Installation de la CSonde

CSONE

Julien VAUBOURG

12 juin 2009

CS One - 42 avenue Montaigne 75008 Paris
Cabinet de consultants en architectures réseaux, sécurité et téléphonie IP

Table des matières

1 Présentation **3**

2 Installation de la CSonde **3**
2.1 Installation du système . . . 3
2.2 Configuration de la CSonde . . . 4

3 Patch et mise à jour du noyau **4**
3.1 Compilation . . . 4
3.2 Installation . . . 5
3.2.1 Le noyau . . . 5
3.2.2 La librairie pcap . . . 5
3.2.3 Configuration de GRUB . . . 6

4 Optimisations **6**
4.1 GRUB . . . 6
4.2 Le BIOS . . . 6

1 Présentation

La CSonde est un outils qui permet de récolter les paquets d'un réseau donné. Elle est installée sur une machine de même type que les PSM Box (mais avec 512Mo de RAM, un pentium IV 2.40GHz et une carte ethernet Gigabit) et utilise un environnement GNU/Debian minimaliste plutôt que l'environnement des PSM. Le noyau est patché avec PF_RING pour accélerer la vitesse de capture des paquets. La capture se fait grâce à tcpdump (un sniffeur qui utilise la librairie pcap) qui écrit les paquets dans un ensemble de fichiers binaires (d'une taille de 1Go chacun maximum, selon les options définies à son appel dans le fichier du service) dans le dossier ***/home/sonde/dumps***. Ces fichiers sont préfixés avec `dump` suivi du timestamp unix du moment auquel il a été créé, d'un underscore et d'un numéro qui s'incrémente à chaque nouveau fichier (donc à chaque nouveau giga entamé).

Ils sont lisibles avec la commande :

```
tcpdump -vSNn -tt -r dumpXXXXXX_X tcp or udp
```

Détails des options :

1. -v : Uniquement les entêtes des paquets
2. -N : Ne jamais convertir des fragments d'IP en domaines
3. -S : Valeurs absolues
4. -n : Ne jamais convertir les IP en nom de domaine (qui ne seront donc visibles que dans les requêtes DNS)
5. -tt : Dates en timestamps UNIX (epoch)
6. -r : Capturer à partir du fichier de capture indiqué
7. tcp or udp : Filtrage des paquets par protocoles

2 Installation de la CSonde

2.1 Installation du système

Pour un gain de temps conséquent, il est conseillé de commencer par lancer la compilation du noyau (premier chapitre de la section suivante) avant toutes choses.

La version de Debian utilisée pour l'écriture de cette documentation est la version Lenny 5.0

Récupérer une version de Debian et l'installer sur le disque entier (partitionnement assisté). N'installer que le système de base : autrement dit, décochez toutes les cases lorsque l'installateur vous demande ce qu'il doit installer (y compris Système standard).

Une fois le système installé et que vous vous êtes loggué en root, commencez par supprimer l'utilisateur que Debian vous a demandé de créer :

```
deluser nom
```

Assurez-vous que internet fonctionne (configurez la passerelle) et faîtes une mise à jour :

```
apt-get update apt-get dist-upgrade
```

Puis lancez l'installation des paquets utiles :

```
apt-get install ssh tcpdump rrdtool psmisc openjdk-6-jre xserver-org ttf-freefont
imagemagick apache2 build-essential
```

Justifications utiles :

1. ssh : Connexion à distance sur la CSonde
2. tcpdump : Le sniffeur qui capturera les paquets
3. rrdtool : Utilitaire indispensable à la création et l'exploitation des bases RRD que nous utiliserons
4. psmisc : Pour avoir le killall utilisé dans le service
5. openjdk-6-jre : Un script en java est utilisé pour la génération des camemberts
6. xserver-xorg et ttf-freefont : Ce même script nécessite un DISPLAY configuré
7. imagemagick : Utilisation de convert pour réduire les images des camemberts

8. apache2 : Serveur web utilisé pour l'interface de configuration
9. build-essential : Bien que nous compilerons un maximum de choses sur le serveur de développement pour un gain de temps, le nécessaire pour compiler sera requis pour la compilation de la librairie pcap qui ne pourra se faire que sur un système disposant du noyau patché avec PF_RING

2.2 Configuration de la CSonde

Copiez l'archive ***sonde.tar.gz*** à la racine de la sonde, et décompressez-là :

```
tar -xzvf sonde.tar.gz
```

Ce qui aura pour effet d'ajouter :

1. ***/home/sonde/*** : Dossier des dumps créés par tcpdump, des bases de RRD, des scripts perl de génération des rapports et des librairies perl
2. ***/home/httpd/*** : Dossier de l'interface web, accessible depuis l'adresse IP de la sonde
3. ***/usr/share/texmf-texlive/tex/latex/PSM/*** : Dossier de quelques fonctions LaTeX qui serviront lors de l'édition du rapport en PDF
4. ***/etc/init.d/sonde*** : Le service qui sera lancé au démarrage et qui servira à contrôler régulièrement si la sonde capture toujours
5. ***/root/.bash_profile*** : Lancement du serveur X au login de root et configuration de $DISPLAY

Mise à jour de l'aborescence des fichiers de LaTeX :

```
mktexlsr
```

Afin d'activer la capture des paquets dés le démarrage du système, ajoutez le service aux services par défauts :

```
update-rc.d sonde defaults
```

Pour que le système vérifie toutes les 5 minutes si la sonde capture toujours, et éventuellement la relance, faîtes :

```
crontab -e
```

Et ajoutez dans le fichier :

```
*/5 * * * * /etc/init.d/sonde restartif > /var/log/sonde.log 2>&1
```

Quittez en enregistrant.

