ESGI

Mini- Projet Python

« Développement d'outils d'Administration Réseau »

Cas Team_NetWay

Proposé par : Céline OULMI

Promotions : 3A SRC1&2&3

Année : 2020-2021

Contexte et objectifs du projet

1) Présentation du contexte :

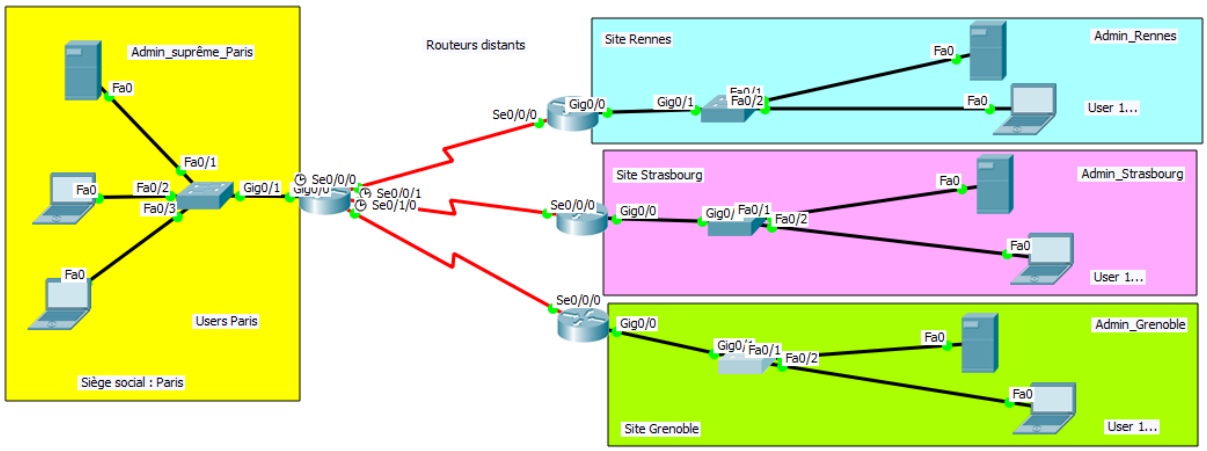
Vous êtes une équipe de 4 techniciens spécialisée dans les métiers liés aux infrastructures réseaux, développement de solutions d'administration, le pilotage de projets, de migration, de mise en production et de gestion/virtualisation/supervision du réseau en collaboration avec divers administrateurs confirmés.

Vous intégrez un projet de développement réseau conséquent et vous intervenez pour le compte de l'entreprise Américaine **Team_NetWay** spécialisée dans des solutions d'administration, d'audit et de diagnostique des réseaux d'entreprises de toute taille. Elle est implantée en France depuis 2010.

Team_NetWay a vocation à intégrer de nouvelles technologies, de nouvelles solutions applicatives et de nouveaux outils au fil du temps, notamment dans la sécurité.
Elle souhaite développer, grâce à ses compétences métiers, ses propres outils et solutions de sécurité personnalisés adaptés à des situations particulières en hacking et forensic pour :

1. Assurer la disponibilité de ses services réseau pour des accès en local et à distance.
2. Gérer ses utilisateurs à l'échelle nationale.
3. Identifier les types d'attaques pour renforcer la sécurité de la partie du réseau local interne.
4. Proposer des solutions aux entreprises clientes auditées.
5. Fournir des infrastructures clef en main supportant les outils de supervision et de gestion des identités…

Team_NetWay est organisée en 3 sites représentés par le schéma (PKT) suivant :



- Le siège social est situé à **Paris** dans le 12 ième arrondissement.
- Les 3 sites distants sont situés à **Rennes**, **Strasbourg** et **Grenoble**.

Par souci de traçabilité, de qualité de ses services et de sécurité, le siège centralise tous les audits d'entreprises clientes et la gestion des utilisateurs/administrateurs de toute la plateforme de l'entreprise.

Au niveau du **siège,** des serveurs de gestion de la base de données des utilisateurs et de stockage de fichiers FTP sont administrés par un **administrateur suprême AS** habilité à :

➔ La gestion des utilisateurs/administrateurs :

- Créer de nouveaux Utilisateurs/Administrateurs selon les profils et les droits.
- Définir les règles de gestion et de sécurité des login/pwd (Login : contraction de la première lettre du prénom et du nom utilisateur (non composé), PWD : génération aléatoire et hashage avant sauvegarde, durée de validité, ….)
- Modifier/supprimer un utilisateur/un admin.
- Consulter la liste des utilisateurs/des admins.

➔ **La gestion du serveur FTP :**

- Le serveur FTP sert essentiellement au stockage.
- Les sauvegardes journalières des fichiers d'audit et répertoires archivés de la forme « nom.version », exemple : audit.12, audit.13….

➔ Périodiquement, en plus des solutions de supervision mises en place, le AS peut tester :

➔ **Un scan de ports au quotidien sur les serveurs** avec sauvegarde dans un fichier pour exploitation.

➔ **Une simulation d'une attaque par force brute avec proposition de solution(s) de renforcement de la sécurité en cas de faille.**

De plus,

- La tenue d'un journal d'activité, horodaté qui sera consulté par le **AS** afin d'éviter les erreurs…

- Les machines clientes et le serveur peuvent simplement communiquer pour s'échanger des messages pour le contrôle de flux et le contrôle de connectivité (exemple d'un ping)

Les administrateurs distants dits classiques AC gèrent les utilisateurs locaux avec la même démarche qu'au siège et envoient périodiquement leur annuaire utilisateur (exemple : un CSV) mis à jour ainsi que les fichiers d'audit au siège pour centralisation.

Enfin, les divers **utilisateurs U** peuvent s'authentifier à chaque accès avec possibilité de personnaliser le password à la première connexion.

2) Travail à réaliser

- Analyser les besoins de **Team_NetWay.**
- Proposer une architecture fonctionnelle.
- Ecrire des scripts modulaires et bien commentés pour répondre aux divers besoins exprimés.
- La réalisation sera faite en langage Python, version 3.x.

Consignes importantes :

1. Se limiter au protocole Ipv4 (associé à TCP et à UDP).

2. Effectuer des essais ponctuels (test shell, prototype sur un point particulier) tout au long de cette démarche pour affiner vos choix, et vous assurer de leur faisabilité.

3. Dans le cadre de l'intégration continue, vous livrez périodiquement un état d'avancement du fonctionnel.

4. Des exemples de scripts existent sur internet parfois d'excellente qualité,

   ⇨ **Attention à la confusion**, la plupart sont écrits en Python2.
   ⇨ Vous devriez coder en Pyhton3 avec éventuellement, des modules et frameworks développés pour cette version.

5. La date de livraison finale de l'outil est fixée au début du mois de juillet ➔**Tout travail rendu en retard sera pénalisé de 2 points par jour de retard.**

Organisation des équipes :

1. Votre équipe est organisée en binôme/trinôme/quadrinôme.
2. Votre capacité à travailler en groupes étant un élément important de ce projet, vous devez résoudre les difficultés d'organisation, de répartition du travail, de compatibilité d'humeur, etc.

   ➔ **Remonter l'information si problème au sein de l'équipe, à temps.**

3. Enfin, une date pour la présentation orale et la démonstration sera planifiée, vous en serez informés via MyGes.

Bon courage,