e-securIT

[Sécuriser l'exécution de BIND]

http://securit.free.fr

[securIT@free.fr]

TABLE DES MATIÈRES

1. INSTALLATION DE BIND

1.1. VERSION DE BIND

BIND, au même titre que Sendmail, est un programme complexe qui a laissé apparaître, au cours des nombreuses années de son utilisation, beaucoup de failles de sécurité (liées également à DNS). Il est donc essentiel de toujours utiliser des versions récentes et/ou des patchs à jour afin d'éliminer le risque de compromission par l'exploitation d'une faille ancienne.

Les dernières versions de BIND sont disponibles directement sur le Web :

http://www.isc.org/products/BIND/

A ce jour, il convient d'utiliser la version 9.1 de BIND.

ftp://ftp.isc.org/isc/bind9/9.1.0/bind-9.1.0.tar.gz

1.2. INSTALLATION DE BIND

Pour installer BIND, se référer au guide d'installation.

Si BIND est installé sur une distribution Redhat 6.2 ou ultérieure (voire Mandrake), se référer au chapitre "Linux DNS and BIND Server" du très bon document "Securing and optimizing Redhat Linux 1.3" de Gerhard Mourani :

http://securit.free.fr/ressources/Securing-Optimizing-Linux-RH-Edition-1_3.pdf

2. SÉCURISER L'EXÉCUTION DE BIND

2.1. EXÉCUTION DE BIND SANS DROIT ROOT

BIND est parfois (dans les versions moins récentes) exécuté avec des droits root, afin d'utiliser le port privilégié 53 (TCP, UDP), inférieur à 1024.

Cependant, depuis la version 8.1.2, le démon named de BIND peut être configuré pour s'exécuter avec une identité différente de root.

Remarque : par défaut, dans les versions récentes (ex. : sous les distributions classiques de Linux), BIND est exécuté avec l'utilisateur named appartenant au groupe named.

2.1.1. Pourquoi exécuter BIND sous une identité différente de root ?

De par sa complexité, BIND est vulnérable à un certain nombre de failles de sécurité exploitables par des pirates. Il est donc essentiel de protéger le système hébergeant le service de résolution de noms de toute attaque potentielle.

Lorsque BIND est exécuté en mode root, un pirate exploitant une faille de sécurité peut obtenir rapidement un accès total au système hébergeur.

Dans le cas où BIND est exécuté avec des droits restreints, le pirate ne pourra pas compromettre l'intégralité du système et sera restreint aux droits attribués à l'utilisateur exécutant named.

2.1.2. Comment configurer BIND pour s'exécuter sans droit root ?

2 étapes sont nécessaires à l'exécution de BIND sous une identité distincte de root.

2.1.2.1. Étape 1 : création du compte d'exécution et mise en place des permissions

Il convient de créer en premier lieu le compte de service utilisé par BIND pour s'exécuter, et de fixer les droits adéquats sur les fichiers et répertoires utilisés par BIND :

- Créer un utilisateur "dns" dans le fichier /etc/passwd et un groupe "dns" dans le fichier /etc/group.
- Utiliser des identificateurs d'utilisateur et de groupe (UID : user-id, GID : group-id) non-présents sur le système.
- L'utilisateur "dns" ne doit pas disposer de shell (/bin/false comme shell) et son compte doit être désactivé (* dans le champs password), soit une ligne de la forme suivante dans le fichier /etc/passwd :

```
dns:*:uid:gid:Compte de service BIND:/home/dns:/bin/false
```

Et dans le fichier /etc/group :

```
dns:x:gid
```

Remarque : pour les utilisateurs de système Linux, les commandes useradd et groupadd permettent de créer respectivement l'utilisateur dns et le groupe dns. Voici un exemple dans lequel UID et GID sont fixés à 53 :

```
useradd -c "DNS User" -u 53 -g 53 -s /bin/false -r -d /home/dns dns
groupadd -g 53 dns
```

Si les mots de passe sont sécurisés avec shadow, ajouter * dans le champs password de /etc/shadow (le champs password de /etc/passwd présente un "x").

- Créer et disposer des droits restreints sur le répertoire de base de l'utilisateur dns :

```
mkdir -m 700 /home/dns
chown dns:dns /home/dns
```

2.1.2.2. Étape 2 : lancer BIND sans l'identité root

Le service named doit être lancé avec l'utilisateur dns créé précédemment. Pour cela, modifier le fichier de configuration du démon named (ex. sous Linux /etc/rc.d/init.d/named) en remplaçant la ligne :

```
daemon named
```

Par :

```
daemon named -u dns -g dns
```

Puis relancer le démon :

```
/etc/rc.d/init.d/named restart
```

2.1.2.3. Alternative : lancer BIND depuis Inetd

Une alternative intéressante, bien que non conseillée ;-), consiste à lancer BIND non pas en tant que démon, mais au travers du super-démon Inetd.

