Diplôme	Micro-ordinateur et Réseau, Installation et Maintenance
Compétences visées	Sécurité internet/intranet, Mise en oeuvre de la sécurité WEB, Services réseau TCP/IP.
Connaissances associés	Les logiciels (S12), Sécurisation des données (S13), Supervision de réseau (S31),

Savoir installer et maintenir une DMZ

Préambule : le propos de ce cours n'est pas d'expliquer comment installer une dmz dans une configuration précise; il est applicable à une entreprise, une administration, etc...;

I. Définition – Objectifs

Une DMZ (anglais : De-Militarized Zone), ou "zone dé-militarisée"[#] est une partie du réseau local dont l'objectif est d'être accessible depuis l'extérieur du réseau local, avec ou sans authentification préalable. En effet, pour des raisons à la fois techniques et stratégiques, les réseaux IP locaux (LAN) sont (paradoxalement) devenus des zones inaccessibles depuis internet !!

Pourquoi nos ordinateurs sont-ils inaccessibles depuis internet ?

Une des raisons du problème réside dans le fait que la pénurie d'adresses IP nous amène à utiliser, pour les machines du LAN, des adresses dites "privées". Ces adresses ne doivent jamais être routées par la passerelle du LAN (c'est la norme), et sont donc déconnectées d' Internet.

Évidemment, du point de vue de la sécurité, cela peut sembler être un "plus" (pour vivre heureux... vivons cachés!); Cependant, la raison même de l'existence des réseaux est de faire communiquer les machines, pas de les isoler (ou alors achetons-nous des machines à écrire!...). Nous allons donc soit acheter une adresse publique supplémentaire, soit utiliser une astuce[*] au niveau de la passerelle pour qu'au moins un des serveurs du LAN possède une identité sur Internet

[#] le mot dé-militarisé fait allusion au fait que le contrôle des utilisateurs est moins strict que dans le réseau local, voire inexistant.

[*] cette astuce consiste à rediriger toutes les requêtes arrivant sur l'adresse publique de la passerelle vers une adresse privée du réseau local (LAN), technique dite de "translation d'adresse" (NAT)

II. La sécurité

L'installation de la DMZ ne pose pas de problème de sécurité intrinsèque : en effet, toutes ses communications sont contrôlées et autorisées par le firewall de la passerelle. Les problèmes de sécurité sont donc en grande partie gérés en amont... D'autre part, l'utilisation du NAT rend très mal-aisé (souvent impossible) l'accès direct à la DMZ par un éventuel pirate.

Il reste des problèmes de sécurité spécifiques aux serveurs :

- Le déni de service (**DOS**) : en surchargeant votre serveur de requêtes, le pirate provoque un plantage
- les "**exploits**" : en profitant d'un "défaut" dans la programmation du logiciel, le pirate le fait planter et récupère un shell ou exécute une commande de son choix, en général l'installation d'un "rootkit"

Les précautions de base pour s'en prémunir :

- le firewall détecte et bloque les tentatives de DOS

- la mise à jour de sécurité REGULIERE du système, ainsi que l'utilisation d'un détecteur de "rootkit" vous protègent efficacement contre les exploits
  => choisissez une distribution commerciale et professionnelle qui justement offre des mise à jour de sécurité rapides, voire automatiques

- Seuls 1 ou 2 utilisateurs ont le droit d'ouvrir une session sur la machine; ces utilisateurs sont de confiance et ont un mot de passe "sérieux"

- Vous n'avez pas installé de services inutilisés (ex : SSH); d'autres part, votre firewall bloque les ports inutilisés. (limitez-vous au service **httpd** dans un 1er temps)

- Les services sensibles (ex : SSH, voire ftp) ne sont accessibles qu'en **hosts.allow**

Vos atouts :

- Vous mettez vos logiciels serveurs à jours régulièrement pour combler toute "faille" (si c'est du Linux; pour Windows : il vous reste la prière... ;))

- Vous vérifiez régulièrement les fichiers de logs (ex : auth.log) et le fichier /etc/passwd, pour détecter toute anomalie (si vous avez deux utilisateurs avec l'uid 0, c'est pas bon signe! ;))

- Votre serveur ne contient aucune information monnayable, ou intéressant des "militaires"...

- Vous faites un backup journalier de vos données

=> alors, les précautions indiquées ci-dessus sont amplement suffisantes, la sécurité de votre système est quasiment parfaite.

Support technique

Si vous pensez avoir besoin d'un support technique pour la maintenance de votre serveur DMZ, et/ou que vous avez le budget pour... consultez les offres des sociétés suivantes :

- Microsoft/Novell (*Suse Linux Entreprise Server*)
- Mandriva (*Mandriva Corporate Server*)
- RedHat (diverses offres)
- etc...

