contrôle - administration système
DUT-2 S4-sept 2010/2011

IUT Villetaneuse
dép. informatique

Les questions sont indépendantes (sauf si c'est indiqué autrement). Total de XXX points. Le contrôle dure 2 heures. Aucun document n'est autorisé.

Pour chaque commande, vous utiliserez « sudo » uniquement si c'est nécessaire. Des points pourront être enlevés en cas d'erreur. On suppose qu'on se trouve, comme en TP, sur un système Debian - GNU/Linux.

## 1- [19] Divers et Culture

1. [3] Quelle commande taper pour copier le répertoire "clients" qui se trouve dans le répertoire personnel de "toto" vers le répertoire /tmp. "clients" se trouve sur exemple2.org et /tmp se trouve sur exemple1.org. On se trouve sur exemple2.org. On suppose qu'on connait le mot de passe de toto. scp -r toto@exemple2.org:clients /tmp
2. [1] Donnez le nom (juste le nom) de deux autres commandes permettant de copier des fichiers entre deux machines. ftp, rsync ...
3. [1] Un service "toto" qu'on vient d'installer ne fonctionne pas. Ou exactement faut-il regarder pour essayer de comprendre ce qui se passe? fichiers logs , par ex: /var/log/toto.log
4. [2] A quoi sert NFS ? Network File System : "disque réseau / partagé" - accéder à des fichiers sur une machine distante
5. [1] Comment s'appelle le protocole écoutant normalement sur le port 25 ? SMTP
6. [3] A quoi sert CRON ? Donnez deux exemples de choses importantes en administration système qu'on pourrait faire avec CRON. Lancer des tâches périodiquement : Exemples: sauvegardes, mise à jour du systeme, "nettoyage" du disque ou BdD ...
7. [2] Donnez le nom de deux logiciels de Système de Gestion de Base de Données (DGBD). Postgres, Mysql, Oracle, Access ...
8. [2] A quoi sert GRUB ? A quel moment intervient-il?
9. [2] Qu'est-ce que le "swap" ? Le swap est une partition (ou un fichier) sur le disque qui sert d'"auxiliaire" à la mémoire vive, lorsque celle-ci est pleine.
10. [2] A quoi servent POP ou IMAP ? Décrivez brièvement. permettent de chercher (et gérer) des courriels stockés sur un serveur. Souvent utilisé par des clients mails comme Thunderbird, Outlook...

## 2- [13] Logiciels

1. [4] Lorsqu'on tape une commande (par exemple "ls"), comment est-ce que le système trouve le fichier "ls" qu'il soit exécuter ? Décrivez en détail. Comment changer ce comportement (donnez un exemple habituel)? Le bash parcourt les répertoires donnés dans $PATH, séparées par des ":". Il s'arrête dans le 1er répertoire ou il trouve le fichier exécutable. export PATH=$PATH:/home/toto/mes-programmes
2. [4] Un utilisateur installe un logiciel « xyz » à l'aide de la commande « sudo apt-get install xyz ». Décrivez en détail, en les numérotant les grandes étapes parcourues par cette commande. vérification des dépendances, téléchargement des paquets nécessaires, dés-archivage / copie des fichiers contenus dans les paquets vers les répertoires du systeme, (éventuellement: exécution de scripts de post-install)
3. [2] On tombe sur un fichier "/usr/bin/abc" qu'on ne connait pas et on voudrait obtenir plus d'informations le concernant. Quelles commandes taper ? (expliquez très brièvement) 1) dpkg -S /usr/bin/abc 2) apt-cache show nom-paquet
4. [3] A quoi nous a servi la commande make? Décrivez le contexte dans lequel on l'a vue en TP et en cours? Elle nous a servi à lancer la compilation d'un logiciel, lorsqu'on installe un logiciel à partir d'un code source (C par exemple) Avec "make install" on copie les fichiers vers leur répertoires finaux.
5. [4] Quels sont les différents types de fichiers constituant un logiciel "xyz" typique? Inventez des exemples précis, en commençant par ceux qui vous paraissent les plus représentatifs. Indiquez dans quels répertoires ils peuvent se retrouver après installation du logiciel. fichiers binaires exécutables, /usr/bin/xyz, fichiers de documentation /usr/share/doc/xyz/... ou /usr/share/man.., librairies: /usr/lib/libxyz.so, fichiers de configuration: /etc/xyz.conf

## 4- [15] Utilisateurs et droits d'accès

1. [2] Dans quel fichier est enregistrée la liste des utilisateurs du système? Dans quel fichier sont enregistrés les mots de passe "cryptés" ? utilisateurs : /etc/passwd et mdp cryptés : /etc/shadow
2. [4] Si on vous donne un mot de passe "crypté" (comme ceux de la question précédente), peut-on le "décrypter" ? Expliquez. Non, ce "cryptage" (en fait un hash) n'est pas réversible. On peut essayer de trouver un mdp ayant le même hash en essayant de nombreuses combinaisons (très

long). On peut aussi utiliser un "dictionnaire" pour limiter la combinatoire. Si le mdp est bien choisi (long et complexe), il est presque impossible de le retrouver.