En particulier, cela permet d'utiliser TCP Wrappers, le célèbre paquetage édité et maintenu par Wietse Venema permettant d'effectuer un contrôle et un filtrage au niveau réseau sur les connexions faites sur un système :

http://securit.free.fr/tools/unix/nettools/tcp_wrappers/

Dans le cas où BIND est lancer via Inetd, il devient possible de contrôler les connexions sur le DNS par adresse IP, nom de machine ou nom de domaine.

Pour lancer le service named non plus comme démon, mais via inetd (le super-démon), il convient d'effectuer les étapes suivantes (exemple donné pour Linux).

a) Ajouter les lignes suivantes dans le fichier /etc/inetd.conf :

```
name dgram udp wait dns /usr/sbin/tcpd named
name stream tcp wait dns /usr/sbin/tcpd named
```

b) Arrêter le démon named :

```
/etc/rc.d/init.d/named stop
```

Veiller à ne plus permettre à named de démarrer en tant que démon, par exemple (sous Linux) :

```
chkconfig --del named
```

c) Relancer le super-démon inetd :

```
/etc/rc.d/init.d/inet restart
```

2.2. EXÉCUTER BIND DANS UN ENVIRONNEMENT CONFINÉ

Exécuter BIND dans un environnement confiné consiste à utiliser chroot pour définir un espace d'exécution isolé dédié à named.

Pour obtenir un niveau de sécurité et d'efficacité optimum, **toujours accompagné l'exécution de BIND dans un environnement confiné (chroot) par un changement d'identité.** En effet, l'utilisateur root est capable de sortir de la prison imposée par chroot, ce qui en réduit considérablement l'intérêt d'un point de vue sécurité.

Remarque : de manière générale, lorsqu'une application est emprisonnée par chroot, ne jamais l'exécuter sous root !

Les étapes décrites ci-après pour "chroot-er" BIND dans un environnement Linux sont extraites du document "Securing and optimizing Redhat Linux 1.3" de Gerhard Mourani et du document "Chroot-BIND-HOWTO" :

http://securit.free.fr/ressources/Securing-Optimizing-Linux-RH-Edition-1_3.pdf

http://securit.free.fr/ressources/Chroot-BIND-HOWTO.pdf

2.2.1. Librairies partagées de named

Il est nécessaire de connaître les librairies utilisées par le démon named :

```
ldd /usr/sbin/named
libc.so.6 => /lib/libc.so.6 (0x4001c000)
/lib/ld-linux.so.2 => /lib/ld-linux.so.é (0x40000000)
```

2.2.2. Construction de l'environnement chroot

Une partition spécifique, /chroot, est normalement attribuée pour recevoir les environnements restreints, en dehors des partitions utilisées par le système.

Cette partition doit être créée à l'installation du système !

Les répertoires suivants doivent être créés :

```
mkdir -p /chroot/named
mkdir /chroot/named/dev
mkdir /chroot/named/lib
mkdir /chroot/named/etc
mkdir -p /chroot/named/usr/sbin
mkdir -p /chroot/named/var/run
mkdir /chroot/named/var/named
```

Si un démon named est lancé, il convient de l'arrêter :

```
/etc/rc.d/init.d/named stop
```

2.2.3. Copie des fichiers dans l'environnement chroot

Dans un premier temps, les fichiers de configuration doivent être copiés :

```
cp /etc/named.conf /chroot/named/etc
cp -a /var/named /chroot/named/var/named
mknod /chroot/named/bin/false c 1 3
chmod 666 /chroot/named/bin/false
cp /usr/sbin/named /chroot/named/usr/sbin
cp /usr/sbin/named-xfer /chroot/named/usr/sbin
```

Attention : le propriétaire du répertoire /chroot/named/var/named (et tous les fichiers dans ce répertoire) doit être l'utilisateur choisi pour exécuter named. Dans notre cas, nous allons reprendre l'utilisateur choisi précédemment : dns.

```
chown -R dns:dns /chroot/named/var/named
```

Remarque : l'utilisateur dns devra avoir pour répertoire de base /chroot/named (cf. étape 4 pour la création de l'utilisateur dns).

