DURCISSEMENT LINUX – PREMIERS PAS **H. TSOUNGUI**

1)-Architecture de travail

Afin de concrétiser nos bonnes intensions en matière de sécurisation des systèmes linux, nous allons mettre en place une architecture réseau concrète et allons la sécuriser étape par étape

-Schéma du réseau Domaine : **HARDENE.TUX**

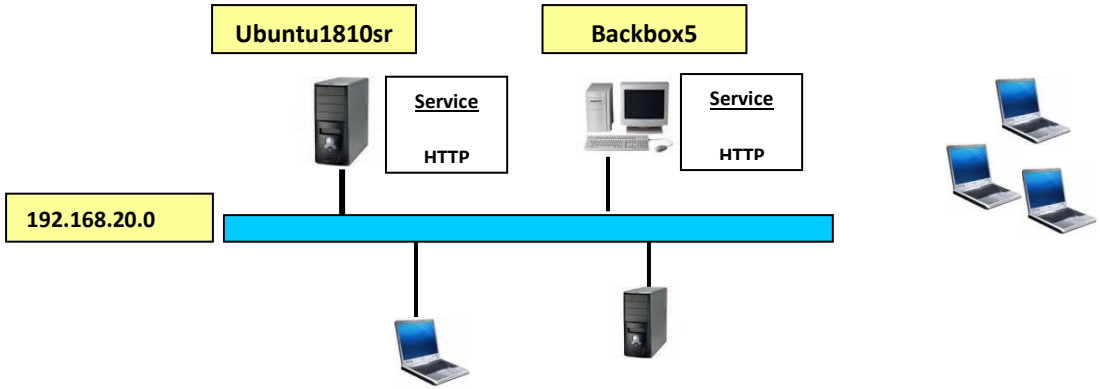

Fig. 1 Architecture du réseau

-Les ressources partagées (partages)

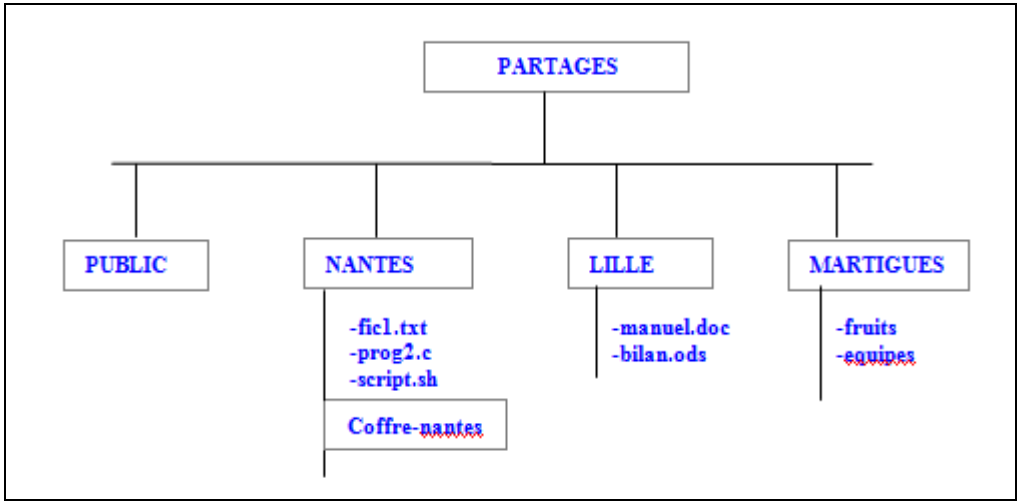

Fig. 2 Ressources

-Les **groupes** d'utilisateurs et les accès aux ressources

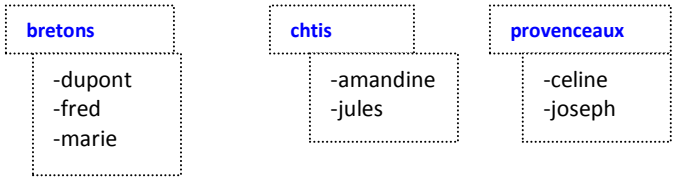

Fig. 3 Utilisateurs

* Les groupes ont par défaut, le droit d'écriture sur leurs fichiers et dossiers respectifs : les bretons peuvent tout faire dans la ressource partagée NANTES,

Les chtis dans LILLE, etc. Le dossier PUBLIC doit être accessible à tous en lecture/écriture et être browsable.

Attention à ce genre d'accès incontrôlé ! Il vaut toujours mieux mettre en place une gestion fine des droits avec login et pass. Ce partage ne devrait servir qu'en phase de test.

2-Les premières tâches à effectuer

Tâches	OK	NON	Commentaires/utilitaires
0)- Consulter doc debian security AVANT install : ouvrir l'UC, rechercher le cavalier (jumper) de protection, enlever la pile, redémarrer, etc Créer un mot de passe du BIOS (ouvrir **1)-Installation du serveur ubuntu 18.10** 1.1)-Partitionnement précis. Création de /home 1.2)-Attribution d'un password pour sudo 1.3)-Fin de l'install - Mot de passe pour **grub** (ou lilo)? 1.4)-Créer un mot de passe pour root 1.5)-Consulter doc Debian Security APRES install … … -Eviter de se connecter à l'Internet			
2)-Premier redémarrage 2.1)-Vérifier la connexion avec l'Internet -Lancer la mise à jour de votre nouveau système (apt update) -Dès que possible, lancer un upgrade, puis à nouveau une update			
3)-Installer un nombre minimal de services 3.1)-SSH (openssh-server), FTP (vsftpd), MYSQL-SERVER ou POSTGRESQL-server, SMB/CIFS minimal en serveur de fichier, HTTP (Apache2), etc.			

