SÉCURITÉ VOIP

Sécurité de l'application

- Firewall hard. (SBC Session Border Controler)
- Firewall software sur la machine
- Mot de passe fort ou authentification forte
- Protéger le sip contre le relaying
- Désactiver les protocole non utilisé
- Activation des log et CDR (call detail record)

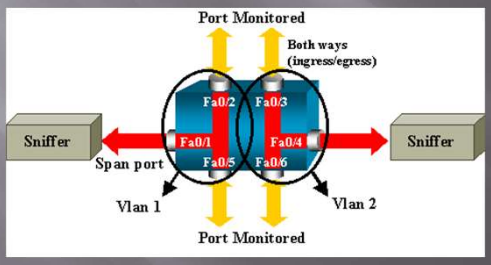
Sécurité de l'authentification

- Exemple d'insécurité au niveau de l'authentification.

Démonstration

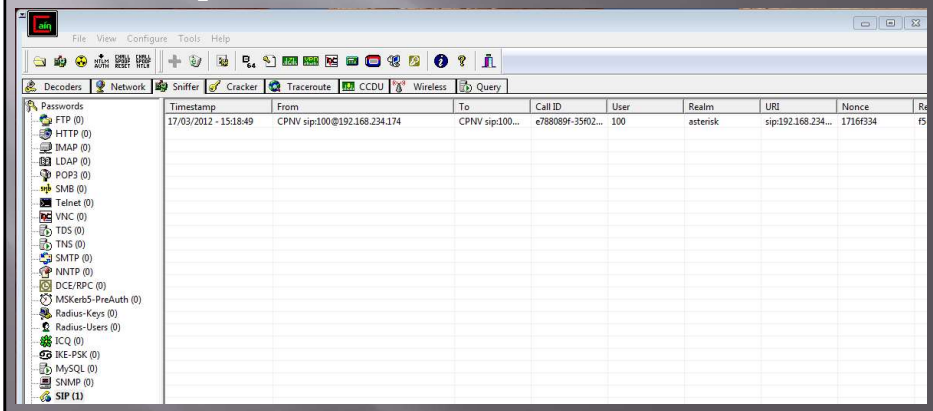
Sniff du réseau

- Collecter les informations entre le téléphone (UA) et le registrar à l'aide d'un port mirroring
- Création d'un dump de l'échange



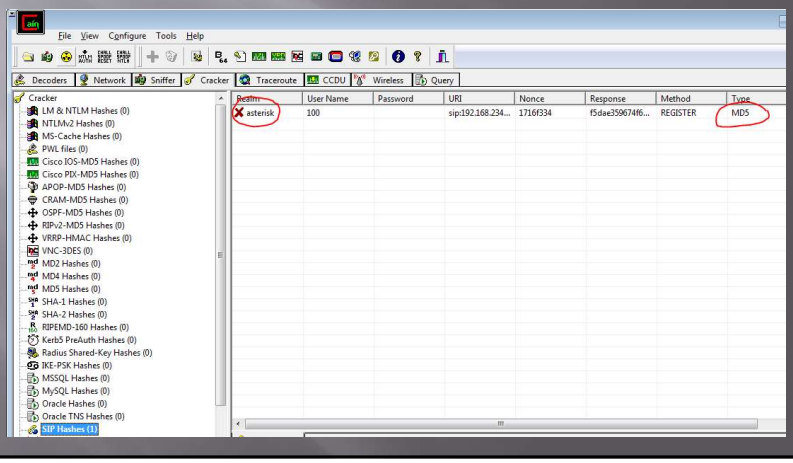
Analyse de l'authentification

- Analyser à l'aide d'un utilitaire le contenu du dump.

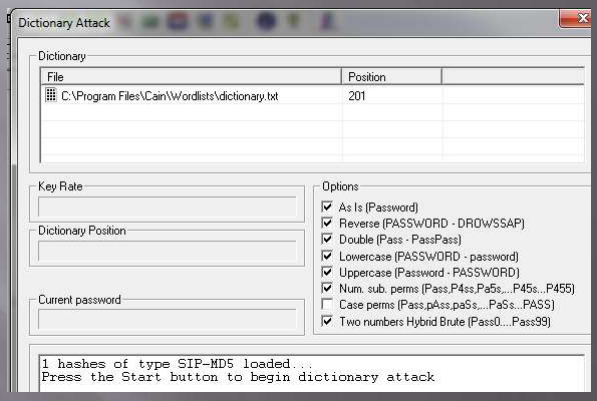


Crack du mot de passe

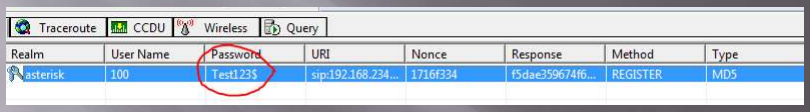
- Brute forcer le challenge md5 pour retrouver le mot de passe



