseau réalise qu'il aurait pu éviter certaines fuites de données en isolant les services critiques. Il souhaite mettre en place un sous-réseau réservé aux agents, et un second sous-réseau pour les services. La connexion entre ces deux réseaux sera contrôlée via un pare-feu / proxy.

Question 11 – *1 point(s)*

On veut découper le réseau 193.74.30.0 en 2 sous-réseaux. Quelle est la valeur du masque de sous-réseau ?

Question 12 – *2 point(s)* Pour chaque sous-réseau, indiquez :

- l'adresse de sous-réseau
- l'adresse de broadcast

Question 13 – *0.5 point(s)* Quel service peut-il utiliser pour distribuer les adresses IP ?

Question 14 – *2 point(s)* Le sous-réseau dédié aux agents doit disposer d'un système d'authentification centralisé pour faciliter la création de compte lors de l'arrivée de nouveaux employés. Les employés doivent pouvoir disposer d'un moyen sécurisé pour accéder ponctuellement à leurs fichiers à distance. Décrivez les différents services (nommez les logiciels employés) à mettre en place ainsi que leur localisation sur le réseau.

Question 15 – *2 point(s)* Comment peut-on protéger le réseau des attaques extérieures ? Citez au moins 3 types d'attaques et les solutions respectives.

Question 16 – *2 point(s)* Un système de sauvegarde distribué doit être mis en place afin de réduire les risques de perte en cas d'attaque (les données circulant devant évidemment être chiffrées). Quelles politiques adopteriez-vous (scripts shells, fréquence, ...) pour mettre en place la sauvegarde distribuée ? Donnez le fichier de configuration de l'utilitaire cron correspondant.

Partie IV : Question pour un champion (1 point)

On exécute les instructions suivantes :

```
  hacker-picardie /tmp $ cat bob.sh
MA_VAR="éponge"
echo $MA_VAR
  hacker-picardie /tmp $ ./bob.sh
éponge
  hacker-picardie /tmp $ echo $MA_VAR

  hacker-picardie /tmp
(rien ne s'affiche)
```

Question 17 – *1 point(s)* Pourquoi la dernière commande n'affiche t-elle rien ? Proposez une solution.