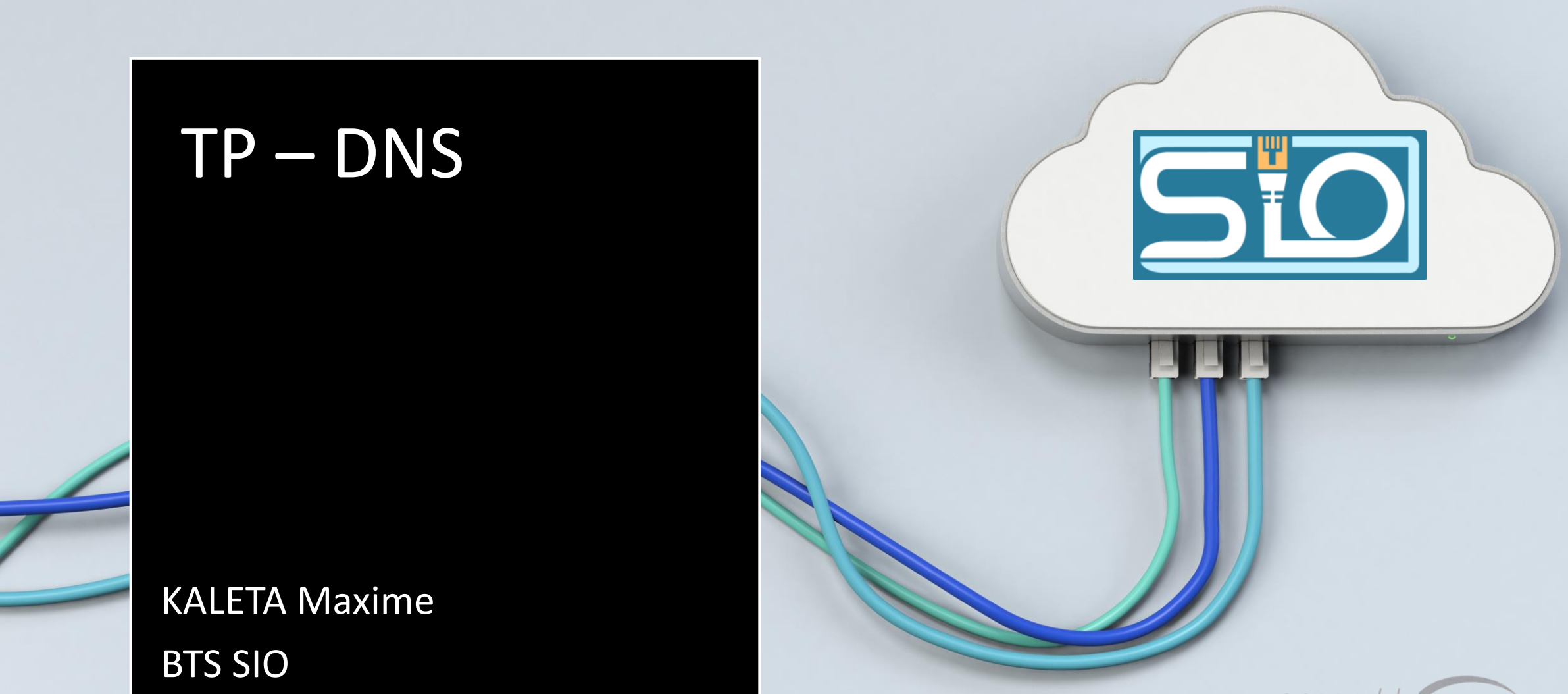
TP – DNS

KALETA Maxime

BTS SIO



ensemble SAINT-LUC Cambrai
Les chemins de la réussite

Sommaire

- Deux commandes liées au DNS
- Sécurisation d'un poste
- Accélération d'un poste
- Capture de trame avec Wireshark
- Reverse DNS

KALETA Maxime

Deux commandes liées au DNS

- Commande: ipconfig/displaydns

L'option "displaydns" va permettre d'afficher les enregistrements DNS actuellement en cache sur votre poste local.

```
C:\Users\windows10>ipconfig/displaydns

Configuration IP de Windows

    oneclient.sfx.ms
    ----------------------------------------
    Nom d'enregistrement. : oneclient.sfx.ms
    Type d'enregistrement : 5
    Durée de vie  . . . . : 1
    Longueur de données . : 8
    Section . . . . . . . : Réponse
    Enregistrement CNAME  : oneclient.sfx.ms.edgekey.net

    Nom d'enregistrement. : oneclient.sfx.ms.edgekey.net
    Type d'enregistrement : 5
    Durée de vie  . . . . : 1
    Longueur de données . : 8
    Section . . . . . . . : Réponse
    Enregistrement CNAME  : e9659.dspg.akamaiedge.net

    Nom d'enregistrement. : e9659.dspg.akamaiedge.net
    Type d'enregistrement : 1
    Durée de vie  . . . . : 1
    Longueur de données . : 4
    Section . . . . . . . : Réponse
    Enregistrement (hôte) : 23.57.82.40
```