3.2)-Test SSH			
3.3)-Test HTTP			
3.4)-Test MYSQL, création d'un password pour root_mysql -Création d'une petite BDD avec au moins 2 tables liées			
4)-Gestion des users et des groupes 4.1)- Créer les groupes nécessaires : bretons, chtis, provenceaux 4.2)- Créer les utilisateurs humains 4.3)- Ajouter les users aux bons groupes			
-Revisiter les droits d'accès pour une cohérence parfaite avec les utilisateurs créés			
5)-Configuration et sécurisation des accès réseau			
-Chaque machine ne devrait avoir qu'une seule interface réseau, en phase de production, pas de filaire et wi-fi en même temps			
6)-Sécurisation des services du système			
6.1)-Sécurisation de HTTP -Gérer le filtrage des clients ordinateurs et réseaux Allow, Deny -Gérer l'accès à un site par **htaccess** -Consulter les journaux **access.log** Apache pour visualiser les accès après quelques essais, tenter d'accéder partout, même à des répertoires protégés de l'arborescence du site			
6.2)-Sécurisation de SSH -Interdire l'accès anonyme -Empêcher l'accès distant de root et des sudoers			

6.3)- Sécurisation de FTP -A l'instar de SSH, réglementer l'accès à distance : pas d'accès anonyme, pas d'accès distant de root, etc			
6.4)-Mise en place du service de courrier mail -Installer Postfix, Dovecot-pop3d rapidement pour revoir les mails du système -Modifier le fichier des alias (root ne doit pas tout recevoir) (cf. /etc/aliases)			
Mise en place d'un pare-feu ufw et IPTABLES			
Mise en place d'un détecteur d'intrusion (IDS)			
Installer des utilitaires d'AUDIT - -			
Outils d'évaluation des vulnérabilités à distance			
Outils pour parcourir le réseau NMAP			
Analyseur de trames WHIRESHARK			
Antivirus			

Quelques règles de base d'iptables			
Recherche des rootkits Tester ces deux utilitaires **-chkrootkit** **-rkhunter**			

3-Phase 2 : évolution de l'architecture (11/02/2019)

-Schéma du réseau Domaine : **HARDENE.TUX**

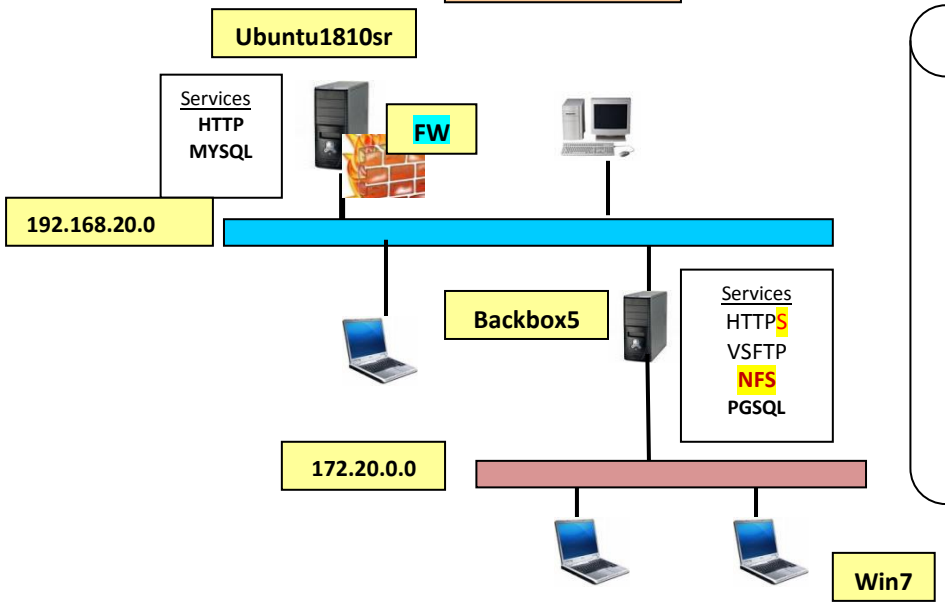

Fig. 2 : nouvelle architecture du réseau

1-Mettre en place le service **NFS** sur **Blackbox5**
* /shares1/dossier1-ro en lecture seule
* /shares2/dossier2-rw en lect/écriture

2-Protéger le serveur **ubuntu1810srv** par un pare-feu
*Autoriser accès pour SSH, ICMP, ICMP
*Refuser accès à partir de 172.20.0.0/16 sauf pour win7 pour SSH
*Autoriser accès MySQL pour win7
* + autres règles

3-Sécuriser un site du serveur Backbox5 par **SSL**