3. [2] Est-ce que les commandes suivantes produisent une erreur (expliquez) ?
   `sudo mkdir /data;cp /tmp/exemple /data` (on suppose que exemple existe) Erreur: Le /data appartient a root et par defaut pas de droit d'ecriture aux autres
4. [5] la commande "ls -l test "affiche ce qui suit (simplifié):
   `-rwxrw-r--  abcd efghi 12345 2010-11-10 09:45 test`
   Qu'est-ce que "abcd" ? Qu'est-ce que "efghi" ? Qu'est-ce que "12345" ?
   Décrivez en français très précisément qui peut faire quoi avec ce fichier ? propriétaire, groupe, taille en octets. abcd peut le lire, le modifier, et l'exécuter. Les membres du groupe efghi peuvent le lire et le modifier. Les autres (ni abcd ni dans le groupe efghi) peuvent juste le lire.
5. [2] On voudrait que l'utilisateur "toto" puisse modifier ce fichier (il ne peut pas le faire actuellement). Donnez deux commandes utilisant des approches très différentes pour y arriver. chmod o+w test ; sudo chown toto test

## 5- [25] Disques, données et sécurité

1. [6] Vous venez d'acheter un disque dur SATA et l'avez juste branché sur la machine. C'est le troisième disque SATA de la machine. Donnez toutes les commandes nécessaires pour arriver à effectivement utiliser ce disque. A chaque étape donnez quelques mots d'explication. 1. partitionner le disque: sudo fdisk /dev/sdc ; 2. créer le système de fichiers: sudo mkfs /dev/sdc1 ; 3) monter la partition (associer à un répertoire): sudo mkdir /disque2 ; sudo mount /dev/sdc1 /disque2
2. [1] Quel est le nom du système de fichiers le plus répandu sous Linux? ext3, ext4
3. [3] Quel type de système permet de se protéger contre une interruption de service en cas d'une panne d'un disque dur? Pourquoi ? RAID (1,5...) grâce à la redondance le système peut reconstituer les données du disque manquant. Un contrôleur RAID matériel de qualité peut survire à la panne d'un disque et continuer à fournir les données.
4. [3] Quel type de système permet de récupérer ses données si on efface des fichiers par erreur et qu'on ne s'en aperçoit que bien plus tard ? Expliquez et décrivez. Une sauvegarde incrémentale conserve un historique complet des fichiers, on peut donc retrouver nos fichiers tels qu'ils étaient à n'importe quel moment.
5. [4] Décrivez brièvement le fonctionnement d'un système RAID-1. Ensuite (ca n'a pas été traité en cours, réfléchissez par vous mêmes) pourquoi est-ce qu'un système RAID-1 permet de doubler la vitesse de lecture mais pas d'écriture ? Le RAID-1 maintient deux disques identiques en permanence. A chaque écriture les données sont écrites sur les deux disques en même temps. Les données peuvent être lues de n'importe lequel des 2 disques, comme ils sont identiques. On peut donc lire 2 données en parallèle (d'ou performance lecture x2). Ce n'est pas le cas en écriture (performance x1).
6. [4] Les pirates ont a leur disposition de très nombreuses machines. Comment s'appelle un groupe de machines de ce type ? Décrivez brièvement. Comment font-ils pour obtenir un tel groupe de machines ? Que font-il avec ? Un botnet est constitué de machines (zombies) contrôlées par des pirates. Ils en prennent le contrôle en circulant diffusant à grande échelle des logiciels malveillants qui exploitent des failles de sécurité pour s'installer. Ces machines peuvent être utilisés par exemple pour envoyer du spam, ou racketter en menaçant de bloquer / submerger des sites web (DDoS).
7. [4] Décrivez en détail et avec précision un exemple de faille de sécurité de votre choix. Montrez comment un pirate peut l'exploiter. buffer overflow, injection sql, failles en PHP ... voir cours

