Rapport de Travaux Pratiques
Sécurisation des systèmes VoIP

Djamil [Ton Nom]

25 Février 2026

1 Accès et Déploiement du Serveur

1.1 Accès SSH via Clé Publique

Conformément aux consignes, une paire de clés SSH a été générée. La clé publique a été déposée sur la plateforme de partage pour permettre l'accès au serveur.

- **Commande :** `ssh-keygen -t ed25519`
- **Connexion :** `ssh -i .ssh/id_ed25519 admin@srv-khennouchi.avalone-formation.com`

1.2 Installation de FreePBX 17

Le déploiement a été effectué sur une base Debian en suivant la procédure officielle de Sangoma :

```
cd /tmp
wget https://github.com/FreePBX/sng_freepbx_debian_install/raw/
   master/sng_freepbx_debian_install.sh  -O /tmp/
   sng_freepbx_debian_install.sh
bash /tmp/sng_freepbx_debian_install.sh
```

Lors de l'initialisation, les services de protection ont été volontairement désactivés pour la phase de test :

```
fail2ban-client stop
fwconsole firewall stop
```

Preuve de l'installation réussi de freePBX :

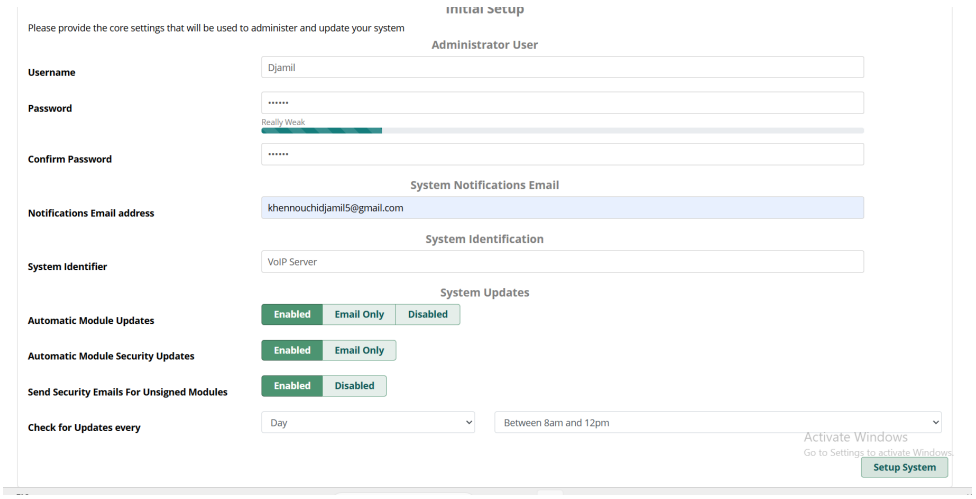

FIGURE 1 – Capture d'écran prouvant l'installation de freePBX

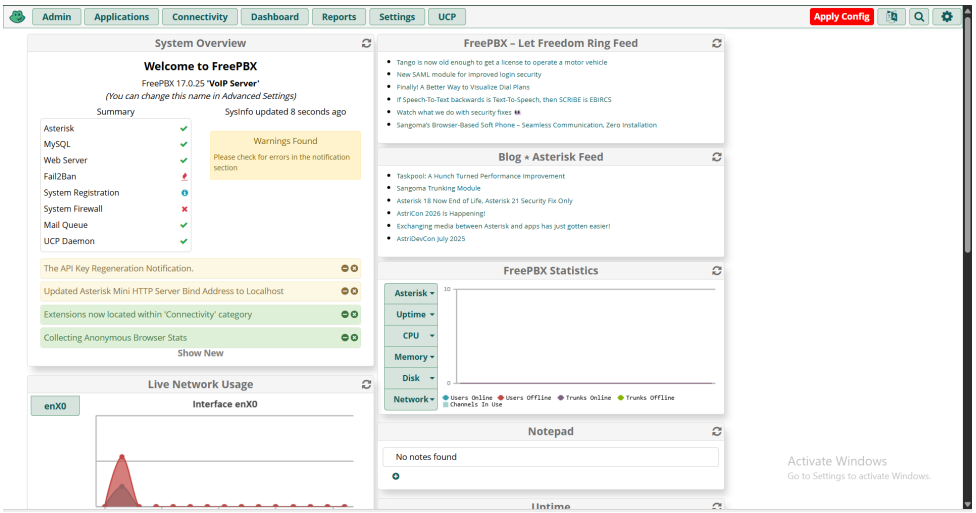

FIGURE 2 – Capture d'écran prouvant l'installation de freePBX

2 Analyse des vulnérabilités et interception

2.1 Paramétrage de base et communication SIP

Deux terminaux (Linphone sur PC et smartphone) ont été configurés pour communiquer via le serveur. Les extensions 101 et 102 ont été créées pour ces tests.

