Licence Professionnel ASRALL
Projet tuteuré.

Ufwi

Sommaire

1

Introduction

Début du doc de Ufwi

2

Liste des solutions de pare-feu par identification

Les pare-feu par identification les plus connus :

- AuthPF : Fonctionne sous OpenBSD et qui se repose sur SSH pour l'identification des utilisateurs : http ://www.openbsd.org/faq/pf/authpf.html
- NuFW : projet ayant donné naissance à UFWI suite à la liquiditation de l'éditeur "EdenWall Technologies"
- Cyberoam : pare-feu entièrement basé sur l'identification, en utilisant une corrélation entre adresse MAC et utilisateur : http ://www.cyberoam.com/fr/firewall.html
- CheckPoint (NAC Blade) : utilisation des règles de filtrage en fonction d'une authentifcation basée sur Kerberos, l'identité de son poste et du niveau de sécurité du poste (mise à jour de sécurité / antivirus) : http ://www.cyberoam.com/fr/firewall.html

3

Externalisation des logs dans une BD MySQL

Configuration du serveur BD
Installation des paquets :
apt-get install apache2 php5 mysql-server nulog
Configuration de la passerelle :
Configuration IP :
ifconfig eth0192.168.1.137/24 ifconfig eth1172.20.8.1/24
Installation des paquets :
apt-get install ulogd ulogd-mysql
Correction d'un bug : ajout d'une ligne dans le script de démarrage qui va charger un module
nano /etc/init.d/ulogd export $LD_PRELOAD = /usr/lib/libmysqlclient.so.16$
Configuration de ulogd : modification de son fichier de configuration
nano /etc/ulogd.conf
Décommenter la ligne 46 (pour charger un module supplémentaire)
Renseigner les informations de connexion à la base de données :
paragraphe «[MYSQL]» ligne 59 : table="ulog" pass="passulog" user="ulog" db="ulog" host="172.20.8.2"
Configuration du serveur de BD :
Configuration IP :
ifconfig eth0172.20.8.2/24
Lister tous les fichiers installés à l'installation de nulog :
dpkg –L nulog | more
Ouvrir le fichier suvant (démarche à suivre pour creer les tables de la base de données)
nano /usr/share/doc/nulog/README.Debian
Connexion à la base de données et création de l'utilisateur(les deux programmes vont se connecter avec ce compte) :
mysql –u root –p create database ulog ; create user 'ulog'@'%' identified by 'passulog' ; grant all privileges on ulog.* to ulog ; exit
Commandes de création de la base :
cd /usr/share/doc/nulog/scripts gunzip ipv4.sql.gz cat ipv4.sql | mysql –uulog –p ulog
Modification du fichier de configuration de mysql
nano /etc/mysql//my.cnf ligne 47
Il faut qu'il écoute sur l'interface 172.20.8.2
bind address= ''172.20.8.2"

Renommer les fichiers de configuration :

cd /etc/nulog cp default. core.conf core.conf cp default.nulog.conf nulog.conf cp default.wrapper.conf wrapper.conf

Renseigner les informations de connexion à la base de données :

nano core.conf host=localhost db=ulog user=ulog password=passulog table=ulog

Prise en compte des changements : redémarrage de services Sur la passerelle :

/etc/init.d/ulogd restart

Sur le serveur :

/etc/init.d/ulogd restart

On choisit ce que l'on veut logueravec iptables