

RAPPORT YDAYS 21/10/20

BAUDRIN CORENTIN

Liste des root me clear :

FTP - Authentication :

On importe le fichier dans wireshark.

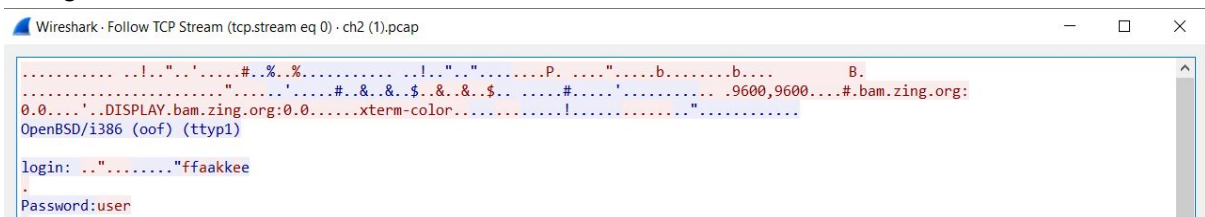
Depuis ce dernier on filtre les lignes FTP.

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 été entré.

FTP	91 Response: 331 Enter password.
FTP	81 Request: PASS cdt3500

TELNET - authentication

En voyant les nombreux bytes SYN, SYN/ACK et ACK on voit une ouverture de connexion. On utilise alors l'outil 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

Hex To String Converter

Enter the hexadecimal text to decode, and then click "Convert!":

```
0000573a00000e995de5e1306d0000
0000009b0c402607530000002abc0000
0000badec0de200141d0000242330000
0000000000049674005bcea7db800c1
d703801800e1cf8a000000101000a093e
69b917a17ed3474554202f20d8545450
2f312e310d0a417574686f72697a6174
696f6e3a20426173696320593239755a
6d6b365a47567564476c6862413d300d
0a557365722d4167656e743a20496e73
616e6542726f777365720d0a486f7374
3a20777772e6d79697076362e6f7267
```

Convert!

The decoded string:

```
Os ai-QZBY ?Q60S *%?hbb-0AD0B3?B-tP%e).A?@eB&Y 000
>?1Ej~cGET / HTTP?/1.1
Authorization: Basic Y29uZ?mk6ZGVudGlibA==
?
User-Agent: Ins?aneBrowser
Host?: www.myspbv.org?
Accept: */*
?
```

Y29uZ?mk6ZGVudGlibA==

For encoded binaries (like im

UTF-8 Sour

Decode each line separately

Live mode OFF Decc

< DECODE > Decc

confidential

Authentication 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

```
deflate --Author
ization: Basic d
XNlcnRlc 3Q6cGFzc
3dvcmQ=- Connect
```

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

Bluetooth HCI Event - Remote Name Request Complete

Event Code: Remote Name Request Complete (0x07)

Parameter Total Length: 255

Status: Success (0x00)

BD_ADDR: SamsungE_b9:4f:c6 (0c:b3:19:b9:4f:c6)

Remote Name: GT-S7390G

0000	04 07 ff 00	e6 4f b9 19	b3 0c	47 54 2d 53 37 33	...	0...	GT-S73
0010	39 30 47 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	90G	
0020	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00		
0030	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00		
0040	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00		
0050	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00		
0060	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00		
0070	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00		
0080	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00		
0090	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00		
00a0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00		
00b0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00		
00c0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00		
00d0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00		
00e0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00		
00f0	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00		
0100	00 00						

Résultat du hash

Le hash de votre texte est :

c1d0349c153ed96fe2fadf44e880aef9e69c122b

Recommencer

CISCO - mot de passe

on repère directement ceci

```
enable secret 5 $1$p8Y6$McdRLBzuGlF0s9S.hX0p0.
```

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 encodés en MD5 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 passe 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 trouvé en bas.

J'essaie donc leurs valeurs de TTL des requêtes, la réponse était bien celle-ci : 13

SIP - Authentification

J'ai analysé les 3 lignes et est remarqué que les mots de passe des deux dernières sont en MD5 donc impossible à cracker j'ai donc pris les mots de passe affichés 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"70fbfdac""MD5"aa533f6efa2b2abac675c1ee6cbde327
172.25.105.3"172.25.105.40"555"asterisk"BYE"sip:1000@172.25.105.40"70fbfdac""MD5"0b306e9db1f819dd824acf3227b60e07
```