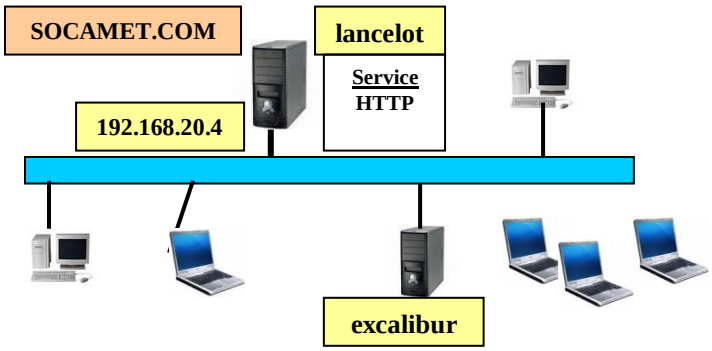
Travaux pratiques administration réseaux licence RT

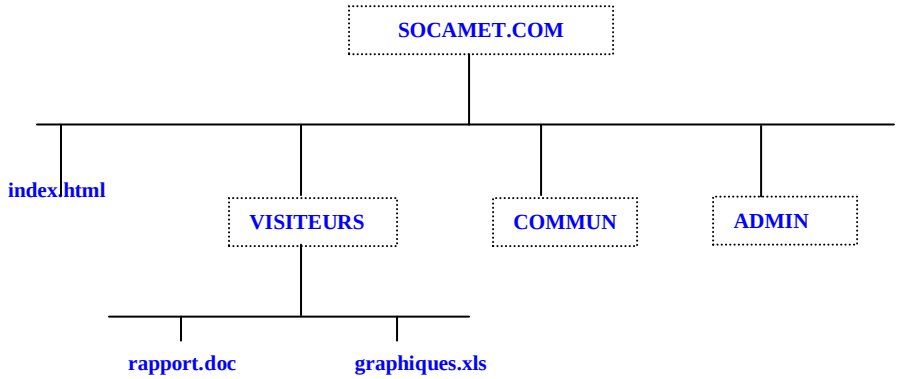
H. TSOUNGUI jan. 2019

TP1 : sécurisation des accès à un serveur HTTP, gestion des partages



Partie 1

On considère l'arborescence suivante du site de l'entreprise SOCAMET. On vous demande de sécuriser les accès à son serveur web **Lancelot** en respectant les conditions ci-dessous :



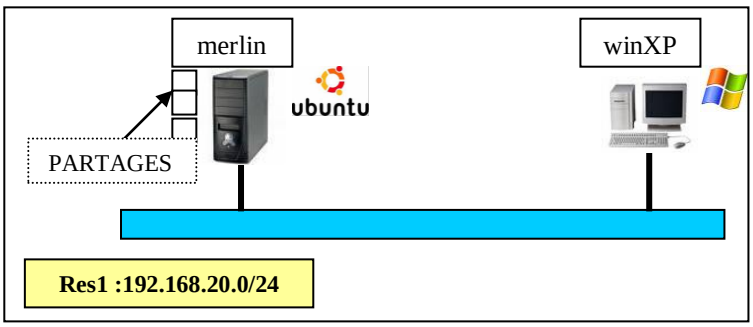
-Le serveur web **lancelot** sera sous linux ou windows (serveur ou même client comme win7 ou XP)
-La racine du site, tout comme le répertoire COMMUN sont accessibles à tous.
-Le dossier VISITEURS n'est accessible qu'aux utilisateurs ayant un compte Apache(login + pass).
-ADMIN n'est accessible qu'aux utilisateurs **admin** et **dubois** (ayant aussi leur compte Apache).
Mettez en place cette sécurisation des accès au site de l'entreprise SOCAMET.

Partie 2 partages Samba

Travail à faire

L'objectif de ce travail est de mettre à la disposition de tous les utilisateurs du réseau des ressources avec des droits d'accès bien définis.

Réaliser l'architecture de réseau hétérogène composée de stations de travail sous Windows (XP, Seven ou tout autre), Linux (ubuntu ou debian). L'objectif avoué est de permettre des accès limités à des partages mis en place sur le serveur merlin.



