Université de VALENCIENNES ISTV Année 2017-2018

TP1 RESEAUX Licence 3 FI et Apprentis

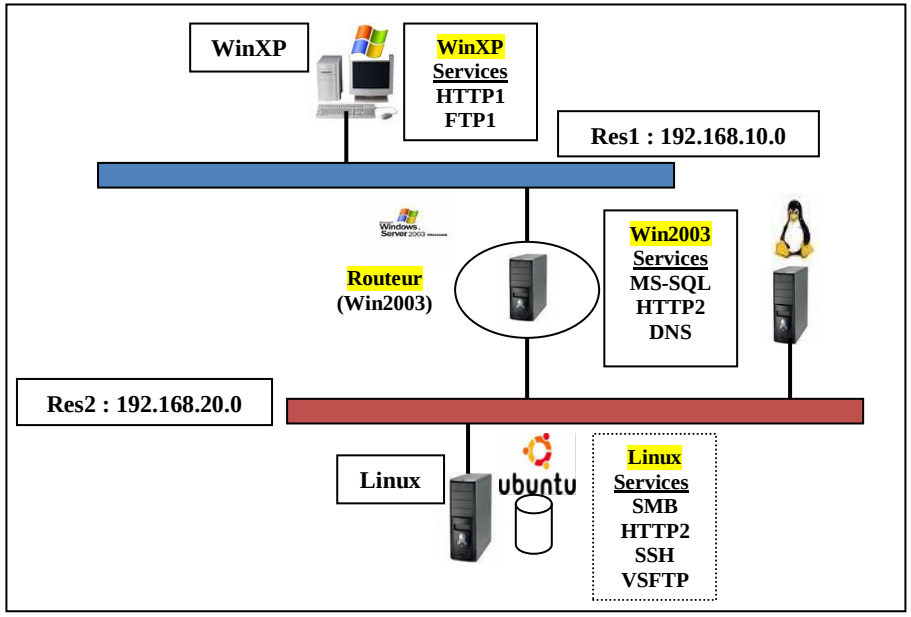
H. TSOUNGUI

Note : les comptes-rendus de TP sont à rendre sur support informatique (clé USB, CD/DVD) ou papier en individuel (seul) ou en binômes

Cet énoncé du TP1 comporte 3 parties

Partie 1 Mise en œuvre du routage

Architecture : mettre en place l'architecture représentée ci-dessous
-Réseau Res1 :192.168.10.0/255.255.255.0 et
-Res2 d'adresse 192.168.20.0/255.255.0.0
-Trois machines : WinXP, Win2003 en routeur et Linux.
-Win2003 joue le rôle de ROUTEUR et comportera **deux** cartes d'interface réseau à configurer correctement.
Etapes :
- Configuration des adresses de chacune des machines.
- Activation de la fonction de routage sur le routeur PC3.
-Test de communication (routage RIP) entre les deux réseaux par des commandes ping ou les accès à des services d'un réseau distant, au-delà du routeur.



1.1)-Mettre en œuvre le routage en permettant la communication entre les postes WinXP et Linux.
1.2)-Tester la traversée du routeur par des commandes PING adéquates.
1.3)-Tester la communication entre les machines des deux réseaux en accédant aux services de machines distantes. Ex : accéder au service HTTP1 de WinXP à partir de Linux ou accéder au service SSH de Linux à partir de WinXP.

Partie2 Mise en œuvre des partages

2.1) Sur winXP, installer les services et clients suivants : HTTP1 (serveur web sous Apache2), filezilla client, secure-shell client ou putty.

2.2) Sur Win2003, installer HTTP2 sous IIS, MS-SQL Server,
-Créer la BDD 'PROSPECTS' et ses tables Client et Region.
-Créez un répertoire partagé appelé **pub_win** et paramétrez ses accès en autorisant son accès en lecture/écriture à **administrateur** et en lecture seule pour tous les autres.
Testez ces droits d'accès et illustrez votre compte rendu par des captures d'écrans significatives.

2 .3) Installer enfin sur Linux : vsFTP-server ou pro-FTP, Open-SSH server, HTTP2 avec Apache 2. Installer également SAMBA et créer les partages suivants :
- « **rapports** » accessible aux utilisateurs mireille et pierre en lecture/écriture
- « **documents** » accessible en lecture et écriture aux membres du groupe «techniciens ». Ce groupe comporte les utilisateurs charlene et patrick. Seul charlene peut écrire dans le partage.
Testez les accès aux ressources partagées.

Notes :- pour gérer les partages sous Linux, installez le paquet samba avec la commande **apt-get install** ou **apt install samba**. Modifiez le fichier **smb.conf**.
-Les ***utilisateurs samba*** sont à créer avec la commande **smbpasswd** –a nom_user ou **pdbedit** –a nom_user.