KALETA Maxime

Deux commandes liées au DNS

- Commande : ipconfig/flushdns

Le cache DNS est vidé.

```
C:\Users\windows10>ipconfig/flushdns

Configuration IP de Windows

Cache de résolution DNS vidé.
```

Un client dispose d'un ou plusieurs serveurs DNS à contacter lorsqu'il a besoin de résoudre un nom

de domaine. Les adresses de ces serveurs sont visibles grâce à la commande IPCONFIG / ALL

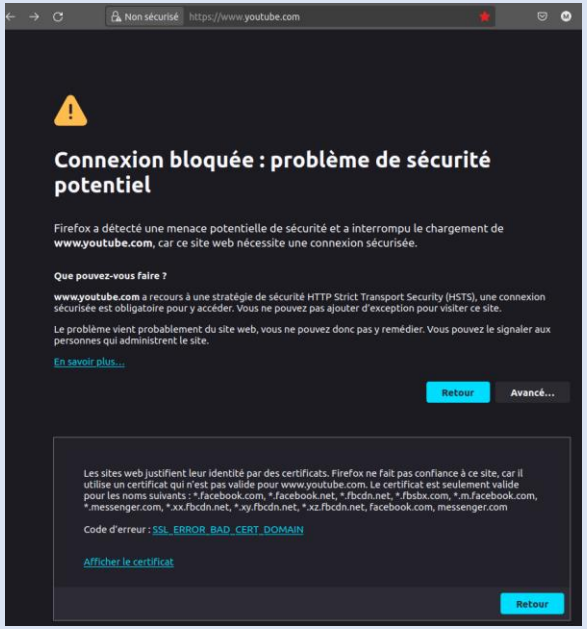
KALETA Maxime

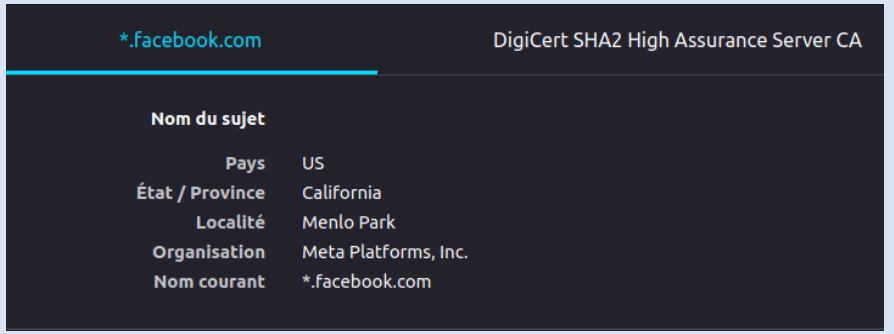
Sécurisation d'un poste

Après avoir **changé l'ip dans le dossier host du pc pour l'URL "www.youtube.com"**, lorsque j'y accède il y a une erreur de connexion. Cependant lorsque je met l'IP de facebook associée au DNS de youtube le navigateur m'informe de la sécurité de navigation.

```
 GNU nano 6.2                                                    hosts
127.0.0.1       localhost
127.0.1.1       maxime-HP-ZBook-15-G5
185.60.219.35   www.youtube.com
# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Cependant nous pouvons voir qu'il ramène bien à facebook

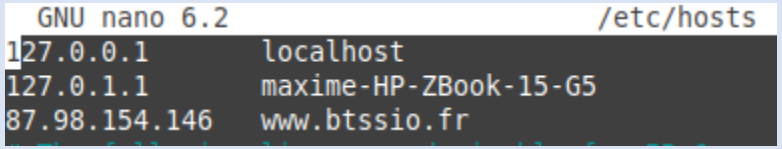




KALETA Maxime

Accélération d'un poste

Le poste client lui va interroger directement l'IP pour permettre une connexion plus rapide.



KALETA Maxime

Capture de trame avec Wireshark

Après avoir recherché « www.btssio.fr » dans un navigateur j’ai obtenu la trame suivant

j’ai filtré les demande DNS en marquant « dns » dans le filtre.

J'ai donc obtenu cette trame.

« 1656 357.685112192 2a01:cb0c:f03:ca00:f281:75ff:fe75:a0f0 2a01:cb0c:f03:ca00:e50a:e886:7e41:367 DNS 116 Standard query response 0xe138 **A btssio.fr A 87.98.154.146** OPT »

L’adresse IP auquel le btssio.fr est associé est 87.98.154.146

KALETA Maxime

Reverse

Reverse:

Désormais nous recherchons un domaine à partir d'une IP

Grâce à la commande "nslookup" puis l'option PTR (PoinTeRs)

```
maxime@maxime-HP-ZBook-15-G5:~$ nslookup
> set type=PTR
> 87.98.154.146
Server:         127.0.0.53
Address:        127.0.0.53#53

146.154.98.87.in-addr.arpa      name = www.btssio.fr.
```

Nous voyons nien que l'IP est associée à l'URL "www.btssio.fr"

KALETA Maxime