Comment installer un serveur FTP sécurisé

Christopher Klaus <cklaus@shadow.net> 26 Juillet 94

Ce document pourra intéresser tous ceux qui envisagent d'installer un serveur FTP anonyme sur leur système Linux. Écrit par Christopher Klaus, il est posté régulièrement dans le groupes de nouvelles `comp.security.misc` sous le titre "computer-security/anonymous-ftp FAQ". Traduction et adaptation par Michel Billaud <billaud@labri.u-bordeaux.fr> (Septembre 1995).

1 Introduction

Ce qui suit est une liste de questions-réponses sur l'installation d'un serveur FTP sécurisé.

Il est bien connu que les serveurs FTP sont utilisés pour effectuer des transferts illégaux de fichiers. Un serveur FTP mal configuré offre beaucoup d'opportunités d'accès à des pirates. Enfin, beaucoup de serveurs présentent des brêches de sécurité.

Cette FAQ (liste de questions fréquentes) est destinée à limiter les dégâts en donnant aux administrateurs une liste de points à contrôler pour s'assurer que leur serveur FTP est bien configuré, et qu'ils possèdent bien la dernière version du démon FTP.

2 Liste de questions-réponses

Le texte est organisé comme suit :

1. Description générale de l'installation d'un serveur de FTP anonyme
2. Installation d'un serveur FTP sécurisé à racine déplacée
3. Informations spécifiques au système d'exploitation et suggestions
4. Où obtenir d'autres démons FTP.
5. Comment savoir si votre serveur FTP anonyme est sécurisé
6. Archie

2.1 Description générale de l'installation d'un serveur de FTP anonyme

Comment installer un ftp anonyme sécurisé ?

Lisez toutes les notes et tous les avertissements !

1. Ajoutez un nouvel utilisateur `ftp` dans `/etc/passwd`. Utilisez un groupe ordinaire. Le répertoire d'accueil de cet utilisateur sera `~ftp`, ce sera la racine de l'arborescence que les utilisateurs anonymes

verront. Utilisez un mot de passe et un shell invalides pour plus de sécurité. Cette ligne du fichier `passwd` ressemblera à ceci :

```
ftp:*:400:400:Anonymous FTP:/home/ftp:/bin/true
```

2. Créez le répertoire d'accueil `~ftp`, et donnez-en la propriété à `root` (**pas à `ftp`**). Ainsi, les permissions du propriétaires seront attribuées à `root`, et les permissions de groupes concerneront les utilisateurs anonymes. Mettez les droits d'accès de `~ftp` à `555` (lecture, pas d'écriture, exécution).

   > Certaines pages de manuel recommandent d'attribuer le répertoire `~ftp` à l'utilisateur `ftp`. **Ne le faîtes surtout pas** si vous tenez à la sécurité de votre système.

3. Créez le répertoire `~ftp/bin` appartenant à `root` (groupe `wheel` par exemple), avec les droits d'accès `111` (pas de lecture, pas d'écriture, exécution).

4. Copiez le programme `ls` dans `~ftp/bin`. `ls` appartiendra à `root`, avec les droits `111` (pas de lecture, pas d'écriture, exécution). Vous donnerez les mêmes droits à toutes les commandes que vous mettrez ultérieurement dans `~ftp/bin`.

5. Créez le répertoire `~ftp/etc`, propriété de `root` avec les droits `111`.

6. Créez des fichiers `passwd` et `group` dans `~ftp/etc`, avec les droits `444`. Le fichier `passwd` ne devrait contenir que `root`, `daemon`, `uucp` et `ftp`. Le fichier `group` contiendra le groupe choisi pour l'utilisateur `ftp`. Utilisez vos fichiers `/etc/passwd` et `/etc/group` comme modèles pour `~ftp/etc/passwd` et `~ftp/etc/group`. Vous pouvez changer les noms d'utilisateurs dans ce fichier, ils ne sont utilisés que par la commande `ls`. Si par exemple les fichiers de votre arborescence `~ftp/pub/linux` sont gérés par un utilisateur `balon` ayant l'`uid` `156`, vous pouvez mettre la ligne

