CONCOURS EXTERNE D'INGENIEUR D'ETUDES
BAP E – Ingénieur système et réseau (MI-21)

Ouvert au titre de 2008
Arrêté du 1er avril 2008 paru au JO du 5 avril 2008
Epreuve écrite
Notation sur 20 - Coefficient 3 – Durée 3h00

17 juin 2008 de 9h30 à 12h30

Le candidat peut traiter les questions dans l'ordre de son choix.

Les copies seront corrigées anonymement. Veuillez donc respecter l'anonymat dans vos réponses et ne pas utiliser d'éléments permettant de vous identifier.

Une attention particulière sera portée à la qualité de la présentation, à l'orthographe et à la grammaire.

Connaissance du monde de la recherche

Exercice 1 (notation sur 1,5 point)

Quels sont actuellement les principaux évènements qui marquent le monde de la recherche ? Quels sont les enjeux pour les métiers de supports à la recherche, notamment pour les moyens informatiques ? (Votre réponse devra faire entre 10 et 20 lignes)

Réseau et système

Exercice 2 (notation sur 1,5 point)

A quoi correspond la norme 802.1Q ? Décrivez en quelques lignes une architecture qui s'appuie sur cette norme.

Exercice 3 (notation sur 2 points)

Expliquez brièvement la différence entre les protocoles de routages OSPF et BGP. Dans quel(s) cas privilégiez-vous l'un par rapport à l'autre ?

Exercice 4 (notation sur 1,5 point)

Que permet la technologie *zeroconf* ? Citez un protocole utilisé par l'une des mises en oeuvre de zeroconf.

Exercice 5 (notation sur 2 points)

L'URL d'un (et d'un seul) site web institutionnel français n'est pas accessible depuis les machines situées dans le VLAN des personnels administratifs de votre réseau. Le site est par contre accessible par son adresse IP. Quels tests allez-vous entreprendre pour déterminer l'origine du problème ?

Sécurité et connaissance de la langue anglaise

Exercice 6 (notation sur 2,5 points)

Vous gérez un site comprenant des postes utilisateurs, fixes et nomades, sous diverses distributions Linux (Fedora, Debian, Ubuntu).
L'accès à votre site se fait à travers une passerelle SSH tournant sous la distribution RedHat.
Vous venez de recevoir un bulletin de sécurité émis par l'éditeur Ubuntu (cf Annexe).

6.1) Décrivez, en **français**, le problème ainsi que le risque encouru.

6.2) Quelles mesures allez vous prendre, en tant que responsable sécurité de votre site, pour pallier à cette vulnérabilité (répondez en **français**) ?

6.3) Rédigez, en **anglais** et en **français**, l'annonce que vous allez envoyer aux utilisateurs.

Problème **: Etude de cas** (notation totale sur 9 points)

Votre centre de recherche INRIA va aménager des locaux dans une université distante de 200 km du site principal, pour accueillir deux équipes de recherche (vingt personnes).
Les membres de ces équipes sont déjà présents sur place et sont hébergés dans d'autres locaux universitaires. Ils sont dotés de machines fixes ou portables, utilisant les systèmes d'exploitation Windows, MacOSX, Linux, et ces machines les accompagneront dans leurs nouveaux bureaux. Ces équipes utilisent pour l'instant les services de l'université pour se connecter au réseau et relever leur courrier.

A l'issue de la migration dans les locaux INRIA, les chercheurs souhaitent disposer des mêmes facilités que les chercheurs du site principal, soit :

- des accès réseaux filaires et Wi-Fi sécurisés pour eux mêmes et leurs invités,
- un service de messagerie électronique complet,
- la mise à disposition de sites web authentifiés de type CMS et WIKI,
- des espaces de stockage importants et des sauvegardes de leurs données.

Un local technique climatisé de 10 m2, relié au réseau de collecte régional via le réseau de l'université, est disponible dans les nouveaux locaux pour accueillir des éléments actifs. Les locaux sont déjà câblés en Ethernet 1000 Base-T, selon une topologie en étoile qui converge dans ce local.

Il n'y a pas de personnel technique sur place et en tant qu'ingénieur systèmes et réseaux de l'équipe des moyens informatiques INRIA, vous êtes en charge de préparer et de piloter ce projet.

Question P.1
Lister l'ensemble des services (d'infrastructure et applicatifs) auxquels devront avoir accès les chercheurs.

Question P.2
Proposez deux scénarios différents d'implantation, en comparant les avantages et inconvénients de chacun.

