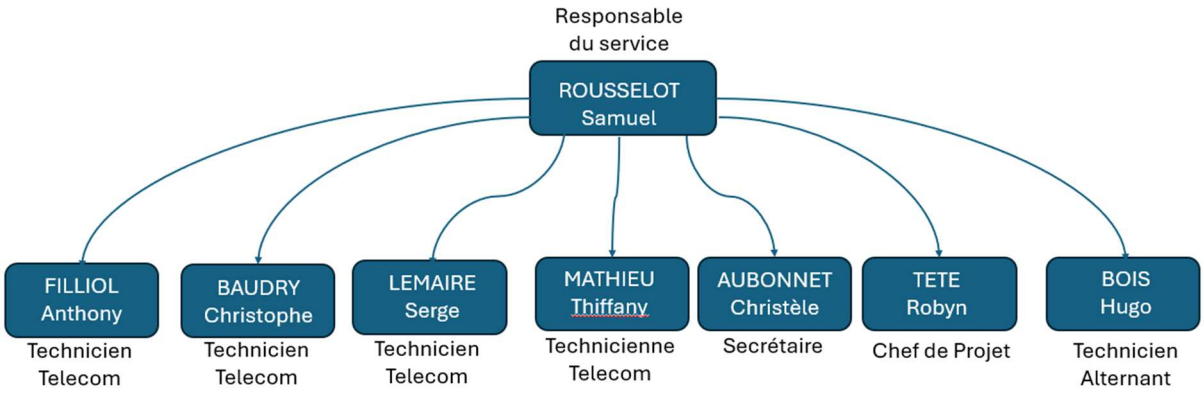
Introduction :

Lors de ma recherche d'alternance pour ma deuxième année de BUT Réseaux et Télécommunications, j'ai découvert GEDIS TELECOM grâce à une recherche sur des entreprises qui ont pour spécialités les réseaux et les télécommunications. J'ai donc décidé de me présenter avec une candidature spontanée. L'entretien avec mon responsable m'a permis de comprendre leurs besoins techniques et de confirmer mon intérêt pour cette entreprise spécialisée dans les solutions de télécommunication.

Lors de ces premières semaines en alternance, mon sujet principal consistait à renforcer la sécurité et l'automatisation des installations de 3CX qui est une solution de téléphonie IP utilisé le plus souvent en entreprise. Ce journal va donc détailler les étapes de mon travail, en commençant par le contexte et les besoins de l'entreprise, puis en détaillant le travail réalisé et enfin par le bilan et les améliorations envisagées.

Le contexte

- **Présentation de l'entreprise** :
  GEDIS TELECOM est une entreprise spécialisée dans les solutions de télécommunications et les infrastructures réseau, avec une expertise reconnue dans l'intégration de systèmes modernes comme 3CX. Basée à Aix-les-Bains, elle dispose également d'un siège à Lissieu, ce qui lui permet de rayonner sur un large territoire. Au sein de l'entreprise, je fais partie du service technique qui est un groupe de 8 personnes, nous collaborons étroitement dans un open-space pour accompagner nos clients, principalement des PME, dans la mise en place de solutions fiables et sécurisées, adaptées à leurs besoins en téléphonie, réseau et services cloud.



Organigramme du service technique de GEDIS TELECOM

- **Existant technique** :
  Dans le cadre de cette mission, je disposais d'une infrastructure technique comprenant un serveur physique dédié à la virtualisation. Ce serveur me permettait de créer des machines virtuelles pour simuler différents environnements réseau. Grâce à cette infrastructure, j'ai pu configurer un pare-feu, segmenter les réseaux en différents VLANs pendant une précédente mission et j'ai donc pu réaliser mon script et tester les différentes attaques sur les machines virtuels pour vérifier le bon fonctionnement.

  J'ai effectué mon script sur un des pcs virtuels et j'ai fait les attaques avec les deux autres pcs virtuels.