   ```
   linux:*:156:120:Kazik Balon::
   ```

   dans le fichier `~ftp/etc/passwd` (indépendemment de son vrai nom). Ne faîtes figurer que les utilisateurs qui possèdent des fichiers dans l'arborescence FTP, (c'est-à-dire `root`, `daemon`, `ftp`...) et supprimez résolument **tous** les mots de passe en les replaçant par une étoile "`*`". Les lignes du fichier `~ftp/etc/passwd` ressembleront donc à ceci :

   ```
   root:*:0:0:Ftp maintainer::
   ftp:*:400:400: Anonymous ftp::
   ```

   Pour plus de sécurité, vous pouvez tout simplement supprimer `~ftp/etc/passwd` et `~ftp/etc/group` (dans ce cas la commande "`ls -l`" ne montrera pas les noms des groupes des répertoires). Le démon FTP de Wuarchive (et d'autres) se base également sur le contenu des fichiers `group` et `passwd` : lire la documentation appropriée.

7. Créez le répertoire `~ftp/pub`. Ce répertoire vous appartiendra et aura le même groupe que `ftp` avec les droits `555`. Sur la plupart des systèmes (comme SunOs) vous pourrez donner les droits `2555` (positionnant le bit `set-group-id`) pour que les fichiers créés dans ce répertoire appartiennent au même groupe.

Les fichiers déposés dans ce répertoire seront accessibles publiquement. Vous mettrez les mêmes droits d'accès `555` à tous les sous-répertoires de `~ftp/pub`.

Ni le répertoire d'accueil `~ftp`, ni aucun de ses sous-répertoires ne devra appartenir à l'utilisateur `ftp` (ni aucun fichier nulle part ailleurs). Les démons FTP modernes supportent des tas de commandes très utiles, comme `chmod`, qui permettent de modifier de l'extérieur les droits d'accès que vous avez laborieusement positionnés. Des options de configurations permettent de désactiver ces commandes (ici WuFTP) :

```
# all the following default to "yes" for everybody
delete          no      guest,anonymous         # delete permission?
overwrite       no      guest,anonymous         # overwrite permission?
rename          no      guest,anonymous         # rename permission?
chmod           no      anonymous               # chmod permission?
umask           no      anonymous               # umask permission?
```

8. Si vous voulez que les utilisateurs anonymes puissent déposer des fichiers, créez le répertoire `~ftp/pub/incoming` (propriétaire `root`, droits `733`). Faîtes un "`chmod +t ~ftp/pub/incoming` ". Normalement le démon FTP interdit aux utilisateurs anonymes d'écraser un fichier existant, mais un utilisateur normal pourrait détruire n'importe quoi. En mettant les droits à `1733` ce ne sera plus possible. Avec `wuftpd` vous pouvez configurer le démon pour que les fichiers créés le soient avec les droits `600` et appartiennent à `root` (ou tout autre utilisateur). Parfois répertoires "incoming" sont utilisés frauduleusement pour échanger de fichiers piratés ou pornographiques. Les fraudeurs y créent des sous-répertoires cachés précisément dans ce but. Ça aide un peu de rendre le répertoire `incoming` illisible par les utilisateurs anonymes. Avec les serveurs FTP usuels, on ne peut pas empêcher la création de répertoires dans `incoming`. Le serveur ftp de WUarchive permet de limiter les dépôts à certains répertoires, et de mettre des restrictions sur les noms que l'on peut donner aux fichiers, comme par exemple:

```
# specify the upload directory information
upload  /var/spool/ftp  *       no
upload  /var/spool/ftp  /incoming       yes     ftp     staff   0600    nodirs

# path filters                                                                          # path-filter...
path-filter  anonymous  /etc/msgs/pathmsg  ^[-A-Za-z0-9_\.]*$  ^\.  ^-
path-filter  guest      /etc/msgs/pathmsg  ^[-A-Za-z0-9_\.]*$  ^\.  ^-
```

Suggestion : installez votre arborescence FTP (ou tout au moins la partie `incoming`) dans un système de fichiers à part. Ceci empêchera une *attaque paralysante* consistant à saturer complètement votre partition principale (via le répertoire `incoming`) avec des cochonneries.