Travail à faire

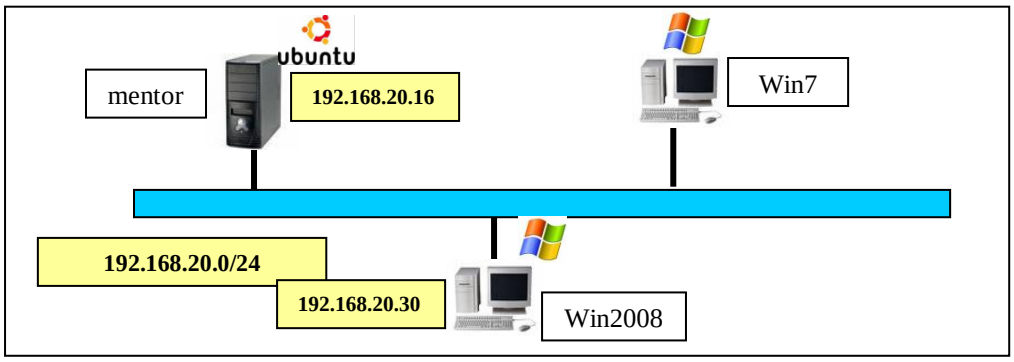
1-Créer les utilisateurs samba ci-après dubois, fred, marine, henri, lenoir, administrateur ;
2-Créer le groupe '**smbusers**' comprenant lenoir et administrateur ayant tous les droits sur les partages;
3-Créer le groupe '**marketing**' des agents commerciaux comprenant les utilisateurs fred et marine ;
4-Créer les « ressources » suivantes dans **/home/samba** :

Répertoire '**public**' : accessible à tous en lecture/écriture ;
Répertoire '**docs** : accessible en lecture/écriture aux seuls utilisateurs marine et dubois.
Répertoire '**commun**' : accessible à tous en lecture pour tous et en lecture/écriture pour henri seul ;
Répertoire '**marketing**' : accessible en lecture/écriture aux commerciaux (fred et marine, d'autres commerciaux peuvent arriver sous peu) ;

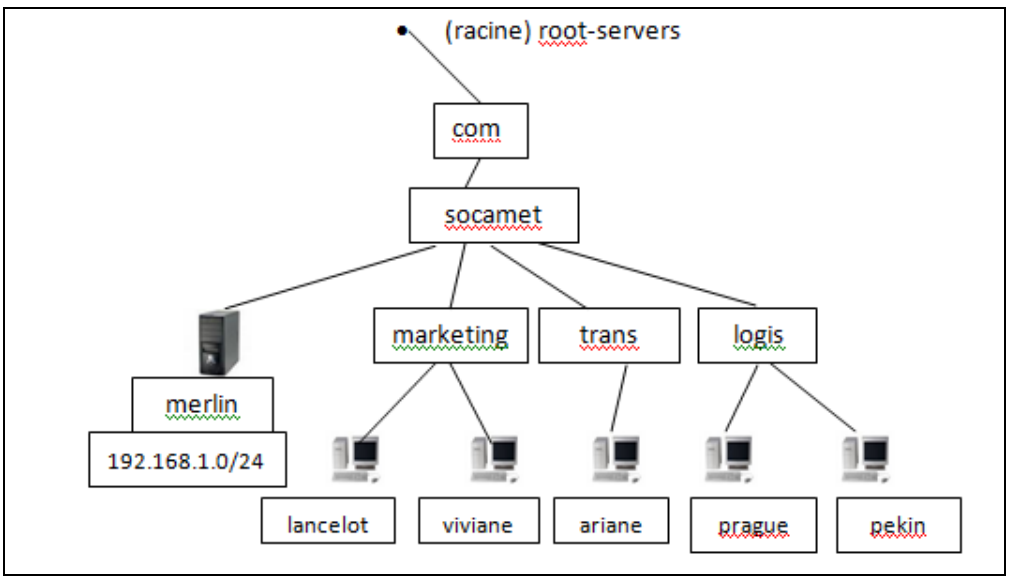
5-Tester les droits d'accès ainsi définis pour tous ces utilisateurs.
6-Rendre les sous-répertoires de /home visibles dans le « voisinage réseau ».
7-Définir un partage de l'imprimante locale de **merlin** (même si elle n'est pas physiquement connectée).