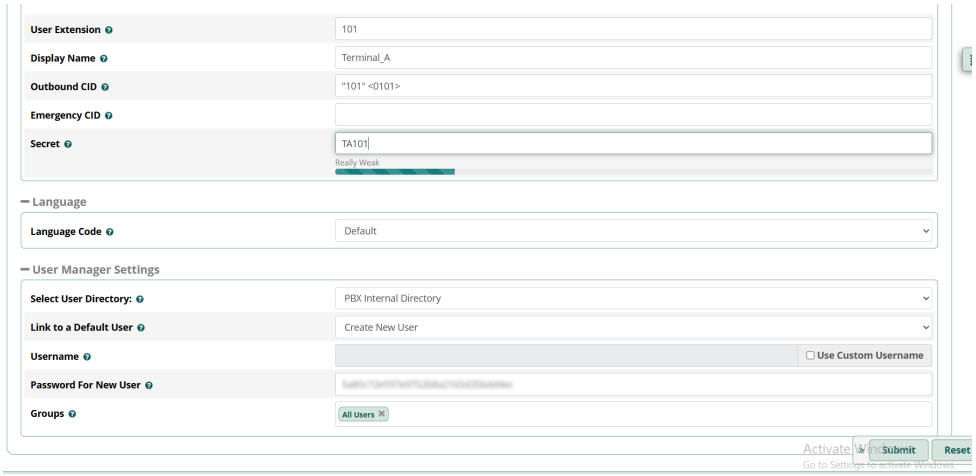

FIGURE 3 – Configuration du compte SIP 101

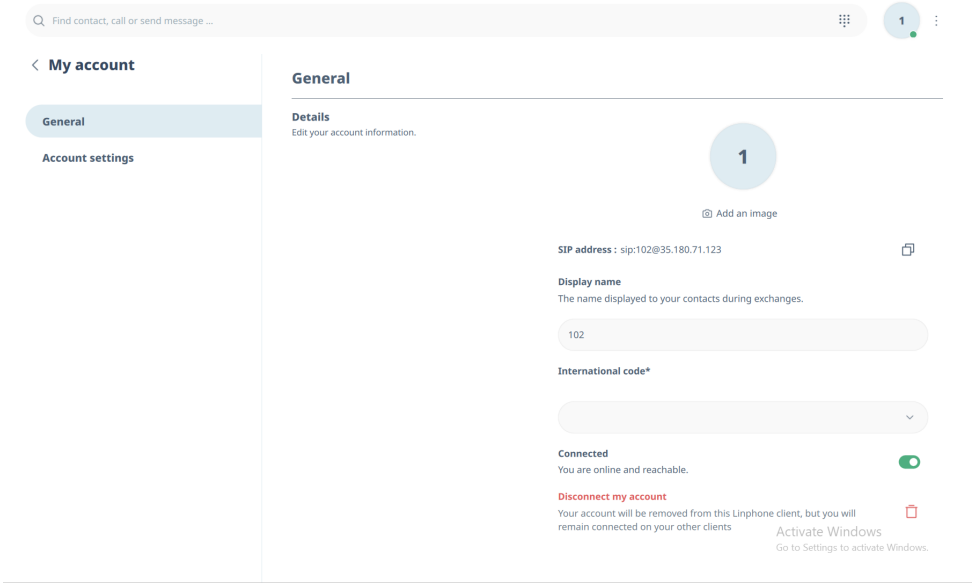

FIGURE 4 – Preuve de Configuration du compte SIP 102

2.2 Interception de trafic (Flux en clair)

À l'aide de Wireshark et de Asterisk, nous avons capturé le trafic entre les deux terminaux.

Vous pouvez retrouver l'intégralité des captures réseau au format .pcapng à l'adresse suivante : Lien vers les captures Wireshark.

