

Master Informatique – 1^{re} année**INF-2211 – Administration des systèmes et des réseaux****1^{re} session – 1^{er} juin 2022 – 14 h 00****Responsables : F. Guidec, Y. Mahéo****3 pages – Durée : 2 h 00**

Avertissements : *Le barème de notation indiqué ci-dessous est purement indicatif et pourrait être révisé lors de la correction. La notation tiendra compte de l'esprit de pédagogie et de synthèse dont vous ferez preuve (soyez clair et concis!), mais aussi de la présentation générale de la copie. Il est notamment impératif que les réponses donnent lieu à des phrases compréhensibles et grammaticalement correctes.*

Dans tous les cas, des réponses précises et argumentées sont attendues ! En particulier, lorsque votre réponse contient des commandes Unix à exécuter, il faut en général donner les commandes avec les arguments appropriés.

1 Partie « Système » (10 points)**1.1 Pitungan (5 points)**

On considère une machine Linux offrant un certain nombre de services (serveur web, serveur ftp...) et permettant notamment d'exploiter une application de calcul scientifique nommée *pitungan*. Cette application prend la forme d'un ensemble d'exécutables stockés dans le répertoire `/usr/local/pitungan/bin`. Il s'agit d'un démon (lancé en tant que root par la commande `pitungand`) et de plusieurs commandes (fichiers débutant par `ptg_`) lancées en mode terminal par les utilisateurs. Ces commandes dialoguent avec le démon et produisent des fichiers temporaires de petite taille dans le répertoire `/var` et des fichiers dont la taille peut atteindre plusieurs Go dans les répertoires personnels des utilisateurs. La machine, accessible par ssh, héberge une centaine de comptes locaux avec des répertoires personnels locaux dont la seule raison d'être est l'utilisation de *pitungan*. Le système et l'ensemble des répertoires personnels sont installés sur l'unique partition du 1er disque dur SATA ayant pour capacité 2 To. L'espace disque est suffisant pour l'exploitation normale de l'application par l'ensemble des utilisateurs.

- a) La situation actuelle est inconfortable pour l'administrateur dans la mesure où il doit lancer le démon `pitungand` à chaque fois qu'il démarre le système, et il doit l'arrêter (en tuant le processus démon) à chaque arrêt du système. Détaillez ce que doit faire l'administrateur pour remédier à cette situation ?
- b) Sur les conseils d'un collègue, l'administrateur équipe la machine d'un deuxième disque dur SATA de 4 To afin de faire en sorte que les répertoires personnels des utilisateurs soient dorénavant stockés sur la première moitié du deuxième disque, la deuxième moitié étant réservée à un usage futur. Pour quelle raison principale cette opération a un intérêt ? Décrivez précisément la suite de manipulations que l'administrateur doit effectuer pour réaliser cette opération, en faisant l'hypothèse que le disque neuf a été connecté et la machine démarrée (elle est utilisée normalement). À l'issue des manipulations, l'application doit être de nouveau disponible pour les utilisateurs. Donnez le texte de certaines commandes Unix et des extraits de contenu de fichiers de configuration si nécessaire.
- c) Un jour, on contacte l'administrateur car un des fichiers de `/var`, généré par *pitungan*, a une taille anormalement grande et qui croît continûment. Expliquez comment l'administrateur peut identifier la source du problème et empêcher, à court terme, la saturation potentielle du disque.

1.2 Virtualisation (2 points)

Expliquez ce qu'est la paravirtualisation. Citez des avantages et inconvénients de cette technique.

1.3 Permissions (3 points)

Soit l'exécution de commandes suivante (les numéros de lignes ont été ajoutés pour simplifier votre travail) :

```
(1) # ls -ld /tmp
(2) drwxrwxrwt 12 root root 1024 Apr 19 04:02 /tmp
(3) # ls -l /home/dupont/bin/*.sh
(4) -rwx---rwx 1 dupont users 198 2008-05-16 11:35 /home/dupont/bin/run.sh
(5) -rwxr-s--- 1 dupont adm 217 2009-03-12 10:54 /home/dupont/bin/check.sh
(6) # ls -ld /data/docshare
(7) drwxrws--- 25 root g2 4096 Mar 13 11:02 /data/docshare
(8) # ls -l /bin/bash
(9) -rwsr-xr-x 1 root root 702160 2008-05-12 20:33 /bin/bash
```

Expliquez l'effet des permissions affichées sur les lignes 2, 4, 5, 7 et 9, en formulant un avis critique le cas échéant.

