**Master Sciences & Technologies**
**Mention Informatique**
**Université Bordeaux 1**

**Architecture des réseaux**
**et systèmes associés**
**Travaux Dirigés**

# De port en port

**Exercice 1.** Tunnel.

Pour cet exercice, nous allons utiliser une version modifiée de la commande `netcat`, rebaptisée `gnunetcat`, que vous pouvez rapatrier ou utiliser directement depuis
*http ://www.labri.fr/perso/casteigt/enseignement/SDRP/ARSA/td1/*

1. Entrez la commande suivante dans un terminal :
   `gnunetcat -x -L google.fr:80 -p 10000`
   À première vue, quel peut être le rôle de chacun des éléments de cette commande ?
2. Dans votre navigateur, visitez l'url `localhost:10000`
   Explicitez maintenant les différents éléments de la commande.

**Exercice 2.** FTP.

Dans cet exercice, nous utiliserons les commandes `ftp` et `netcat` (dans sa version d'origine, cette fois) afin de nous familiariser avec le protocole FTP.

1. À l'aide de la commande `ftp`, connectez-vous au serveur `ftp.lip6.fr` en utilisant le login *anonymous* et un mot de passe quelconque. Une fois connecté, listez le contenu du répertoire d'accueil, puis récupérez le fichier `jussieu/README`. On pourra s'aider au besoin de la page de manuel de la commande `ftp`.
2. En recommençant la procédure précédente en mode *debug* (man ftp), notez les commandes FTP correspondant à chacune de vos actions, en portant une attention particulière à la commande PORT.
3. A l'aide de la commande `grep` et du fichier `/etc/services`, retrouvez le numéro de port correspondant au protocole FTP, que l'on appelera *nftp*.
4. En tapant la commande `netcat ftp.lip6.fr nftp`, tentez de reproduire les actions correspondant aux commandes FTP que vous avez noté précédemment. Cela fonctionne-t-il ? D'où vient le problème ? Appelez-moi pour tenter de m'expliquer.
5. L'utilisation conjointe des commandes `netcat` et `netcat -l` (dans deux terminaux distincts) devrait vous permettre de récupérer le fichier, comment procédez-vous ? Appelez-moi pour me faire une démo.

**Exercice 3.** SSH - Authentification.

On pourra s'aider du manuel de la commande `ssh`, de celui du démon `sshd` et de celui du fichier de configuration `ssh_config`, mais avant tout, entrez la commande `killall  ssh-agent` pour éliminer vos éventuels agents ssh.

1. Connectez-vous sur une machine via la commande `ssh -v` et observez la trace de connexion. Quel type d'authentification est finalement utilisée ? pourquoi ?
2. Retournez sur votre machine (`exit`, `logout` ou `Ctrl-d`). Créez une identité au moyen de la commande `ssh-keygen` ; on utilisera une *passphrase* (un mot de passe) non vide, mais pas très longue. Observez au passage les droits d'accès aux fichiers de votre répertoire `~/.ssh/`

3. Réitérez l'étape 1. Quelque chose a changé ? Quel type d'authentification est finalement utilisée ?
4. Retournez sur votre machine, recopiez votre clef publique dans le fichier `~/.ssh/authorized_keys`, puis réitérez l'étape 1. Quel type d'authentification est finalement utilisée ?

**Exercice 4.** SSH - Redirection

Au sein d'une entreprise de 1200 personnes, M. X rencontre des difficultés à lire les forums internes à l'entreprise depuis chez lui.

Afin de faciliter la consultation de ces forums à lui même et à ses amis, il décide de proposer leur accès via le serveur http. Il utilise un système d'authentification basé sur une copie de la liste des mots de passe unix, automatisant ainsi l'administration du système. Pour consulter les forums, l'utilisateur n'a qu'à simplement saisir son mot de passe sur une page accessible sur le web.

1. Expliquez pourquoi l'ingénieur chargé de la sécurité ordonne l'arrêt immédiat du service sous peine de sanction.
2. Afin de résoudre ce problème M. Y propose de rediriger directement le port 119 du serveur nntp vers un port accessible depuis l'extérieur. Que pensez-vous de cette solution ?
3. Prendre connaissance des options `-L` et `-R` de SSH.
4. L'entreprise étant dotée du service SSH, proposez une solution simple, légale et sécurisée à ce problème. Faire une démonstration avec le service nntp de l'université (disponible au port 119 de la machine news.u-bordeaux1.fr) et firefox.

**Exercice 5.** SSH - Agents.

Dans un shell annexe, lancez la commande `netstat -tca` afin de *bien* observer à chaque étape l'évolution des connexions réseau. Vérifier que vous n'avez pas de processus exécutant le programme `ssh-agent`.

1. Observez l'effet sur les connexions d'une ouverture et d'une fermeture d'une connexion `ssh`.
2. Créez un agent en tapant `ssh-agent` puis `ssh-add`[1] ; exécutez les affectations et exportations produits à l'écran par `ssh-agent` puis lancez `ssh-add`[2].
3. Connectez-vous maintenant sur une machine *via* `ssh`. l'agent. Recommencez à partir d'un nouveau shell lancé dans ce même terminal.
4. Qu'est ce qu'un agent ? À quel niveau préférera-t-on lancer un agent ? Comparer les intérêts relatifs de la passphrase (ssh), du mot de passe (unix), de la copie multiple des clefs privées.

**Exercice 6.** Client FTP

Ceux d'entre vous qui ont fini en avance peuvent se lancer (discrètement) dans l'écriture d'un client FTP minimaliste, en langage C.

[1] une erreur se produit, la comprendre
[2] une technique plus directe est `exec ssh-agent bash` puis `ssh-add`