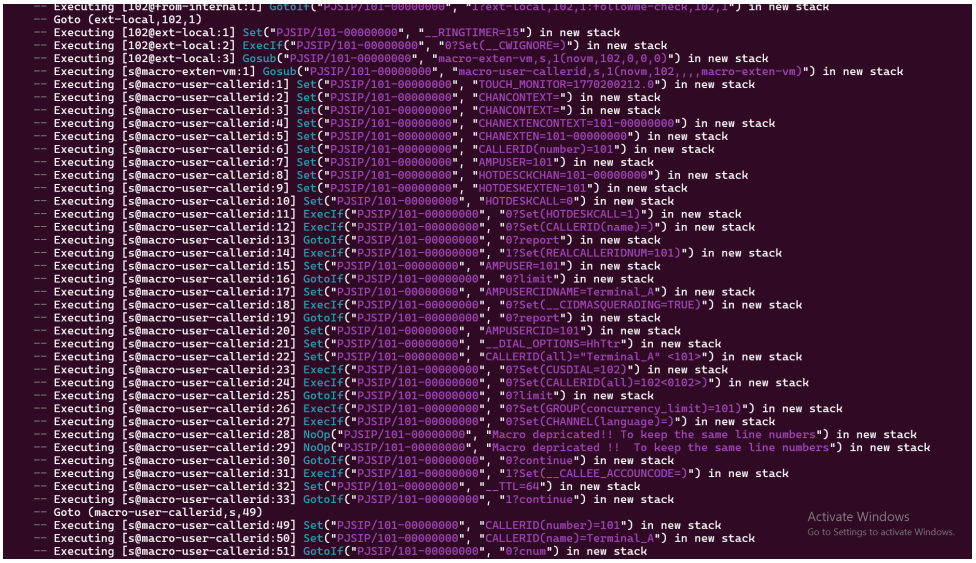

FIGURE 5 – Ecoute de l'appel entre les deux compte SIP sur Asterisk

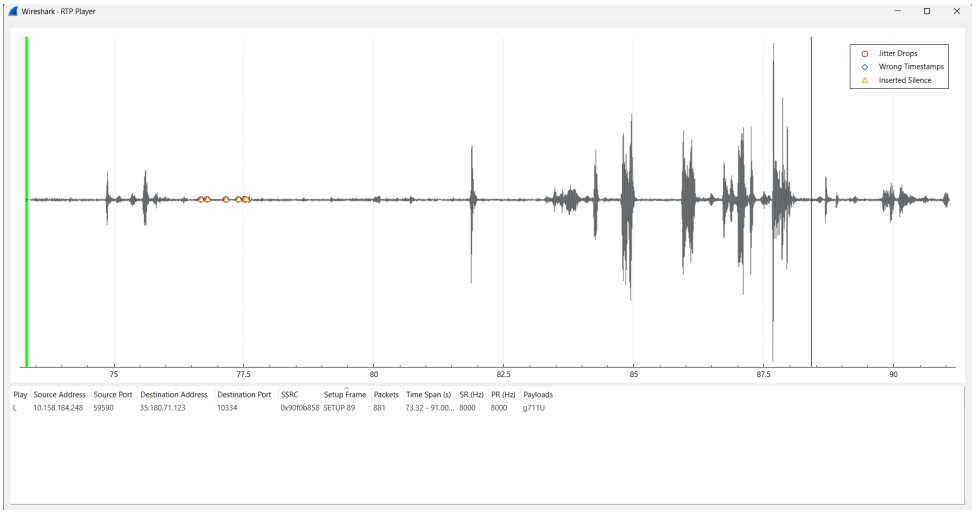

FIGURE 6 – Ecoute de l'appel entre les deux compte SIP sur Wireshark

— **Observation :** Les messages SIP circulent en UDP sur le port 5060.
— **Résultat :** Le flux RTP n'étant pas chiffré, l'outil "RTP Player" de Wireshark permet de reconstituer et d'écouter l'intégralité de la conversation.

3 Sécurisation des communications

3.1 Activation du SRTP

Le protocole SRTP a été activé pour chiffrer les flux médias.

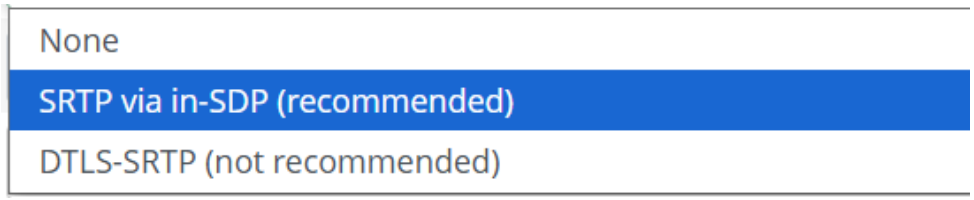

FIGURE 7 – Activation du SRTP sur FreePBX

— **Démonstration :** L'écoute n'est plus possible (bruit blanc ou données illisibles).
— **Analyse de la clé :** Bien que les médias soient chiffrés, la clé de chiffrement est visible dans le message SIP INVITE sous l'attribut `a=crypto`. La sécurité est donc partielle.