2 Partie « Réseau » (10 points)

On considère la mise en service d'un parc informatique constitué de quelques dizaines de stations de travail tournant toutes sous Linux. Ces stations vont être réparties sur deux LAN Ethernet A et B, entre lesquels on installe une station R_1 ayant vocation à devenir un routeur garde-barrière. Cette station R_1 est dotée de trois interfaces réseau : deux interfaces Ethernet (baptisées *eth0* et *eth1*) desservent respectivement les LAN A et B, et une interface PPPoE (baptisée *ppp0*) mène vers Internet via une ligne de type VDSL2.

L'administrateur installe sur R_1 un serveur DHCP afin de distribuer aux stations des LAN A et B des adresses IPv4. Le LAN A doit à terme faire office de DMZ et les stations de ce LAN reçoivent donc via DHCP des adresses publiques prises dans la gamme d'adresses 195.85.72.0/23. En revanche les stations du LAN B reçoivent via DHCP des adresses privées prises dans la gamme d'adresses 192.168.1.0/24.

2.1 Auto-configuration IP (3 points)

En examinant l'état de l'interface *eth0* de la station R_1 , on constate que cette interface porte les trois adresses suivantes : 195.85.72.1, fe80::a6ba:dbff:fe18:b43b/64, et 2ab2:db8:3bfd::a6ba:dbff:fe18:b43b/64.

- a) De quels types d'adresses s'agit-il ? Comment les adresses préfixées fe80: et 2a02: ont-elles été attribuées à cette interface ?

On considère une station S_1 appartenant au LAN A. On constate qu'après démarrage de cette station son interface *eth0* porte les adresses 195.85.72.5 et fe80::b46c:aef:fe12:c8c6/64. L'administrateur déploie alors un démon *radvd* sur R_1 et le configure pour que le mécanisme de *Router Advertisement* soit actif sur l'interface *eth0* de R_1 (et sur cette interface seulement).

- b) Après le déploiement de ce démon, et après redémarrage de la station S_1 (ou simple relance de ses services réseau), quelles vont être les adresses attribuées à l'interface *eth0* de S_1 ?

2.2 Configuration de R_1 en tant que routeur (1 point)

L'administrateur exécute la commande suivante pour activer la fonction de routage sur R_1 :

```
%> sysctl net.ipv4.conf.all.forwarding=1
```

À ce stade, le trafic IP est-il possible entre les machines des deux LAN A et B d'une part, et entre ces machines et le reste d'Internet d'autre part ? (Soyez précis !)

2.3 Configuration de R_1 en tant que garde-barrière (6 points)

L'administrateur exécute ensuite la série de commandes suivantes (les lignes sont ici numérotées pour vous permettre d'y faire référence dans votre copie) :

```
%1> iptables -F
%2> iptable -P OUTPUT DROP
%3> iptables -P INPUT DROP
%4> iptables -P FORWARD DROP
%5> iptables -t nat -A POSTROUTING -s 192.168.1.0/24 -o ppp0 -j MASQUERADE
%6> iptables -A FORWARD -d 195.85.72.0/23 -i ppp0 -j ACCEPT
%7> iptables -A FORWARD -s 195.85.72.0/23 -o ppp0 -j ACCEPT
%8> iptables -A FORWARD -s 192.168.1.0/24 -o ppp0 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
%9> iptables -A FORWARD -d 192.168.1.0/24 -i ppp0 -m state --state ESTABLISHED,RELATED -j ACCEPT
```

a) Quelle est l'influence de la ligne 5 sur le trafic traversant R_1 ?

b) Même question concernant les lignes 8 et 9.

Après l'exécution des commandes précédentes, l'administrateur constate qu'aucun trafic n'est possible entre les stations du LAN A et celles du LAN B. Il souhaite pourtant que ce trafic soit possible, mais seulement à l'initiative des stations du LAN B.

c) Proposez des commandes permettant d'atteindre cet objectif.

L'administrateur souhaite que le routeur R_1 puisse être administré à distance par SSH (port TCP n°22), mais uniquement depuis les stations du LAN B.

d) Proposez des commandes permettant d'atteindre cet objectif.

L'administrateur souhaite qu'un serveur Web (port TCP n°80), déployé dans le LAN A sur la machine d'adresse 2ab2:db8:3bfd::a6ba:dbba:fb8c:b26b/64, soit accessible en IPv6 depuis Internet, mais que tout autre trafic IPv6 soit impossible à travers R_1 .

e) Proposez des commandes permettant d'atteindre cet objectif.

L'administrateur déploie enfin un serveur NIS sur une machine du LAN A, et souhaite que ce serveur soit accessible des machines clientes situées indifféremment dans les LAN A et B (et en IPv4 uniquement).

f) Que pensez vous de cet objectif? (Il ne vous est cette fois pas demandé de proposer des commandes, mais de discuter de la pertinence de cet objectif, et de proposer une démarche permettant de l'atteindre le cas échéant.)