Si vous avez `wuftpd` vous pourrez installer quelques extensions comme la compression-décompression *au vol*, ou la création de fichiers `tar` pour les arborescences. Récupérez les sources nécessaires (`gzip`, `gnutar`, `compress`), compilez-les avec une édition des liens *statique*, et éditez le fichier qui contient la définition des conversions autorisées. Le programme `/usr/bin/tar` est déjà lié statiquement. Vous préférerez probablement utiliser GNU-tar de toutes façons. Garry Mills a écrit le petit programme qui fait çà :

> J'ai pris `compress` sur `ftp.uu.net`, à la racine je crois, et je l'ai compilé. Pour `tar` et `compress`, j'ai écrit un petit programme appelé "`pipe`", que j'ai lié statiquement. Mon fichier `/etc/ftpconversions` ressemble à ceci :[1]

```
#strip prefix:strip postfix:addon prefix:addon postfix:external command:
#types:options:description
 :.Z:  :  :/bin/compress -d -c %s:T_REG|T_ASCII:O_UNCOMPRESS:UNCOMPRESS
 :-z:  :  :/bin/compress -d -c %s:T_REG|T_ASCII:O_UNCOMPRESS:UNCOMPRESS
 :  :  :.Z:/bin/compress -c %s:T_REG:O_COMPRESS:COMPRESS
 :  :  :.tar:/bin/tar cf - %s:T_REG|T_DIR:O_TAR:TAR
 :  :  :.tar.Z:/bin/pipe /bin/tar cf - %s | /bin/compress -c:T_REG|T_DI
R:O_COMPRESS|O_TAR:TAR+COMPRESS
 :  :  :.tar:/bin/gtar -c -f - %s:T_REG|T_DIR:O_TAR:TAR
 :  :  :.tar.Z:/bin/gtar -c -Z -f - %s:T_REG|T_DIR:O_COMPRESS|O_TAR:TAR
+COMPRESS
 :  :  :.tar.gz:/bin/gtar -c -z -f - %s:T_REG|T_DIR:O_COMPRESS|O_TAR:TA
R+GZIP
```

> Voilà le programme:

```
/* pipe.c: exec two commands in a pipe */

#define NULL (char *)0
#define MAXA 16

main(argc, argv) int argc; char *argv[]; {
    char *av1[MAXA], *av2[MAXA];
    int i, n, p[2], cpid;
    i = 0; n = 0;
    while ( ++i < argc && n < MAXA ) {
        if ( *argv[i] == '|' && *(argv[i]+1) == '\0' ) break;
        av1[n++] = argv[i];
    }
    if ( n == 0 ) uexit();
    av1[n] = NULL;
    n = 0;
    while ( ++i < argc && n < MAXA )
      av2[n++] = argv[i];
    if ( n == 0 ) uexit();
    av2[n] = NULL;
    if ( pipe(p) != 0 ) exit(1);
```

1. Note du traducteur: les 3 lignes qui ne commencent pas par deux-points ou dièse sont la continuation de celles qui les précèdent. J'ai dû les tronquer pour des raisons de formattage.

```
    if ( ( cpid = fork() ) == (-1) ) exit(1);
    else if ( cpid == 0 ) {
        (void)close(p[0]);
        (void)close(1);
        (void)dup(p[1]);
        (void)close(p[1]);
        (void)execv(av1[0], av1);
        _exit(127);
    }
    else {
        (void)close(p[1]);
        (void)close(0);
        (void)dup(p[0]);
        (void)close(p[0]);
        (void)execv(av2[0], av2);
        _exit(127);                                                                             }
    /*NOTREACHED*/
}

uexit() {
    (void)write(2, "Usage: pipe <command> | <command>\n", 34);
    exit(1);
}
```

9. Autres choses à faire :

   – Sous `root` créez des fichiers `.rhosts` et `.forward` vides, appartenant à `root`n en faisant par exemple

   ```
   touch ~ftp/.rhosts ~ftp/.forward
   chmod 400 ~ftp/.rhosts ~ftp/.forward
   ```

   – Prévoyez un alias de courrier pour que les utilisateurs puissent signaler leurs problèmes à l'administrateur FTP.