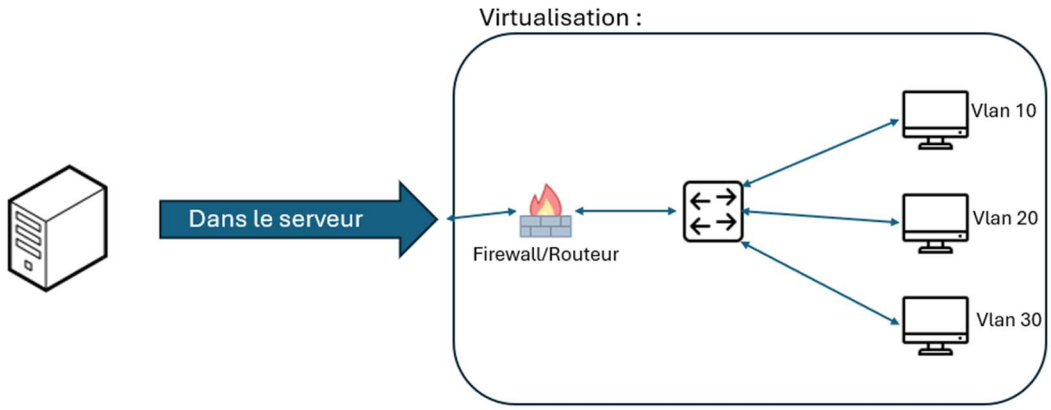


Schéma de l'existant technique

- **Le besoin identifié** :

  GEDIS TELECOM souhaite moderniser et renforcer la sécurité de son infrastructure face aux menaces telles que les scans de ports et les attaques de force brute. L'objectif est également d'automatiser l'installation et la sécurisation de 3CX pour faciliter son déploiement sur d'autres projets similaires.

- **Cahier des charges** :

  Script doit permettre :

  1. Installation automatique 3CX (linux)
  2. Gestion des connexions réseaux
  3. Surveillance pour détecter les scans de ports
  4. Sécuriser les connexions SSH
  5. Ajout d'une liste blanche
  6. Création profil pour 3CX

- **Objectif et procédure mise en place** :
  Mon travail se concentre sur :

  1. Automatiser l'installation de 3CX à l'aide d'un script bash.
  2. Intégrer des solutions de sécurité (UFW, PortSentry, fail2ban).
  3. Tester et améliorer la compatibilité de ce script sur différents environnements Linux.

Ma mission à été réaliser entre plusieurs missions données par mon tuteur, le planning est donc fait en fonction de nombres de jours par étapes.

Etapes	Analyse des besoins (1 jour)	Script (2 jours)	Tests Compatibilité (1 jour)	Amélioration Continue (1 jour)
Descriptif	Identification outils de sécurité	Ecriture du script en bash	Tentatives d'attaques et tentatives de connexions	Ajustements suite aux tests et correction de bugs

Le travail réalisé

Détails techniques :

- Le script commence par mettre à jour le système et installer les paquets requis pour le fonctionnement de 3CX. Il ajoute ensuite le dépôt 3CX et procède à l'installation du logiciel.
- Le script configure UFW pour refuser par défaut les connexions entrantes, n'autoriser que les connexions sortantes et les services nécessaires comme le SSH.

Pare-feu UFW :

```
# Configuration des règles UFW par défaut
echo "Application des règles par défaut du pare-feu"
sudo ufw default deny incoming > /dev/null
sudo ufw default allow outgoing > /dev/null
```

- PortSentry est configuré pour surveiller les tentatives de scans de port. Lorsqu'uneadresse IP suspecte est détectée, elle est automatiquement ajoutée à une liste deblocage, empêchant tout accès futur à la machine concernant la connexion à distance ou même le ping depuis l'adresse IP Blacklistée et notre machine.

Logiciel PortSentry :

```
# Configuration de Portsentry
echo "Configuration de Portsentry..."
# Modifier le fichier de configuration des modes
sudo sed -i 's/TCP_MODE="tcp"/TCP_MODE="atcp"/' /etc/default/portsentry
sudo sed -i 's/UDP_MODE="udp"/UDP_MODE="audp"/' /etc/default/portsentry

# Modifier les options de blocage dans portsentry.conf
sudo sed -i 's/^BLOCK_UDP="0"/BLOCK_UDP="1"/' /etc/portsentry/portsentry.conf
sudo sed -i 's/^BLOCK_TCP="0"/BLOCK_TCP="1"/' /etc/portsentry/portsentry.conf
```

- Fail2ban est configuré pour surveiller les tentatives de connexion via SSH et bannir les adresses IP après trois échecs de mot de passe. Cette mesure empêche les attaques par force brute sur le serveur.

Logiciel Fail2Ban :

```
        # Configuration de fail2ban
        echo "Configuration de fail2ban..."
        sudo tee /etc/fail2ban/jail.local > /dev/null <<EOL
[sshd]
enabled = true
port = ssh
filter = sshd
logpath = /var/log/auth.log
maxretry = 3
bantime = 86400  # 1 jour
```

- L'ajout d'une liste blanche est configuré pour permettre aux adresses IP publiques de GEDIS TELECOM de ne pas se faire bloquer par le script pour toujours avoir la main à distance.