TP-2 : Configuration d'un serveur DNS sous windows server et linux

La société SOCAMET a créé trois départements **marketing**, **transports**, **logistique**, selon l'arborescence ci-dessous. Le service DNS doit donc être modifié en conséquence.
L'adresse du serveur est fournie à titre indicatif, vous pouvez la modifier.



1er cas : serveur DNS sous windows 200X



1-Ajouter le rôle DNS et configurez le service DNS étape par étape
2-Réaliser les modifications nécessaires ainsi que les tests de résolutions directe et inverse
-ajout des différents enregistrements SOA, NS, A, CNAME, etc, en respectant l'arborescence ci-dessus.

2ème cas : serveur DNS sous linux (ubuntu 16)

Ajouter le paquet bind9 à linux et modifier les fichiers proposés dans /etc/bind9.

1-Fournir les fichiers de configuration **resolv.conf** (linux)
-fichiers de zone directe : **marketing.socamet.com.host** (résolution directe)
-fichier de zone inverse : **marketing.socamet.com.rev** (résolution inverse)
-Tests avec **nslookup**, **dig** et **host** (ping est facultatif)

2-Fournir les captures d'écrans des tests de résolution et leurs résultats.

NB : quelques documents intéressants concernant ces thèmes se trouvent ici http://tsoungui.fr

TP3 Filtrage TCP par pare-feu

Objectifs : réglementer les accès à une machine ou à un réseau par la mise en place d'un firewall sur une machine ou sur un routeur qui devient ***routeur filtrant***.
Cas 1 : sécurisation des accès à un PC.
Architecture : au moins deux PC sur le même réseau.
Dans ce premier cas, après avoir capturé par un logiciel de métrologie comme Sniffer et observé des paquets de données circulant sur le réseau, mettre en place des « Règles » sur le FW.
Le FW fonctionne au niveau Transport et ses règles s'appuient sur les protocoles(souvent ICMP, TCP et UDP, etc), la source, la destination des paquets et les ports utilisés. La règle a pour but de spécifier l'**action** à effectuer sur le paquet selon sa source, sa destination, le protocole, le port : bloquer, autoriser, détruire, logger, etc.
Ex : Bloquer tous les paquets TCP/UDP de 172.16.0.2 à destination de 192.168.1.2

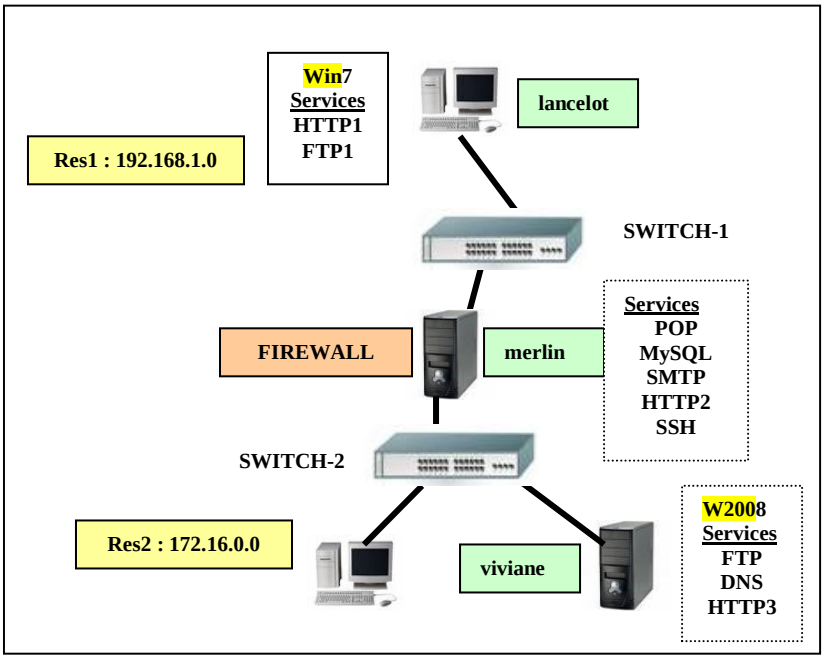
Cas 2 : Filtrage sur un routeur (sous Linux) par l'outil ***iptables*** (Netfilter)
Architecture : deux réseaux interconnectés par un routeur faisant aussi office de Firewall.

