TD N°5 Réseaux – R&T 2A

Rappel sur les droits d'accès sous Unix :

Un fichier appartient à un propriétaire et à un groupe. Il possède des droits de lecture/écriture/exécution pour le propriétaire, pour le groupe, pour les autres.

- L'utilisateur toto du groupe gtr2 ne peut **lire** un fichier que si :
  - le fichier appartient à toto et est en mode lecture pour le propriétaire ;
  - le fichier appartient au groupe gtr2 et le fichier est en lecture pour le groupe ;
  - le fichier est en lecture pour les autres.

- L'utilisateur toto du groupe gtr2 ne peut **créer** un fichier dans un répertoire que si :
  - le répertoire appartient à toto et est en mode écriture pour le propriétaire ;
  - le répertoire appartient au groupe gtr2 et est en mode écriture pour le groupe ;
  - le répertoire est en mode écriture pour les autres.

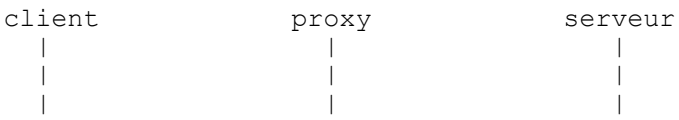
1. Droits d'accès

Soit la configuration suivante. L'administrateur du site est webmaster, son groupe est www. Le groupe www ne comporte qu'un seul membre : webmaster. L'arborescence du site appartient à webmaster et au groupe www. Elle est en lecture/écriture pour webmaster et en lecture seule pour www. Les scripts CGI sont exécutables par webmaster et par le groupe www.

1) Montrer que les documents locaux du site ne peuvent pas être accédés par les utilisateurs du serveur (sauf webmaster).
2) Pourquoi le serveur httpd ne doit-il pas avoir les droits suivants : propriétaire root, groupe root ?
3) Pourquoi le serveur ne peut-il pas avoir les droits : propriétaire : webmaster, groupe nogroup ?
4) Pourquoi le serveur ne peut-il pas avoir les droits : propriétaire : nobody, groupe nogroup ?
5) Que se passe-t-il si le serveur a été configuré avec les droits : propriétaire : nobody, groupe www ?
6) Dans ce dernier cas, quels doivent être les droits des pages personnelles des utilisateurs ? Problème ?

2. Proxy HTTP

- Un client demande une page web d'un serveur en utilisant un serveur web proxy qui n'a malheureusement pas cette page dans son cache. Sur le diagramme suivant indiquez par des flèches les messages HTTP échangés en précisant à chaque fois s'il s'agit (a) d'un message GET ou (b) d'une réponse HTTP positive de code 200. (Ne précisez pas le contenu exact des messages.)



- Un commerçant sur Internet veut créer un site web et permettre à ses clients d'y naviguer pour remplir un caddie virtuel. Donnez au moins deux possibilités de gérer le caddie virtuel de ses clients. (On n'utilisera pas le numéro IP pour identifier les clients, à cause des serveurs proxy.)

3. Protocoles

Alice envoie un mail de la machine *toto.iutc3.unicaen.fr* à *Marc@free.fr*. Le serveur de mail du domaine *free.fr* est ***imp.free.fr***. Marc lit son courrier à partir de la machine *titi.emn.fr* (du domaine emn.fr) avec un navigateur web sur l'adresse *http://imp.free.fr/*, qui est une interface webmail pour lire son courrier en passant par le proxy ***proxy-gw.emn.fr***.

- Faites un schéma avec les machines citées, en précisant les connexions et les protocoles d'application utilisés dans ce scénario (HTTP, SMTP, POP3 ou IMAP).

4. Pourriel et serveurs relais

Les deux en-têtes de courriers électroniques suivants proviennent de pourriels (Spam) qui ont été relayés par des serveurs SMTP probablement mal configurés. Pour chacun de ces en-têtes, déterminer l'adresse IP (éventuellement

le nom) de la machine émettrice du message et du serveur SMTP qui a accepté de le relayer. Vérifier (sur machine) si ces serveurs SMTP acceptent encore le relais.

```
From root Sat Aug 11 20:54 MET 2001
Received: from cnshow.com ([210.77.145.198])
        by crcsun15.eplf.ch (8.8.X/EPLF-8.1a) with ESMTP id UAA18188
        for <oechslin@crc.eplf.ch>; Sat, 11 Aug 2001 20:54:10 +0200 (MET DST)
Received: from slip-12-64-6-240.mis.prserv.net (HELO 12.64.6.240) (12.6.64.240)
        by cnshow.com with SMTP; 11 Aug 2001 01:03:55 -0000
Message-ID: <0000318379cc$0000404c$00000f94@>
From: jo221@qatarmail.com
To: <Undisclosed.Recipients>
Subject: test
Date: Fri, 10 Aug 2001 18:41:49 -0000
```

```
From root Sat Aug 18 04:56 MET 2001
Received: from ns.tsp.co.kr ([203.228.72.78])
        by crcsun15.eplf.ch (8.8.X/EPLF-8.1a) with ESMTP id EAA27998
        Sat, 18 Aug 2001 04:54:22 +0200 (MET DST)
Received: from gw05_[192.168.227.29] (cust-90-62-as01.chcg.eli.net
[209.210.90.62])
        by ns.tsp.co.kr (8.9.3/8.9.3) with SMTP id LAA29540;
        Sat, 18 Aug 2001 11:45:27 +0900
Message-ID: <0000340654bc$000010af$00001290@mail2.howareyoutoday.org>
From: illsdoil@howareyoutoday.org
To: <illsdoil@howareyoutoday.org>
Subject: Are You Ready For Wealth & Freedom????
Date: Fri, 17 Aug 2001 21:47:36 -0000
```

5. Courrier forgé

En ouvrant une session **telnet** sur le port 25 de son serveur SMTP, il est possible d'envoyer un courrier électronique. Illustrer cette technique en utilisant les commandes SMTP **HELO**, **MAIL FROM :** , **RCPT TO:** , **DATA** et **QUIT** pour envoyer un courrier à votre propre adresse électronique.