FIGURE 8 – Visualisation de la clé de chiffrement SRTP dans le paquet SIP

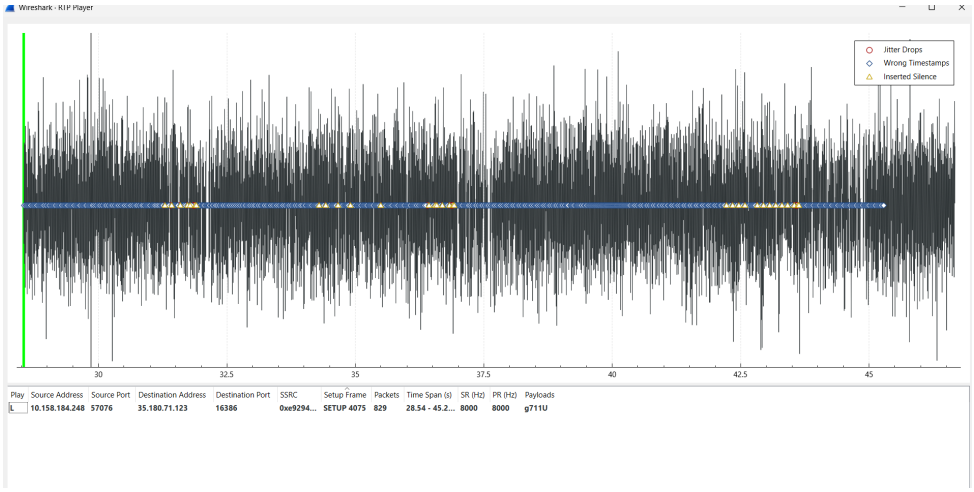

FIGURE 9 – Ecoute de l'appel en SRTP

3.2 Activation de SIP sur TLS

Pour rendre la sécurité robuste, nous avons encapsulé la signalisation dans un tunnel TLS.

— **Configuration :** Utilisation du port TCP/5061 avec un certificat Let's Encrypt.

```
        apt install certbot python3-certbot-apache
        certbot --apache -d srv-khennouchi.avalone-formation.
           com
        cp /etc/letsencrypt/archive/srv-masset.avalone-
           formation.com/privkey1.pem /etc/asterisk/keys/
           default.key
        cp /etc/letsencrypt/archive/srv-khennouchi.avalone-
           formation.com/fullchain1.pem /etc/asterisk/keys/
           default.crt
        chown asterisk:asterisk /etc/asterisk/keys/default.*
        #permet d'installer un certificat valide sur FreePBX
```

— Dans le fichier **/etc/asterisk/pjsip.transports.conf** on as rajouter ceci :

```
        [0.0.0.0-tls]
type=transport
protocol=tls
bind=0.0.0.0:5061
external_media_address=82.65.56.108
external_signaling_address=82.65.56.108
ca_list_file=/etc/ssl/certs/ca-certificates.crt
cert_file=/etc/asterisk/keys/default.crt
priv_key_file=/etc/asterisk/keys/default.key
method=tlsv1_2
verify_client=yes
verify_server=yes
allow_reload=no
tos=cs3
cos=3
```

```
    local_net=172.31.0.0/20
```

— **Résultat :** Wireshark ne peut plus déchiffrer les messages SIP. La clé SRTP n'est plus exposée. La communication est désormais sécurisée de bout en bout contre l'interception et l'homme du milieu (MITM).

4 Travaux pratiques

4.1 Fail2ban et Pare-feu

Après les phases de test, Fail2ban et le pare-feu ont été réactivés pour protéger le serveur contre les attaques par force brute (Brute Force).

