Télécom 3000

Contexte :

L'entreprise est en recherche d'un administrateur système et sécurité suite à la démission soudaine et inexpliquée de son ancien administrateur.

Kyan était en train d'installer un nouveau serveur qui allait permettre de remplacer le site vitrine de l'entreprise.

Seul l'OS et le SSH ont été installés, Kyan avait laissé des indications sur le travail qu'il était en train de mener sur ce serveur, votre rôle est de reprendre et de finir l'installation, la sécurisation et la documentation.

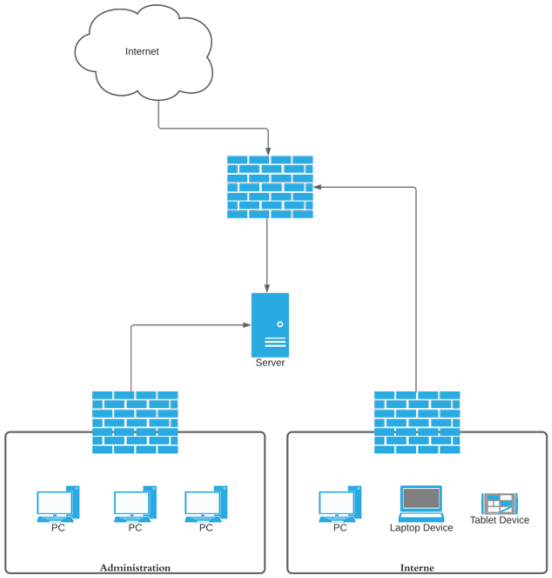
Vous pourrez retrouver les indications dans le fichier '/home/kyan/taches-de-travail.txt', sur le serveur.

Notes de Kyan :

```
Préparation :
- Création des certificats pour le HTTPs (voir dans /home/kyan) => OK
- Réaliser la matrice de flux
- Choix de la technologie pour implémenter le firewall
- Choix de la technologie pour délivrer le service http

Installation
- Installer le serveur SSH => OK
- Mettre à jour le serveur => OK
- Installation d'un serveur HTTP
- Installation de la technologie pour le firewall

Configuration :
- Configuration et sécurisation du serveur HTTP
- Sécurisation du service SSH
- Sécurisation des mots de passe sur le système (politique de mot de passe compte locaux)
- Mettre en place la matrice de flux
- Suppression / désactivation des services non utilisés
- Activer les mises à jour automatiques

Vérifications :
- Vérification avec sslscan de la bonne configuration SSL
- Faire un NMAP sur l'interface métier
```

Sécurité des Systèmes - TP01

Architecture :



Indications supplémentaires :

Le serveur doit :

- Servir le site fourni en archive.
- Être sécurisé avec les notions vues plus tôt dans le cours.

Vous êtes libre de choisir :

- La technologie permettant de servir le protocole http.
- La technologie permettant de mettre en place un firewall local.

Vous devez :

- Rendre la matrice de flux en suivant le formalisme fourni en annexe.
- Fournir le scan NMAP
- Rendre l'ensemble des actions réalisées de manière synthétique dans un fichier word avec une mise en page simple.

Installation et connexion :

Une fois l'archive récupérée, il vous faudra monter le disque dans une nouvelle machine virtuelle. Le disque peut être monté avec VirtualBox ou VMWare. Vous pouvez vérifier l'intégrité du disque avec sha1sum : **a6eadf5581dfcb98f2612d1e0af6dcefae4b3e39**

La machine devrait tourner sans problème avec les ressources suivantes :

- 1Go RAM
- 1vCPU
- 2 Interfaces réseaux (Elles sont en DHCP):
    - Eth0 : Interface métier (en NAT)
    - Eth1 : Interface d'administration (en Host-only)

Les informations pour s'y connecter sont 'kyan:kyankyan'.

Annexes :

Exemple de commande pour faire un NMAP :

nmap -sS -sV -oA NomDeMonFichierDeSortie MonIP

Exemple de matrice de flux :

ID	Source IP	Source Port	Destination IP	Destination Port	Protocole	Description
	127.0.0.1	ANY	127.0.0.1	53	UDP	DNS

Politique de mot de passe à implémenter :

- 12 caractères
- Chiffres
- Majuscules et minuscules
- A minima 1 caractère spécial
- Renouvèlement tous les 90 jours.

SSLScan, si vous n'utilisez pas Kali qui embarque directement ce package, il est possible de l'installer avec les instructions suivantes : https://github.com/rbsec/sslscan