Si vous avez du personnel avec les compétences requises, vous pouvez toujours customiser une *Debian Linux* (gratuite au départ), mais **attention** aux frais de développement, gestion, maintenance, veille technologique, etc!..

Quelques principes basiques de sécurité :

- Si vous possédez un parc de serveurs, sur un ou plusieurs sites, l'hétérogénéité est un gage de sécurité. Si une faille affecte l'un de vos serveurs, les autres ne sont pas compromis
- Sur chaque serveur, utilisez un mot de passe unique, une adresse IP unique, un O.S. unique, etc... ne facilitez pas la tâche d'un éventuel pirate !!
- Si vous en avez la compétence, fuyez les configurations classiques sur les serveurs sensibles (changez les n° de ports, les noms des fichiers de conf, ...)
- Utilisez TOUJOURS des mots de passe de + de 8 caractères (min, maj ,ponct)
- En cas de changement de personnel, mutation , etc... changez tous les mots de passe.
- FONDAMENTAL : Sécurisez l'accès local aux serveurs (au besoin, retirez les claviers et écrans)
- Qui cherche à "pirater" votre réseau ? Réponse : (quasi) exclusivement vos propres utilisateurs, employés, élèves, étudiants,... Balisez l'accès à vos serveurs.
- Connaissez vos utilisateurs et cherchez à savoir qui a la compétence de faire quoi, ou qui a des relations...
- Évaluez le coût de tous ces dispositifs, le coût de leur absence.
- Ne soyez pas paranoïaque...

III. Exemple d'installation du serveur WEB

Dans notre exemple, nous installons un serveur web sur la DMZ d'un établissement scolaire avec 2 parties externes (statique et CMS), et 2 parties intranet (élèves et profs)

1) les logiciels requis

logiciel	Commande d'installation (ex : Mandriva)
le serveur web *Apache 2*	urpmi apache2
l'extension PHP	urpmi apache2-mod_php
l'extension PHP/MySQL	urpmi php-mysql
le serveur *MySQL*	urpmi mysql
Wget et *unzip*	urpmi wget, urpmi unzip
option : le serveur SSH	urpmi openssh-server
option : le serveur *ProFTP*	urpmi proftpd
option : *Webmin*	urpmi webmin

2) méthode d'installation de la machine hôte

- Utiliser le CD 1 de Mandriva free 2007...
- niveau de sécurisation : plus élevé
- choix des paquetage : tout décoché
- Utiliser le CD 2 de Mandriva free 2007...
- Créer l' utilisateur « admin » (indispensable!)
- Configurer le réseau avec les données ci-dessous...
- Rebootez, connectez-vous en « admin », puis « su » (tapez le mot de passe root)
- Faisons du nettoyage : « rpm -e shorewall », puis « service iptables stop »
- Installer les logiciels requis (voir 1))
- Rebootez

3) les paramètres IP

Nous accédons au réseau Internet par la passerelle dont les paramètres sont les suivants :

- adresse IP publique : 194.214.168.10
- adresse IP privée : 10.145.69.173 / 255.255.255.240
- elle offre le service proxie, DNS et NAT les requêtes sur le port 80 vers l'adresse IP : 10.145.69.162

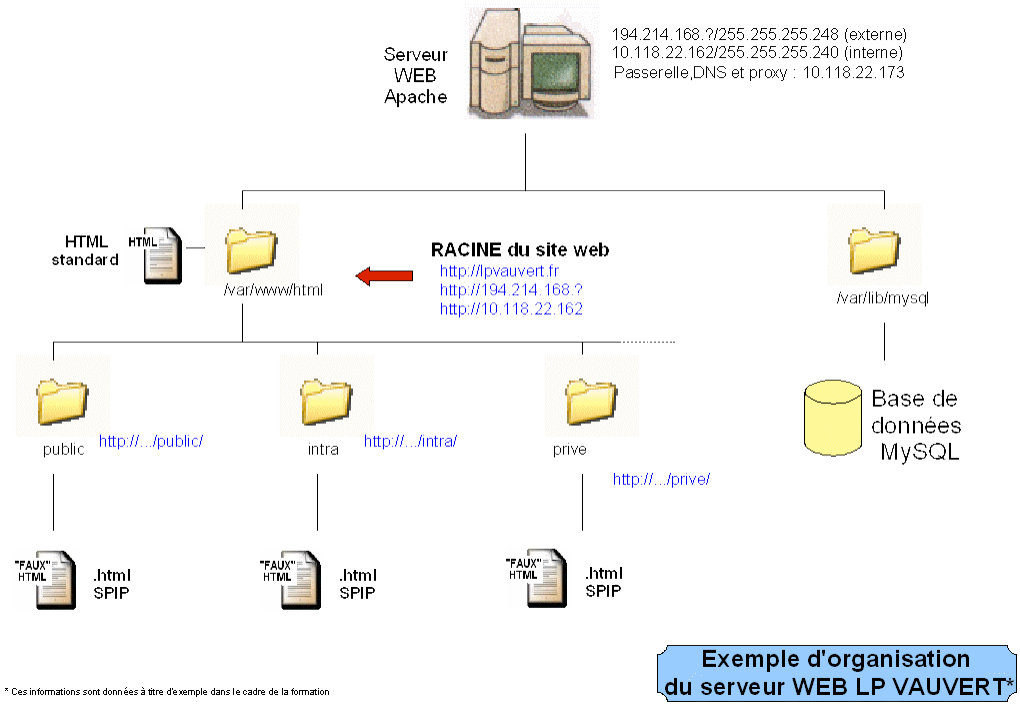
Nous en déduisons les paramètres de notre serveur DMZ :