Il est ensuite nécessaire de copier les librairies partagées identifiées à l'étape 1 :

```
cp /lib/libc.so.6 /chroot/named/lib
cp /lib/ld-linux.so.2 /chroot/named/lib
```

Puis copier les fichiers nécessaires à l'horodatage correct des messages de log :

```
cp /etc/localtime/ /chroot/named/etc/
cp /etc/nsswitch.conf /chroot/named/etc/
```

Certains fichiers critiques ne doivent pas pouvoir être modifiés, renommés ou effacés de manière inopportune :

```
chattr +i /chroot/named/etc/nsswitch.conf
chattr +i /chroot/named/etc/named.conf
```

2.2.4. Création du compte de service utilisé pour l'exécution de named

Comme nous l'avons vu précédemment, il convient de créer le compte et le groupe utilisé par named pour s'exécuter. Pour cela, nous allons procéder de la même manière que dans la partie II.1. de ce document.

Nous avons ici choisi d'utiliser un utilisateur nommé dns et un group dns. Il convient de sélectionner un UID et un GID non déjà utilisés, par exemple 53 :-)

Vérifier cela en observant le contenu des fichiers /etc/passwd et /etc/group.

La création de l'utilisateur et du groupe doit ensuite être effectuée :

```
useradd -c "DNS User" -u 53 -g 53 -s /bin/false -r -d /chroot/named dns
groupadd -g 53 dns
```

Comme précédemment, l'utilisateur dns ne doit pas pouvoir ouvrir de session sur le serveur et donc ne pas disposer de mot de passe (remplacement du caractère !! par * dans le champ password du fichier /etc/shadow).

2.2.5. Re-direction des messages de logs

Il est nécessaire de préciser au démon syslog d'écouter les logs produits par named dans son nouvel environnement.

Dans le fichier de configuration de syslog (/etc/rc.d/init.d/syslog), remplacer la ligne :

```
daemon syslog -m 0
```

Par la ligne :

```
daemon syslog -m 0 -a /chroot/named/dev/log
```

Relancer ensuite le démon syslog :

```
/etc/rc.d/init.d/syslog restart
```

2.2.6. Configuration du démon named

Il est nécessaire de modifier le script de lancement du démon named afin de prendre en compte le nouvel environnement. Dans le fichier /etc/rc.d/init.d/named, modifier les lignes suivantes :

CONTENU ORIGINEL	LIGNE MODIFIÉE
[-f /usr/sbin/named] || exit 0	[-f /chroot/named/usr/sbin/named] || exit 0
[-f /etc/named.conf] || exit 0	[-f /chroot/named/etc/named.conf] || exit 0
daemon named	daemon /chroot/named/usr/sbin/named -t /chroot/named/ -u dns -g dns

Les options -u et -g précisent à BIND respectivement l'utilisateur et le groupe qu'il doit utiliser pour s'exécuter.
L'option -t force BIND à s'exécuter dans la prison que nous venons de construire.

2.2.7. Modification du ndc

A partir de la version BIND 8.2, ndc (name daemon control) n'est plus un script mais un programme. Il convient de le recompiler afin de prendre en compte les modifications opérées.

Il faut alors effectuer les opérations suivantes (ex. donné pour un système Linux) :

```
cp bind-src.tar.gz /var/tmp ; cd /var/tmp
tar xzpf bind-src.tar.gz
cd src ; cp port/linux/Makefile.set port/linux/Makefile.set-orig
cd port/linux/
```

Éditer le fichier Makefile.set et modifier les variables suivantes en précisant l'environnement chrooté :

```
'DESTSBIN=/chroot/named/usr/sbin'
'DESTEXEC=/chroot/named/usr/sbin'
'DESTRUN=/chroot/named/var/run'
'DESTLIB=/usr/lib/bind/lib'
'DESTINC=/usr/lib/bind/include'
```

Recompiler alors le programme ndc :

```
cd /var/tmp/src ; make clean
make
cp bin/ndc/ndc /usr/sbin/
cp: overwrite 'usr/sbin/ndc'? y
strip /usr/sbin/ndc
```

2.2.8. Un peu de nettoyage

Effacer les fichiers et répertoires inutiles :

```
rm -f /usr/sbin/named
rm -f /usr/sbin/named-xfer
rm -f /etc/named.conf
rm -rf /var/named/
```

2.2.9. Lancement de named

Il est maintenant possible de lancer named dans son environnement restreint :

/etc/rc.d/init.d/named start

Priez... Puis vérifier alors que named est démarré et fonctionne correctement et qu'il s'exécute sous l'identité choisie (i.e. : dns) :

ps auxw | grep named
named [....] /chroot/named/usr/sbin/named -t /chroot/named/ -u dns -g
dns

2.3. RÉFÉRENCES

Quelques références :

- "Securing and optimizing Redhat Linux 1.3" - Gerhard Mourani : http://securit.free.fr/ressources/Securing-Optimizing-Linux-RH-Edition-1_3.pdf
- "Chroot-BIND-HOWTO" : http://securit.free.fr/ressources/Chroot-BIND-HOWTO.pdf

*****
***
*