   – Si vous montez des disques d'autres machines (ou même de la vôtre) dans l'arborescence `ftp`, montez-les en lecture seulement. La ligne correcte dans `/etc/fstab` (sur la machine où tourne `ftpd`) ressemble à :

   ```
   other:/u1/linux /home/ftp/pub/linux nfs ro,noquota,nosuid,intr,bg 1 0
   ```

   Ceci monte le disque de la machine `other` sur le répertoire `/home/ftp/pub/linux` sans quotas, sans aucun programme à “suid” (on ne sait jamais), interruptible (pour le cas où `other` s'arrête), et en arrière-plan “`bg`”, pour que si vous redémarrez votre machine alors que `other` est arrêté, elle ne vous bloque pas en réessayant continuellement de monter `/home/ftp/pub/linux`.

2.2 Installation d'un serveur FTP sécurisé à racine déplacée

Note du traducteur : Il s'agit là des serveurs "chrooted FTP", c'est-à-dire qui ne montrent à tous les utilisateurs (pas seulement les anonymes) qu'une sous-arborescence volontairement limitée, dont la racine apparente *n'est pas* la vraie racine de la hiérarchie de fichiers.

Contribution de Marcus J. Ranum <`mjr@tis.com`>.

Etapes d'installation :

1. Faites une version de `ftpd` qui soit liée *statiquement*, et mettez dans `~ftp/bin`. Assurez-vous que `root` en est le propriétaire.
2. Si vous avez besoin de `/bin/ls`, faîtes-en une version *statique* également, que vous mettrez dans `~ftp/bin`. Il y a un portage de la commande `ls` de BSD net2 pour SunOs sur `ftp.tis.com` dans `pub/firewalls/toolkit/patches/ls.tar.Z` . Vérifiez que `root` en est propriétaire.
3. Remplissez `~ftp/etc/passwd` `~ftp/etc/group` comme vous le feriez normalement, **mais surtout** ne mettez pas la racine `/` comme répertoire d'accueil pour l'utilisateur `ftp`. Assurez-vous que ces deux fichiers appartiennent à `root`.
4. Écrivez un "lanceur" (wrapper) pour `ftpd` et installez-le dans `/etc/inetd.conf`. En supposant que `~ftp` = `/var/ftp`, le lanceur ressemble à ceci :

```
main()
{
        if(chdir("/var/ftp")) {
                perror("chdir /var/ftp");
                exit(1);
        }
        if(chroot("/var/ftp")) {
                perror("chroot /var/ftp");
                exit(1);
        }
        /* optional: seteuid(FTPUID); */
        execl("/bin/ftpd","ftpd","-l",(char *)0);
        perror("exec /bin/ftpd");
        exit(1);
}
```

Autres possibilités :

- Vous pouvez utiliser `netacl` de la boite à outils standard, ou des "tcp-wrappers" pour obtenir le même résultat.
- Nous utilisons `netacl` pour pouvoir activer/désactiver le confinement pour que quelques machines qui se connectent au service FTP **ne soient pas** confinées dès le début. Ceci rend le transfert de fichiers un peu moins pénible.

- Vous pouvez aussi modifier les sources de `ftpd` et enlever tous les appels à `seteuid()`. Ceux qui connaissent des trous de sécurité qui permettent de passer `root` n'y arriveront plus. Détendez-vous et imaginez combien ils vont être frustrés.
- Si vous bricolez les sources de `ftpd`, je vous recommande de désactiver un tas d'options dans `ftpcmd.y` en enlevant l'indicateur "`implemented`". Ça ne sera commode que si votre serveur FTP est destiné uniquement à la consultation.
- Comme d'habitude, faites un tour dans votre zone FTP, et vérifiez que les fichiers ont des droits convenables et que rien ne traîne qui puisse être exécuté.
- Notez que le fichier `/etc/passwd` de votre zone FTP est maintenant complètement séparé de votre vrai `/etc/passwd`. Il y a des avantages et des inconvénients.
- Certains programmes peuvent ne pas fonctionner, comme `syslog`, parce qu'il n'y a pas de `/dev/log`. Dans ce cas vous pouvez construire une version de `ftpd` avec une routine `syslog()` basée sur UDP, ou encore faire tourner un second `syslogd` reposant sur le code BSD Net2, qui avec l'option `-p ~ftp/dev/log` gèrera un socket *unix-domain*.