- IP : 10.145.69.162
- masque : 255.255.255.240
- gateway : 10.145.69.173
- DNS : 10.145.69.173
- Nom d'hôte : DMZTEST

4) la configuration des services WEB

les **fichiers de configuration par défaut d'Apache** nous conviennent. (Nous n'utilisons pas les fonctionnalités exotiques d'Apache qui sont source de plantage et/ou de failles...)

Nous devons **créer l'arborescence** suivante (4 directories : **racine** (site en HTML classique), **public** (site en CMS pour le Weblog), **intra** (intranet pour tous en CMS), **prive** (intranet pour les personnels en CMS).



racine : à la racine du site, nous plaçons un site en pages HTML (voire javascript/PHP) classiques; c'est le "frontend", la façade de l'établissement pour le public au sens large; le contenu change rarement. On y décrit l'établissement avec des photos, des plans, etc.. ainsi que les formations dispensées. Un lien ramène à la partie Weblog du site externe. l'accès est non-authentifié.

public : cette partie publique du site permet de publier des informations au jour le jour pour les élèves et les parents d'élève, des actualités, les évènements marquants de la vie du Lycée, etc... Il est gérée par un CMS (ex : SPIP); le contenu change plusieurs fois par jour. l'accès est non-authentifié.

intra : cette partie du site (intranet) permet de publier des informations au jour le jour pour les élèves et les parents d'élève et les professeurs, des actualités, les absences des professeurs, le menu de la cantine, des cours en ligne, des exercices de soutien scolaire, des liens vers les applications web (cahier de texte ou notes, etc...), etc...Il est gérée par un CMS (ex : SPIP); le contenu change plusieurs fois par jour. l'accès est authentifié, éventuellement sur plusieurs niveau d'accès.

prive : cette partie du site (intranet) permet de publier au jour le jour des informations réservée pour les personnels de gestion, professeurs, et autres personnels. Il est gérée par un CMS (ex : SPIP); le contenu change plusieurs fois par jour. l'accès est authentifié, et éventuellement restreint à l'accès local.

Connectons en tant que « admin » puis « su »
Créons les directories requis :

```
mkdir /var/www/html/public
mkdir /var/www/html/intra
mkdir /var/www/html/prive
service mysqld start
```

Puis nous téléchargeons le CMS :

```
wget http://www.spip.net/spip-dev/DISTRIB/spip.zip
```

Extrayons cette archive

```
unzip spip.zip
```

Nous les copions dans nos directories avec les droits ad-hoc :

```
cp -r spip /var/www/html
cd /var/www/html
cp -r spip public
cp -r spip intra
cp -r spip prive
chmod -R ug+w public
chmod -R ug+w intra
chmod -R ug+w prive
chown -R apache:apache public
chown -R apache:apache intra
chown -R apache:apache prive
rm -rf spip
```

Nous copions les fichiers HTML de la partie racine :

```
cp -r /mnt/cdrom/* /var/www/html
```

Nous configurons le SPIP public :

Créer la base MySQL : public; cf. formation SPIP

Nous configurons le SPIP intra :

Créer la base MySQL : intra; cf. formation SPIP

Nous configurons le SPIP prive :

Créer la base MySQL : prive; cf. formation SPIP

Voilà, le site est opérationnel !
Testez-le à l'adresse http://10.145.69.162 depuis le réseau local
ou http://194.214.168.10 depuis Internet.