Suite page 2 ➔

Partie 3 Filtrage des paquets

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 192.168.10.3 à destination du port 21 de 192.168.10.2

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

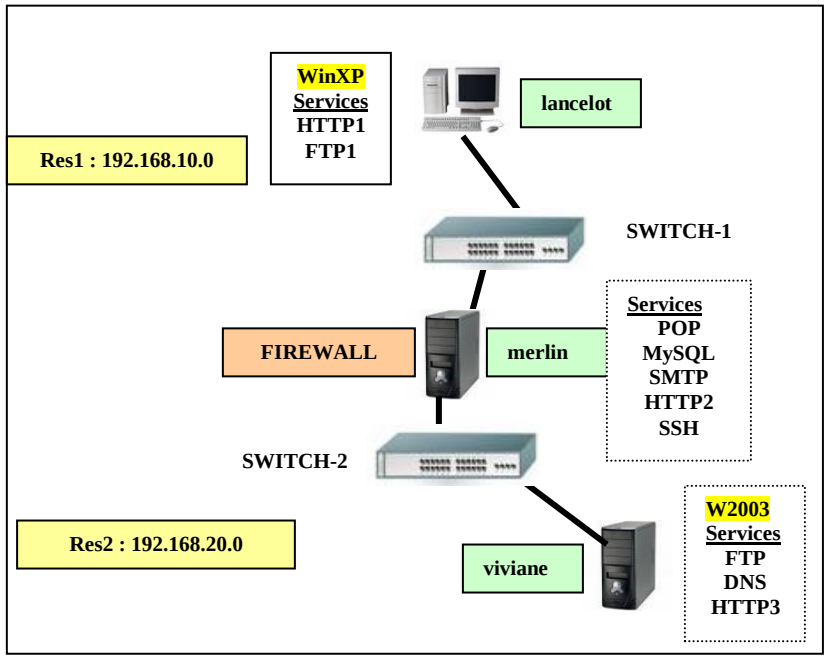
-l'outil ***webmin*** pour spécifier et activer les règles du FW.

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

NB : Adresses pour envoyer vos comptes rendus :

henri.tsoungui@univ-valenciennes.fr ET htsoungui@sfr.fr et à vous-mêmes.

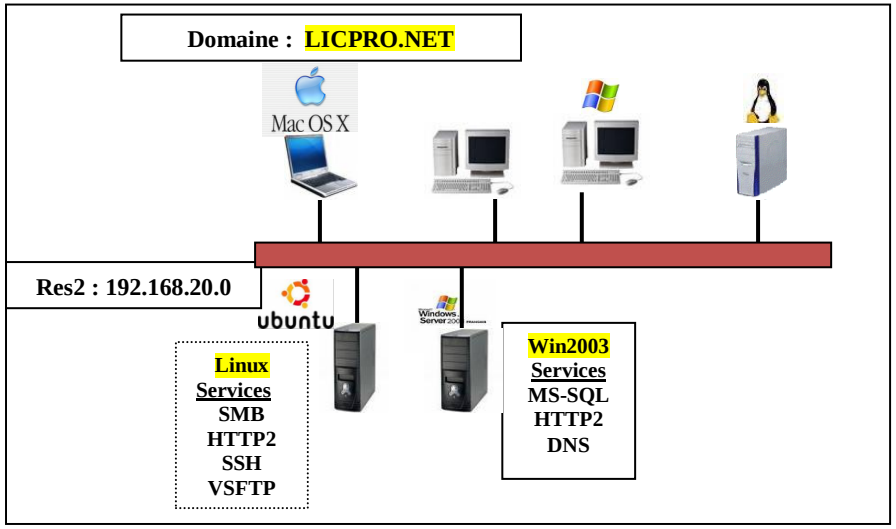
Université de VALENCIENNES ISTV Année 2017-2018

TP2 RESEAUX Licence 3 FI et Apprentis

H. TSOUNGUI

Cet énoncé comporte 2 parties

Partie 1 : Mise en place d'une authentification globale par un serveur linux PDC



Objectif : configuration d'un serveur de domaine (réseau hétérogène, clients d'OS divers)

Dans le TP précédent, vous avez mis en place différentes ressources partagées en réseau. Votre serveur linux qui n'était qu'un serveur de fichiers est appelé à évoluer : il doit permettre de remplacer l'ancien contrôleur de domaine sous windows server 2003 pour différentes tâches.

1-Créer un groupe machines, ajoutez-y au moins un client winXP et un win7

2-Créer des utilisateurs locaux et des utilisateurs du domaine. Expliquer la différence.