Question P.3
Détaillez plus particulièrement vos recommandations pour la sécurisation des accès filaires et Wi-Fi.

Question P.4
Quelle organisation technique allez-vous mettre en place pour gérer ce site ?

Question P.5
Comment allez-vous organiser la communication avec les utilisateurs de ce site ?

Question P.6
Décrivez votre plan de migration des vingt postes dans la nouvelle infrastructure.

Annexe : bulletin de sécurité SSH

```
==========================================================
Ubuntu Security Notice USN-612-2                May 13, 2008
openssh vulnerability
CVE-2008-0166, http://www.ubuntu.com/usn/usn-612-1
==========================================================

A weakness has been discovered in the random number generator used
by OpenSSL on Debian and Ubuntu systems.  As a result of this
weakness, certain encryption keys are much more common than they
should be, such that an attacker could guess the key through a
brute-force attack given minimal knowledge of the system.  This
particularly affects the use of encryption keys in OpenSSH.

This vulnerability only affects operating systems which (like
Ubuntu) are based on Debian.  However, other systems can be
indirectly affected if weak keys are imported into them.

We consider this an extremely serious vulnerability, and urge all
users to act immediately to secure their systems.

The following Ubuntu releases are affected:

Ubuntu 7.04
Ubuntu 7.10
Ubuntu 8.04 LTS

This advisory also applies to the corresponding versions of
Kubuntu, Edubuntu, and Xubuntu.


Updating your system:

1. Install the security updates

   Ubuntu 7.04:
     openssh-client                  1:4.3p2-8ubuntu1.3
     openssh-server                  1:4.3p2-8ubuntu1.3

   Ubuntu 7.10:
     openssh-client                  1:4.6p1-5ubuntu0.3
     openssh-server                  1:4.6p1-5ubuntu0.3

   Ubuntu 8.04 LTS:
     openssh-client                  1:4.7p1-8ubuntu1.1
     openssh-server                  1:4.7p1-8ubuntu1.1

   Once the update is applied, weak user keys will be automatically
   rejected where possible (though they cannot be detected in all
   cases). If you are using such keys for user authentication,
   they will immediately stop working and will need to be replaced
   (see step 3).

   OpenSSH host keys can be automatically regenerated when the
```

OpenSSH security update is applied. The update will prompt for confirmation before taking this step.

2. Update OpenSSH known_hosts files

   The regeneration of host keys will cause a warning to be displayed when connecting to the system using SSH until the host key is updated in the known_hosts file. The warning will look like this:

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle
attack)! It is also possible that the RSA host key has just been
changed.
```

   In this case, the host key has simply been changed, and you should update the relevant known_hosts file as indicated in the error message.

3. Check all OpenSSH user keys

   The safest course of action is to regenerate all OpenSSH user keys, except where it can be established to a high degree of certainty that the key was generated on an unaffected system.

   Check whether your key is affected by running the ssh-vulnkey tool, included in the security update. By default, ssh-vulnkey will check the standard location for user keys (~/.ssh/id_rsa, ~/.ssh/id_dsa and ~/.ssh/identity), your authorized_keys file (~/.ssh/authorized_keys and ~/.ssh/authorized_keys2), and the system's host keys (/etc/ssh/ssh_host_dsa_key and /etc/ssh/ssh_host_rsa_key).

   To check all your own keys, assuming they are in the standard locations (~/.ssh/id_rsa, ~/.ssh/id_dsa, or ~/.ssh/identity):

```
$ ssh-vulnkey
```

   To check all keys on your system:

```
$ sudo ssh-vulnkey -a
```

   To check a key in a non-standard location:

```
$ ssh-vulnkey /path/to/key
```

   If ssh-vulnkey says "COMPROMISED", the key is vulnerable and should be replaced.

   If ssh-vulnkey says "Unknown (no blacklist information)", then it has no information about whether that key is affected because the key is of a type for which no blacklist is available.

If in doubt, destroy the key and generate a new one.

4. Regenerate any affected user keys

   OpenSSH keys used for user authentication must be manually regenerated, including those which may have since been transferred to a different system after being generated.

   New keys can be generated using ssh-keygen, e.g.:

```
$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/user/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/user/.ssh/id_rsa.
Your public key has been saved in /home/user/.ssh/id_rsa.pub.
The key fingerprint is:
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00 user@host
```

5. Update authorized_keys files (if necessary)

   Once the user keys have been regenerated, the relevant public keys must be propagated to any authorized_keys files on remote systems. Be sure to delete the affected key.