Travail à faire

1-Mettre en place l'architecture de réseau logique donnée en annexe 1.
Cette architecture présente une interconnexion de deux réseaux TCP/IP.
Le poste ***merlin*** sous linux est à la fois routeur et filtre de paquets. Mettre en œuvre le **routage** IP entre les deux réseaux.
2-Installer les services réseau proposés
3-Mettre en œuvre le **filtrage** TCP/UDP en utilisant
-l'outil GUFW, interface de configuration de **Netfilter** (intégré au noyau)
-l'utilitaire ***iptables*** en ligne de commande ou fichier de configuration à exécuter
-l'outil ***webmin*** pour spécifier et activer les règles du FW.
4-Tester le respect des règles dans plusieurs cas. Exemples dans le tableau en annexe 1.
5-Créer un fichier **script** des règles à lancer automatiquement au démarrage.

Mots-clés : Protocole de transport, Paquet, filtrage, firewall, règle de filtrage, Netfilter, *iptables*, shorewall, fwbuilder

Annexe 1 Architecture du réseau logique



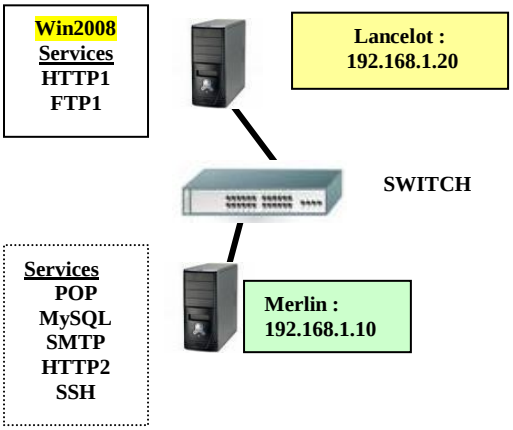
Annexe

Exemples de règles de filtrage à paramétrer et tester

Destination	Source	Protocole	Port	ACTION
merlin	lancelot	FTP		REFUSER
merlin	lancelot	Ping		ACCEPTER
merlin			8080	REFUSER
merlin		HTTP2		ACCEPTER
merlin	lancelot	FTP1		REFUSER
www.google.fr	merlin			LOGGER
*	*	*	*	REFUSER

TP4 Monitoring de composants et services avec Nagios 3.5/Icinga2 et ZABBIX 3.x

Dans cette partie, je vous propose un travail de découverte et mise en œuvre de la supervision des services et composants par le logiciel l'un des logiciels nagios/icinga et zabbix.



Travail à faire

I)-Pour zabbix :

1)-Réaliser l'architecture ci-dessus comprenant :
- -un serveur windows (2008 server par ex .)
- -un serveur linux (ubuntu, xubuntu ou debian)

2)-Installer les services réseau proposés.
3)-Installer zabbix-server (avec les paquets ou les sources).
4)-Installer les agents zabbix
- Sur windows
- Sur linux.

5)-Configurer/Créer les hôtes à monitorer lancelot windows et merlin sous linux.
6)-Créer les services des hôtes précédents.
7)-Visualiser les états des différents services.
8)-Créer deux incidents (arrêts volontaire des services) et revisualiser les
Graphes des hôtes et services.

NB : Vous proposerez toutes les captures qui vous semblent illustrer des situations intéressantes.

II)-Pour Nagios 3.5/ Icinga2 :

Faire la même chose, changer les icones des hôtes et essayer la gestion d'**alertes par mail et par SMS**.