Utilisation d'un dictionnaire



Crack à l'aide du dictionnaire

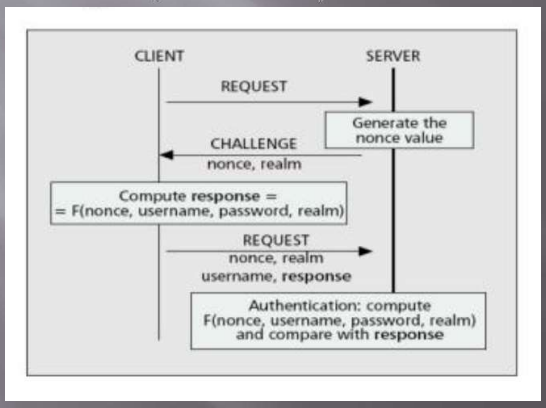


Authentification SIP

$$HA1 = MD5(A1) = MD5(username : realm : password)$$

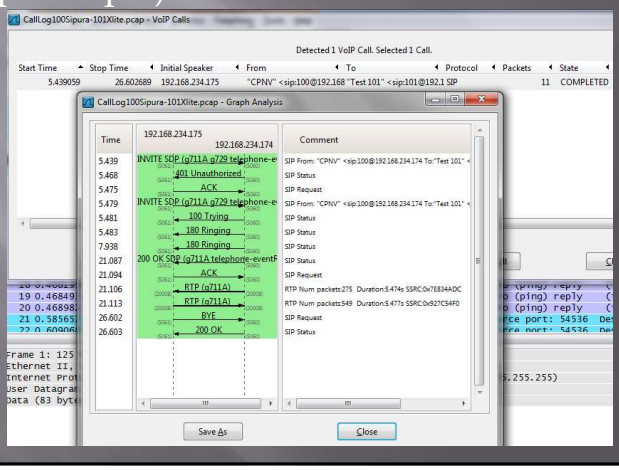
$$HA2 = MD5(A2) = MD5(method : digestURI)$$

$$response = MD5(HA1 : nonce : HA2)$$

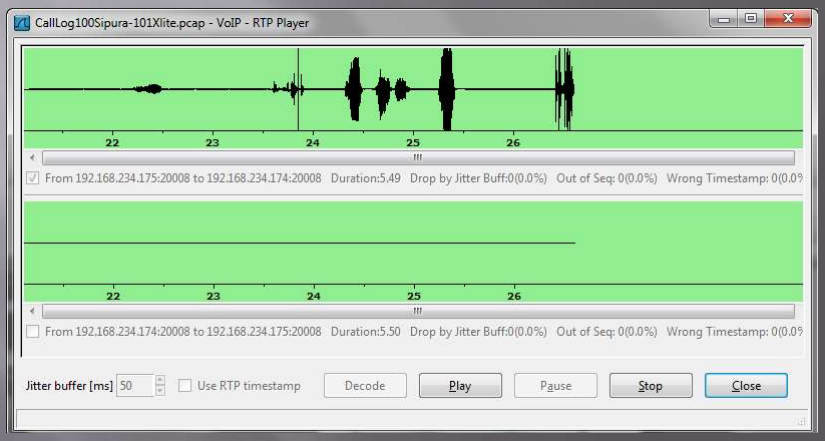


Ecoute d'une conversation

- Problème de confidentialité (Ecoute téléphonique)

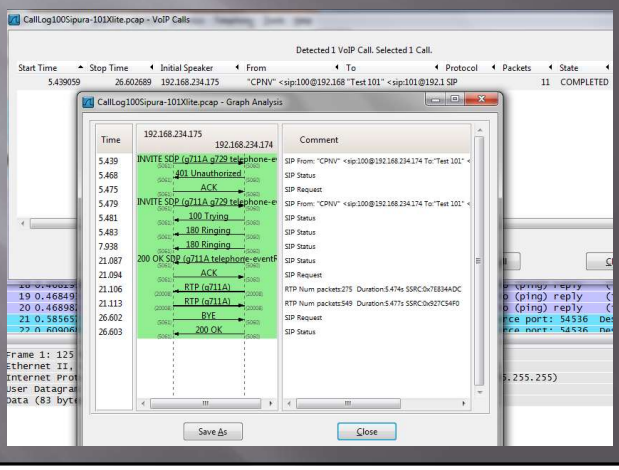


Décodage flux audio



Sécuriser la signalisation

- Sans encryptions de la signalisation.



Sécuriser la signalisation

- Mise en place de TLS