3-Mettre en œuvre l'authentification globale par le serveur SAMBA configuré en Contrôleur du domaine LICPRO.NET.

-Créer les partages suivants :

« stagiaires » accessible en lecture/écriture aux étudiants victor et mariane

« fournisseurs » accessible à tous ceux qui ont un compte samba

** Vous présenterez clairement

- les modifications effectuées dans le fichier de configuration **smb.conf**

et fournirez les captures des tests **: ajout de client, connection d'un utilisateur au domaine, etc.**

Partie 2 : supervision de composants et services réseau(sous Linux) avec NAGIOS 3.5 ou supérieure

Objectifs : Surveiller l'état de composants matériels adressables et avertir par des **alertes** (sonore, **mail** ou SMS), les responsables lors d'un état critique.

Dans ce dernier TP, je vous propose un travail de découverte et de mise en œuvre de la supervision ou monitoring des services et composants par le logiciel **Nagios**.

Architecture du réseau

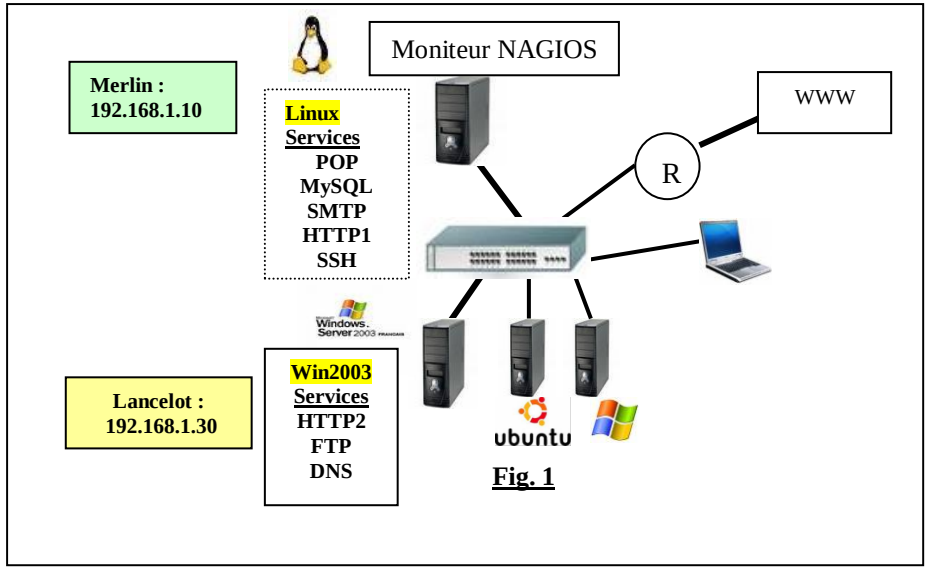


Fig. 1

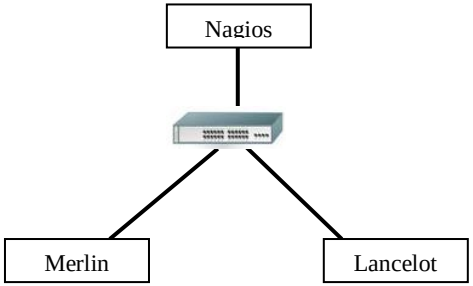


Fig. 2

Travail à faire

1)-Réaliser l'architecture ci-dessus comprenant (Fig. 1) :
-un serveur windows (2003 server par ex .)
-un serveur linux (ubuntu, xubuntu ou debian)
2)-Installer et tester les services réseau proposés, les ports TCP par défaut figurent entre parenthèses
-Sur Merlin : HTTP1(80), MySQL-server(3306), OpenSSH-server(22), Postfix(25) et Dovecot-pop3d(110)
-Sur Lancelot : HTTP2/IIS (80), FTP-server(21), DNS(53)
3)-Installer **nagios3** sur linux(avec les paquets, conseillé, ou les sources).
4)-Installer des agents si nécessaire. Faire de SWITCH, le **parent** des composants Merlin et Lancelot (Fig 2).
5)-Visualiser les états des différents hôtes et services. Effectuer des captures d'écrans.
6)-Créer des incidents (arrêts volontaires des services) et revisualiser les Graphes des hôtes et services.
-Effectuer des captures d'écrans.
-Examiner les messages envoyés à root ou tout autre responsable choisi et configuré pour recevoir les messages d'alerte.
-Examiner les logs système.
7)-Conclusion sur votre travail de supervision.

NB : Vous trouverez quelques docs ici : http://tsoungui.fr et ailleurs, sur la toile.

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

NB : Adresses pour envoyer vos comptes rendus :
henri.tsoungui@univ-valenciennes.fr ET
htsoungui@sfr.fr
et à vous-mêmes.