3 Patch et mise à jour du noyau

3.1 Compilation

La compilation se fera sur le serveur de dév plutôt que sur la sonde, histoire de gagner du temps et un processeur.

Sur le serveur de dév, n'importe où, récupérez les sources de PF_RING avec la commande :

```
svn co https://svn.ntop.org/svn/ntop/trunk/PF_RING
```

Si svn n'est pas installé, exécuter :

```
apt-get install subversion-tools
```

Déplacez-vous dans le dossier fraîchement téléchargé :

```
cd PF_RING
```

Puis éditez le fichier ***mkinstall.sh*** et répérez les lignes suivantes :

```
VERSION=${VERSION:-2}
PATCHLEVEL=${PATCHLEVEL:-6}
SUBLEVEL=${SUBLEVEL:-29.4}
```

Dans cet exemple, le fichier est configuré pour utiliser un noyau 2.6.29.4 (la version installée pour l'écriture de cette doc). Rendez-vous sur kernel.org et renseignez-y la dernière version stable actuelle.

Exécutez le script, qui ira télécharger les sources du noyau indiqué :

```
./mkinstall.sh
```

Une fois le téléchargement abouti, rendez-vous dans ***workspace/linux-{VERSION}-1-686-smp-PF_RING***. Afin de générer le fichier ***.config***, exécutez :

```
make menuconfig
```

Si ça ne fonctionne pas, vous devez peut-être installer de quoi compiler :

```
apt-get install build-essential libncurses5-dev
```

Attention à la version de libncurses (utilisez `apt-cache search libncurses` pour connaître la version actuelle).

Une fois le menu affiché, contentez-vous de quitter en faisant `exit` puis `Yes`.

Vous pouvez ensuite passer à la compilation du noyau et de ses modules :

```
make && make modules
```

Cette opération peut prendre plusieurs heures.

3.2 Installation

3.2.1 Le noyau

Si un probléme survient pendant le `./configure` au sujet de flex, installez la dernière version de flex sur le serveur de développement :

```
apt-get install flex
```

Depuis le serveur de dév, envoyez le dossier du noyau et des sources de la libraire pcap sur la sonde :

```
scp -r userland/libpcap-{VERSION}-ring root@{IP DE LA SONDE}:/root
scp -r workspace/linux-{VERSION}-1-686-smp-PF_RING root@{IP DE LA SONDE}:/usr/src
```

Quittons le serveur de dév, et en route pour la sonde, avec un premier :

```
cd /usr/src
```

Il s'agit dans un premier temps de créer un traditionnel lien symbolique `linux` vers les sources du futur noyau :

```
ln -s linux-{VERSION}-1-686-smp-PF_RING linux
cd linux
```

Il est temps d'installer tous ces binaires :

```
make install && make install_modules
```

Il faut à présent créer le fichier initrd correspondant à la version du noyau qui vient d'être installé :

```
update-initramfs -c -k {VERSION}
```

3.2.2 La librairie pcap

Pour profiter des optimisations de PF_RING, la librairie pcap qui capture les paquets pour tcpdump doit être recompilée.

Changeons de répertoire :

```
cd /root/libpcap-{VERSION}-ring
```

Il faut que PF_RING soit installé pour compiler la sonde, nous sommes donc contraint de le faire directement ici.

Il faudra donc quelques outils supplémentaires :

```
apt-get install flex byacc
```

Compilez et installez :

```
./configure
make
make install
```

Vous pouvez ensuite supprimer le dossier dans lequel vous étiez.

3.2.3 Configuration de GRUB

Dernière étape, la modification du fichier de menu de grub pour que la sonde démarre sur le nouveau noyau.

Editez le fichier ***/boot/grub/menu.lst*** et ajoutez-y vers la fin, au dessus des autres :

```
title CSonde (Debian GNU/Linux, kernel {VERSION}_PF-RING)
root (hd0,0)
kernel /boot/vmlinuz-{VERSION}root=/dev/sda1 ro quiet
initrd /boot/initrd.img-{VERSION}
```

Vérifier dans le fichier ***/etc/fstab*** que les disques sont bien pointés avec `/dev/sdaX` et non `/dev/hdaX`, sinon modifier.

Rebooter la machine et la laisser booter sur le nouveau noyau.

4 Optimisations

4.1 GRUB

Pour que le système démarre plus rapidement, modifiez ***/boot/grub/menu.lst***, repérez :

```
timeout 5
```

Et remplacez le 5 par 0 pour ne plus avoir l'affichage du menu de grub au démarrage.

4.2 Le BIOS

Dans le BIOS (`Suppr` au démarrage), modifiez les options comme ceci :

```
Standard CMOS Features > Halt On > No Error
Integrated Peripherals > PWRON After PWR-Fail > On
Integrated Peripherals > USB Controller > Disabled
Set user password
```

Respectivement, le système pourra alors démarrer sans clavier, il se relancera tout seul si une coupure de courant intervient, les USB seront désactivés et le BIOS sera protégé par mot de passe.