Rappellez-vous: si on peut passer `root` par une faille de votre `ftpd`, on peut vous causer des dégâts même sur un serveur à arborescence déplacée. Si vous n'avez pas peur de bricoler du code, s'arranger pour faire tourner `ftpd` sans permissions est une très bonne chose. Vous pouvez vérifier le bon fonctionnement de votre serveur bricolé en vous y connectant et (pendant qu'il en est à la chaîne d'invite utilisateur) en faisant un `ps-axu` pour voir s'il le tourne pas sous `root`.

2.3 Informations sécifiques au système d'exploitation et suggestions

2.3.1 Vieux systèmes SVR2 et SVR3, ...

... RTU6.0 (Masscomp, maintenant dénommée Concurrent Real Time UNIX), machines AT&T 3B1 et 3B2:

Ces systèmes peuvent avoir besoin de `dev/tcp`.

(dev/tcp) Ces implémentations de `ftpd` peuvent requérir un `~ftp/dev/tcp` en état de marche pour que le FTP anonyme fonctionne.

Il faut créer un fichier spécial en mode caractères avec les nombres majeur et mineur convenables. Les nombres convenables pour `~ftp/dev/tcp` sont ceux de `/dev/tcp`.

`~ftp/dev` est un répertoire, et `~ftp/dev/tcp` est un fichier spécial en mode caractères. Fixez-en le groupe et le propriétaire à `root`. Les droits d'accès de `~ftp/dev` sont lecture-écriture-exécution pour `root`, et lecture-exécution pour le groupe et les autres. Pour `~ftp/dev/tcp`, `root` aura le droit de lire et écrire, les autres et le groupe le droit de lire seulement.

2.3.2 HPUX

(Fichiers de trace) Si vous utilisez le `ftpd` de HP, la ligne de `/etc/inetd.conf` devrait lancer `ftpd -l`, qui fait des traces supplémentaires.

2.3.3 SunOs

(Bibliothèques) Pour que SunOs utilise ses bibliothèques dynamiques partagées, suivez ces étapes :

1. Créez le répertoire `~ftp/usr`. Le propriétaire est `root`, avec les droits `555`.
2. Créez le répertoire `~ftp/usr/lib`. Le propriétaire est `root`, avec les droits `555`.
3. Copiez le chargeur dynamique `ld.so` dans `~ftp/usr/lib` pour qu'il soit utilisable par `ls`. `ld.so` appartient à `root` avec les droits `555`.
4. Copiez la version la plus récente de la bibliothèque X partagée, (`libc.so.*`) dans `~ftp/usr/lib` pour qu'elle soit utilisée par `ls`. La copie `libc.so.*` appartiendra à `root` avec les droits `555`.

   Utilisateurs de 4.1.2 (ou au-delà) : il faut aussi copier `/usr/lib/libdl.so.*` dans `~ftp/lib`.
5. Créez le répertoire `~ftp/dev`. Propriétaire `root` et droits d'accès `111`.
6. Le chargeur a besoin de `~ftp/dev/zero`. Placez-vous dans le répertoire `~ftp/dev` et créez-le par la commande :

   ```
   mknod zero c 3 12
   ```

   transférez-en la propriété à `root`. Assurez-vous qu'il est lisible.

   > **Avertissement aux novices :** N'essayez pas de copier `/dev/zero` dans `~/ftp/dev/zero`!!! C'est un fichier sans fin de zeros et il va remplir complètement votre partition !
7. Si vous voulez que l'heure locale s'affiche quand les gens se connectent, créez le répertoire `~ftp/usr/share/lib/zoneinfo` et copiez-y `/usr/share/lib/zoneinfo/localtime`.
8. Si vous n'aimez pas l'idée de copier vos bibliothèques pour pouvoir utiliser le `ls` de Sun qui est lié dynamiquement, vous pouvez essayer de récupérer un `ls` statique à la place. Il y en a un sur le CD-ROM de distribution de SunOS. Dans ce cas vous pouvez vous dispenser des étapes 6 à 8. Si vous voulez un autre `ls` statique, récupérez `fileutils` de GNU sur un serveur d'archives proche et liez-le statiquement.