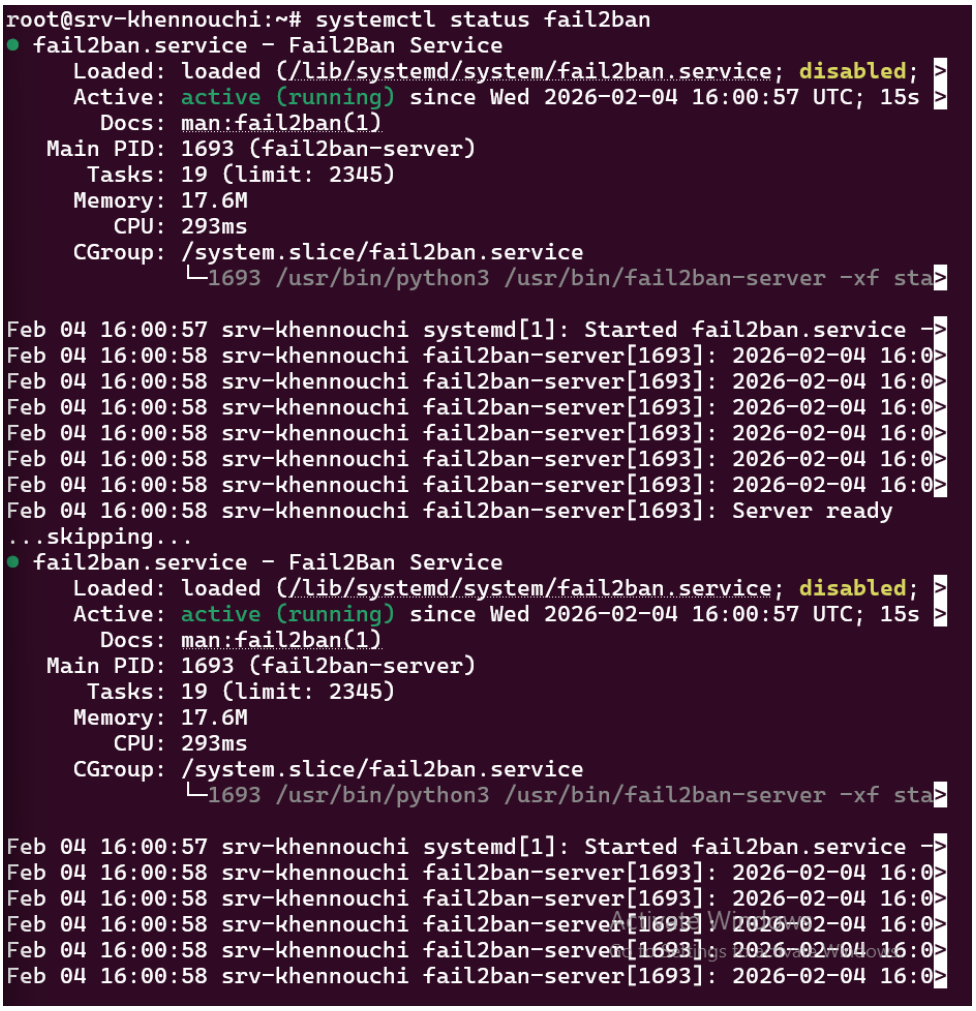

FIGURE 10 – Réactivation du service fail2ban

4.2 Teste d'attaque

Afin de s'assurer de l'activation du fail2ban sur FreePBX nous avons tenter de se connecter a un compte SIP en utilisant un faux mot de passe et après plusieurs tentatives voici le résultat afficher sur Asterisk grace a la commande :

```
fail2ban-client status asterisk-iptables
```

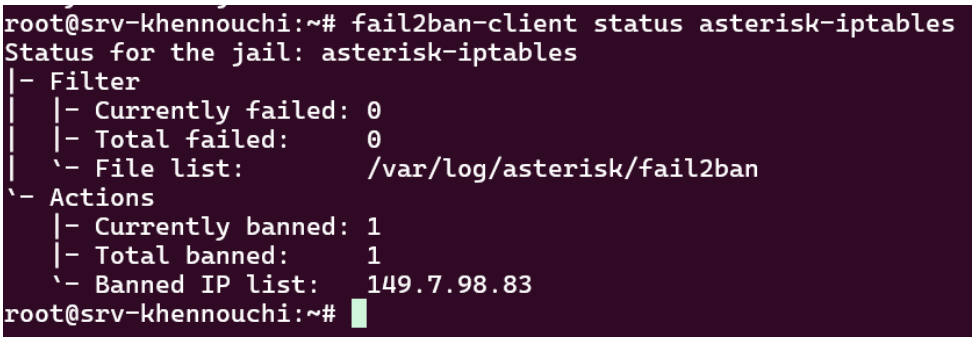

FIGURE 11 – Affichage de l'IP bannie

5 Conclusion

Ce TP a permis de démontrer les risques d'une infrastructure VoIP non sécurisée. Le passage au couple TLS/SRTP, complété par Fail2ban, assure une protection efficace contre les interceptions et les intrusions.