RAPPORT YDAYS 21/10/20
BAUDRIN CORENTIN

Liste des root me clear :

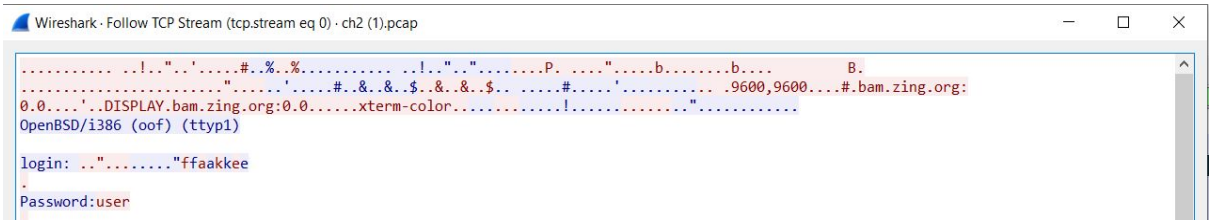
FTP - Authentification :

On importe le fichier dans wireshark.
Depuis ce dernier on filtre les lignes FTP.
Dans ces lignes on peut remarquer notamment 2 lignes où l'on peut y voir ligne d'entrée password et ce qu'il y a était entré.

```
FTP        91 Response: 331 Enter password.
FTP        81 Request: PASS cdts3500
```

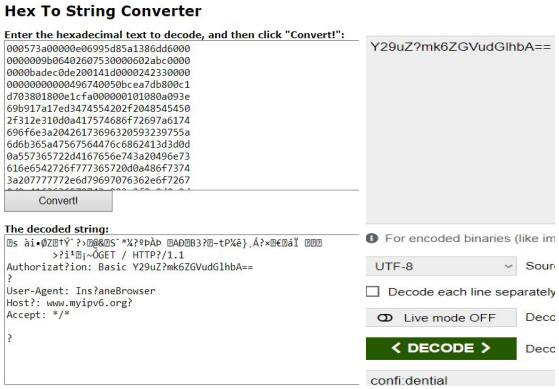
TELNET - authentification

En voyant les nombreux bytes SYN, SYN/ACK et ACK on voit une ouvertures de connexion.
On utilise alors l'outils analyser => suivre => flux tcp qui nous donne alors une boîte de dialogue nous donnant toutes les informations dont nous avons besoins



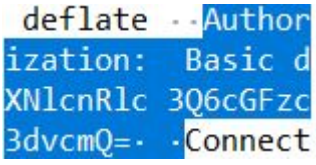
ETHERNET - trame

On nous donne une trame en hexadécimal à convertir.
Dans cette dernière après avoir chercher dans la documentations on repères un mot de passe à déchiffrer en base64



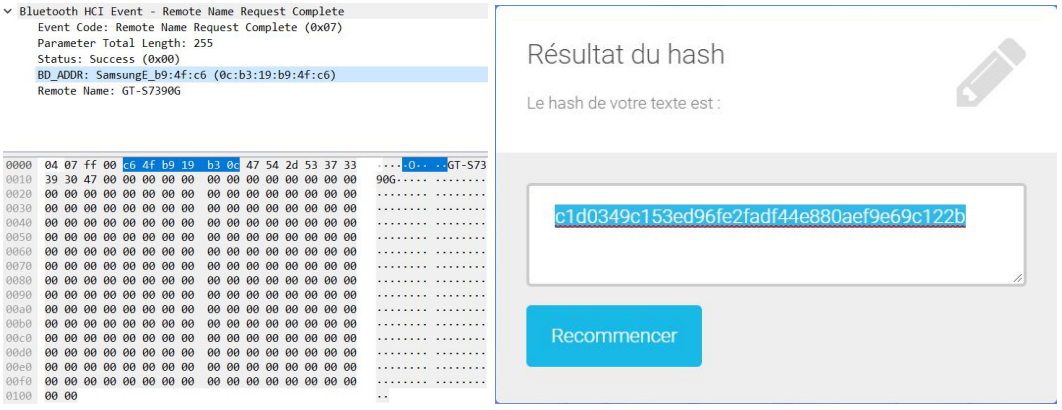
Authentification twitter

je repère une ligne ressemblant fortement à celle de l'exercice précédent précédé de “Authorization basic”et suivi de “connect” je décrypte en base 64 cette ligne et obtient le mot de passe



Bluetooth - Fichier inconnu

Je charge le fichier dans wireshark et cherche dedans afin d’obtenir le modèle du téléphone et son adresse mac ensuite je met tout en majuscule comme stipuler dans l’énoncé et obtient le code en SAH1



CISCO - mot de passe

on repère directement ceci

```
enable secret 5 $1$p8Y6$MCdRLBzuGlfOs9S.hXOp0.
```

Mais impossible à cracker car encoder en MD5.

Dessous on repère ceci

```
username hub password 7 025017705B3907344E
username admin privilege 15 password 7 10181A325528130F010D24
username guest password 7 124F163C42340B112F3830
```

Ces mot de passe sont encoder en MD7 on peut donc les cracker
Mot de passe de hub : *6sK0_Hub*
Mot de passe de admin : *6sK0_Admin*
Mot de passe de guest : *6sK0_Guest*

On nous a demandé de cracker le mot de pass de enable.
J'en déduis donc que le mot de passe est *6sK0_Enable*

IP - Time To Live

Je cherche les ping avec des réponses je l'ai trouve en bas.
J'essaie donc leurs valeur de TTL des request, la réponse était bien celle ci : 13

SIP - Authentification

J'ai analysé les 3 lignes et est remarqué que les mot de passe des deux dernières sont en MD5 donc impossible à cracker j'ai donc pris les mot de passe afficher 1234 et l'est rentré et c'est tout

```
172.25.105.3"172.25.105.40"555"asterisk"REGISTER"sip:172.25.105.40"4787f7ce"""PLAIN"1234
172.25.105.3"172.25.105.40"555"asterisk"INVITE"sip:1000@172.25.105.40"70fbfdae"""MD5"aa533f6efa2b2aba
c675c1ee6cbde327
172.25.105.3"172.25.105.40"555"asterisk"BYE"sip:1000@172.25.105.40"70fbfdae"""MD5"0b306e9db1f819dd824
acf3227b60e07
```