Liste blanche :

```
# Ajouter les IP à la whitelist si elles ne sont pas déjà présentes
echo "Ajout des adresses IP GEDIS à la whitelist..."
for ip in "[redacted]" "[redacted]"; do
    if ! grep -q "$ip" /etc/portsentry/portsentry.ignore.static; then
        echo "$ip" | sudo tee -a /etc/portsentry/portsentry.ignore.static > /dev/null
        echo -e "${GREEN}IP $ip ajoutée à la whitelist.${NC}"
    else
        echo -e "${YELLOW}IP $ip déjà présente dans la whitelist.${NC}"
    fi
done
```

- Explication des choix techniques : UFW a été choisi pour sa simplicité et sa compatibilité avec 3CX. PortSentry permet de réagir aux scans de ports en temps réel, ajoutant une couche de sécurité proactive. Fail2ban complète cette protection en gérant les accès SSH, un vecteur courant d'attaques

Le bilan de cette période

Résultats :

- Le script permet d'automatiser efficacement l'installation de 3CX avec une configuration de sécurité robuste. Les scans de ports sont correctement détectés et bloqués par PortSentry, et fail2ban assure une protection efficace contre les tentatives de brute force sur SSH. Les tests sur différents environnements ont montré une installation stable et sécurisée.
- Concernant les résultats personnels, j'ai découvert et dû m'adapter aux conditions de travail et à la méthodologie de travail de l'entreprise. J'ai pu découvrir à l'aide de mon script des logiciels de sécurisation pour éviter tout types d'attaques de vecteurs courants. J'ai donc développé mes compétences en bash et en système mais aussi j'ai pu acquérir de nouvelles compétences en matière de Cybersécurité en sécurisant les postes.

Difficultés rencontrées :

- **Connaissance des outils :** J'ai commencé par me renseigner sur les outils que j'allais devoir ajouter dans le script car je ne les connaissais pas. J'ai dû commencer par comprendre le fonctionnement et le déroulement de chaque logiciel pour permettre d'activer les bons paramètres pour obtenir la sécurité la plus adapté à la demande.

- **Problème de fichiers non existant :** J'ai rencontré des problèmes au niveau des fichiers par défauts qui n'étaient pas présents dans les dossiers, j'ai donc dû ajouter dans mon script la création et les liens entre les fichiers manquants qui m'ont permis d'activer la liste noire des adresses IP.
- **Vérification de la robustesse du script :** s'assurer que le script fonctionne correctement en cas de réinstallation ou de mise à jour, qu'il soit capable de gérer les erreurs sans interrompre le processus d'installation et qu'il permet de bloque les adresses IPs qui tentent d'attaquer la machine cible

Prochaines étapes :

- Mise en place de la documentation afin de la rendre plus claire et accessible pour d'autres techniciens.
- Tester le script sur un plus grand nombre de distributions Linux pour garantir sa compatibilité et sa robustesse.
- Envisager l'ajout de fonctionnalités supplémentaires, comme le changement du numéro de port du service SSH qui est par défaut le 22 pour le passer en 2222 par exemple.

Conclusion

Ce projet de script pour l'installation et la sécurisation de 3CX a permis de répondre aux besoins de l'entreprise en simplifiant le déploiement tout en renforçant la protection contre les menaces courantes. Grâce à l'intégration de mesures de sécurité telles qu'un pare-feu UFW, PortSentry et fail2ban, l'environnement de téléphonie IP est désormais mieux protégé contre les tentatives d'intrusion et les attaques par force brute. Les résultats obtenus démontrent l'efficacité de ce script pour automatiser le processus tout en minimisant les risques liés aux configurations manuelles. Bien que des défis aient été rencontrés, notamment

l'apprentissage des outils de sécurité et la résolution des problèmes liés aux fichiers manquants, ce projet a permis de développer des compétences techniques et de renforcer la sécurité des communications de l'entreprise. Les prochaines étapes visent à améliorer la documentation, à tester le script sur un plus large éventail de distributions Linux et à envisager l'ajout de nouvelles fonctionnalités pour une gestion encore plus proactive de la sécurité.

Cette première période m'a permis de me familiariser avec l'environnement technique de GEDIS TELECOM et d'acquérir des compétences en script bash et en sécurisation des systèmes Linux.