(Fichiers de trace) Le démon `ftpd` standard de Sun enregistre *tous* les mots de passe. Pour corriger ça, passez le patch :

```
101640-03     SunOS 4.1.3: in.ftpd logs password info when -d option is used.
```

Dans **/etc/inetd.conf** trouvez la ligne qui commence par `ftp`. La fin de la ligne qui devrait être "`in.ftpd`", remplacez-la par "`in.ftpd -dl`». Dans `/etc/syslog.conf`, ajoutez une ligne

```
daemon.*                                     /var/adm/daemonlog
```

L'information peut-être ventilée sur plusieurs fichiers, en faisant :

```
daemon.info                                 /var/adm/daemon.info
daemon.debug                                /var/adm/daemon.debug
daemon.err                                  /var/adm/daemon.err
```

Attention, l'espace entre les deux colonnes doit contenir au moins une tabulation, et pas seulement des espaces, sinon ça ne va pas marcher. Vous pouvez mettre vos fichiers de traces où vous voulez. Ensuite, créez les fichiers de traces (par exemple par `touch /var/adm/daemonlog`). Pour finir, relancez `inetd` et `syslogd`, soit manuellement, soit en démarrant le système. Ça devrait fonctionner.

Si vous n'installez pas le patch, assurez-vous que le fichier de traces appartient bien à `root` et qu'il a les droits `600`, parce que le démon `ftpd` enregistrera absolument tout, y compris les mots de passe des utilisateurs.

> Pour des raisons de sécurité les fichiers de traces ne doivent être lisibles que par `root` : si par erreur un utilisateur tape son mot de passe au lieu de son nom, il pourrait être piraté par quiconque peut lire les traces.

2.4 Où se procurer d'autres démons FTP ?

Wuarchive FTP 2.4 - Un démon FTP sécurisé qui améliore le contrôle d'accès, les fichiers de traces, les bannières d'avant-login, et offre de nombreuses options de configuration. Par `ftp` sur `ftp.uu.net` dans le répertoire `/networking/ftp/wuarchive-ftpd`. Vérifiez bien le checksum pour être sûr d'avoir chargé une copie valide. (**Avertissement** : les anciennes versions de `Wu-FTP` sont très vulnérables et certaines ont des chevaux de Troie.)

```
                   BSD        SVR4
File               Checksum   Checksum    MD5 Digital Signature
-----------------  --------   ---------   --------------------------------
wu-ftpd-2.4.tar.Z  38213  181  20337 362  cdcb237b71082fa23706429134d8c32e
patch_2.3-2.4.Z    09291    8  51092  16  5558a04d9da7cdb1113b158aff89be8f

For DECWRL ftpd, sites can obtain version 5.93 via anonymous FTP
from gatekeeper.dec.com in the "/pub/misc/vixie" directory.

                   BSD        SVR4
File               Checksum   Checksum    MD5 Digital Signature
-----------------  --------   --------- --------------------------------
ftpd.tar.gz        38443  60  1710 119  ae624eb607b4ee90e318b857e6573500

For BSDI systems, patch 005 should be applied to version 1.1 of
the BSD/386 software.  You can obtain the patch file via
anonymous FTP from ftp.bsdi.com in the "/bsdi/patches-1.1"
directory.

                   BSD        SVR4
File               Checksum   Checksum    MD5 Digital Signature
-----------------  --------   ---------   --------------------------------
BU110-005          35337 272  54935 543   1f454d4d9d3e1397d1eff0432bd383cf
```

Sources dans le domaine public :

```
ftp.uu.net            ~ftp/systems/unix/bsd-sources/libexec/ftpd
gatekeeper.dec.com    ~ftp/pub/DEC/gwtools/ftpd.tar.Z
```

2.5 Comment savoir si votre serveur FTP anonyme est sécurisé

Cette section offre à l'administrateur une petite liste de points à vérifier pour vérifier que son serveur n'est pas trop facile à fracturer.

1. Vérifiez que votre serveur n'a pas la commande `SITE EXEC` en vous connectant par `telnet` sur le port 21 et en tapant "`SITE EXEC`". Si votre démon FTP accepte cette commande, vérifiez qu'il est dans sa version la plus récente (c'est-à-dire `Wu-FTP 2.4`). Dans les versions plus anciennes, la commande permet à n'importe qui d'exécuter un shell par le port 21.

2. Vérifiez que personne ne peut se connecter et créer des fichiers et des répertoires dans le répertoire principale. Si n'importe qui peut se connecter sous `anonymous` et créer des fichiers `.rhosts`, et `.forward`, l'accès est alors ouvert à tout intrus.