## 6- [28] Hébergement et serveur apache

1. [4] Qu'est-ce qu'un hébergement mutualisé? Et un serveur dédie? Comparez les avantages et inconvénients pour l'hébergement d'un site web.
2. [2] Qu'est-ce qu'une machine virtuelle ? (vu en cours) Donnez un nom de logiciel permettant de créer des machines virtuelles. La possibilité de faire tourner plusieurs machines (avec des OS) à l'intérieur d'une même machine physique. Xen, KVM, VirtualBox, VMWare...
3. [4] Pourquoi et comment peut-on utiliser des machines virtuelles pour des serveurs ? Elles permettent de donner le contrôle complet (root) sur une machine virtuelle tout en hébergeant plusieurs MV sur une machine physique (moins cher). Avec des serveurs de fichiers, on peut facilement migrer d'une machine physique à une autre: + robuste aux pannes, avantages de gestion de parc pour l'hébergeur... on vend du CPU/Mémoire/Stockage
4. [7] Décrivez de manière détaillé ce qui se passe entre la saisie d'une url dans un navigateur web et l'affichage de la page web correspondante dans ce navigateur. Vous distinguerez bien les différents logiciels intervenant coté client et coté serveur, en les décrivant brièvement. Vous décrirez le flux de l'information. On se placera d'abord (a) dans le cadre d'une page html

simple et ensuite (b) dans le cas d'un script php accédant à une base de données. (attention: on attend une description précise et détaillée)

5. [4] Décrivez les différents répertoires ou se trouvent les fichiers de configuration apache. /etc/apache2: répertoire principal avec apache2.conf, fichier de configuration centrale qui inclut tous les autres. /etc/apache/sites-available: un fichier de config par site (VirtualHost) hébergé. /etc/apache2/sites-enabled: liens symboliques vers les fichiers sites-available (permet d'activer / désactiver facilement des sites).
6. [2] Pour apache, qu'est-ce qu'un VirtualHost ? Les VirtualHost permettent d'heberger plusieurs sites web avec un seul serveur apache. On les distingue souvent grace à leur nom (ServerName).
7. [3] Donnez un exemple de VirtualHost avec les directives qui vous semblent les plus importantes permettant de définir un VirtualHost en les expliquant (si vous ne vous souvenez pas du nom exact d'une directive, inventez et expliquez a coté) [Exemple de fichier avec au moins DocumentRoot et ServerName. plus de points si: Directory, ErrorLog, CustomLog ...]
8. [2] Pour faire des statistiques, on voudrait savoir combien de visiteurs se sont connectés à un site web. A partir de quel fichier peut-on déterminer cette information? fichier log, /var/log/apache2/access.log

## 7- [11] Logiciels Web

9. [2] A quoi sert PhpMyAdmin ? Comment fait-on si on ne l'a pas ? Sert à gérer un BdD mysql : créer de BdD, des tables, visualiser, manipuler... on peut utiliser la commande mysql (client mysql en ligne de commande)
10. [3] On est sur un système Debian (comme celui vu en TP). Un logiciel PHP veut pouvoir modifier le contenu d'un fichier (par exemple avec <?php file_put_contents("nomfichier") ;?>). "ls -l nomfichier" donne:
    ```
    -rw-------  abcd efghi 12345 2010-11-10 09:45 nomfichier
    ```
    Quelle(s) commande(s) taper pour que ce soit possible, sans que tout le monde puisse le changer?
    chown www-data nomfichier
11. [6] Vous gérez un site web utilisant un logiciel comme PhpBB ou Drupal . Vous voulez changer d'hébergeur (on suppose, par exemple, que vous êtes sur un hébergeur mutualisé). Qu'est-ce qu'il faudra transférer ? Quelles opérations faudra-t-il faire ? On suppose que vous avez un accès ssh sur les deux machines. Donnez les commandes (mêmes approximatives), pour chaque étape en inventant les informations qu'il vous manque. Il faut 1) transférer les fichiers du logiciel et les fichiers générés ou uploadés par les utilisateurs du site : rsync rsync, scp , ftp : ex: rsync -a monsite/ toto@machine2:monsite/ et 2) transférer la BdD: mysqldump ou phpmyadmin: mysqldump -u toto -p > dump.sql, copie du fichier dump scp/ftp: scp dump.sql toto@machine2: et chargement du fichier dump: mysql, phpmyadmin mysql -u toto -p < dump.sql