3. Vérifiez que le répertoire principal **n'appartient pas** à `ftp`. Sinon un intrus peut faire "`SITE CHMOD 777`" sur le répertoire principal et installer des fichiers qui lui donneront immédiatement un accès. La commande `SITE CHMOD` devrait être supprimée parce que les utilisateurs anonymes n'ont besoin d'aucun privilège particulier.

4. Vérifier qu'**aucun** fichier ou répertoire n'appartient à `ftp`. Si c'etait le cas, un intrus pourrait les remplacer par un cheval de Troie.

5. Il y a plusieurs erreurs dans les vieux démons, il est donc très important de vous assurer que vous avez les versions les plus récentes.

2.6 Archie

Recherche des programmes dans les sites FTP. Connectez-vous à ces sites sous le nom `archie` ou utilisez un client Archie pour un accès plus rapide. Pour faire ajouter votre site dans la liste des serveurs explorés par Archie, envoyez un courrier électronique à `archie-updates@bunyip.com`.

```
archie.ac.il               132.65.20.254    (Israel server)
archie.ans.net             147.225.1.10     (ANS server, NY (USA))
archie.au                  139.130.4.6      (Australian Server)
archie.doc.ic.ac.uk        146.169.11.3     (United Kingdom Server)
archie.edvz.uni-linz.ac.at 140.78.3.8       (Austrian Server)
archie.funet.fi            128.214.6.102    (Finnish Server)
archie.internic.net        198.49.45.10     (ATT server, NY (USA))
archie.kr                  128.134.1.1      (Korean Server)
archie.kuis.kyoto-u.ac.jp  130.54.20.1      (Japanese Server)
```

archie.luth.se	130.240.18.4	(Swedish Server)
archie.ncu.edu.tw	140.115.19.24	(Taiwanese server)
archie.nz	130.195.9.4	(New Zealand server)
archie.rediris.es	130.206.1.2	(Spanish Server)
archie.rutgers.edu	128.6.18.15	(Rutgers University (USA))
archie.sogang.ac.kr	163.239.1.11	(Korean Server)
archie.sura.net	128.167.254.195	(SURAnet server MD (USA))
archie.sura.net(1526)	128.167.254.195	(SURAnet alt. MD (USA))
archie.switch.ch	130.59.1.40	(Swiss Server)
archie.th-darmstadt.de	130.83.22.60	(German Server)
archie.unipi.it	131.114.21.10	(Italian Server)
archie.univie.ac.at	131.130.1.23	(Austrian Server)
archie.unl.edu	129.93.1.14	(U. of Nebraska, Lincoln (USA))
archie.uqam.ca	132.208.250.10	(Canadian Server)
archie.wide.ad.jp	133.4.3.6	(Japanese Server)

3 Remerciements

Merci à toutes les personnes suivantes, dont les suggestions ont aidé à réaliser cette FAQ :

Tomasz Surmacz (tsurmacz@asic.ict.pwr.wroc.pl)
Wolfgang Ley (Ley@rz.tu-clausthal.de)
Russel Street (russells@ccu1.auckland.ac.nz)
Gary Mills (mills@CC.UManitoba.CA)
Nicholas Ironmonger (ndi@sam.math.ethz.ch)
Morten Welinder (terra@diku.dk)
Nick Christenson (npc@minotaur.jpl.nasa.gov)
Mark Hanning-Lee (markhl@romoe.caltech.edu)
Marcus J Ranum <mjr@tis.com>

4 Copyright

5 Dénégation de responsabilités

Les informations contenues dans ce document peuvent changer sans préavis. Elles sont présentées *en l'état*, et leur utilisation constitue une acceptation de cette condition. Elles ne sont nullement garanties. En aucun cas l'auteur ou le traducteur ne pourront être tenus responsables des dommages pouvant résulter directement ou indirectement de l'usage ou de la diffusion de ces informations. Tout usage se fait aux risques de l'utilisateur lui-même.

6 Adresse de l'auteur

Vous pouvez envoyer vos suggestions, mise-à-jour et commentaires à


```
Christopher Klaus <cklaus@shadow.net>
Internet Security Systems, Inc. <iss@shadow.net>
Internet Security Systems, Inc.
2209 Summit Place Drive,
Atlanta,GA 30350-2430. (404)998-5871.
```